European Parliament
2019-2024

Committee on Economic and Monetary Affairs
Committee on Civil Liberties, Justice and Home Affairs

2021/0239(COD)

Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

Rapporteur: Eero Heinäluoma, Damien Carême

(Joint committee procedure – Rule 58 of the Rules of Procedure)

COMPROMISE AMENDMENTS
AML REGULATION (FULL TEXT)

Outcome of shadows of 22 March 2023 - new changes following political and technical meetings are highlighted in *turquoise*

**Text is cleaned from technical deletions of amendments already agreed]*

***Amendments on articles subject to compromises will normally fall if the compromise is adopted*

CHAPTER I

GENERAL PROVISIONS

Section 1

Subject matter and definitions

COMP A

Article 1 - Subject matter
AMs covered: 19 (co-rapporteurs), 20 (co-rapporteurs),
AMs falling: 253 (The Left), 254 (The Left), 255 (ECR), 256 (The Left)

Recitals 1, 2, 2a, 3, 3a, 3b, 4
AMs covered: 1 (co-rapporteurs), 123 (ECR), 124 (S&D), 126 (Renew), 127 (ECR), 128 ECR, 130 (Renew), 131 (ID), 167 (Renew)
AMs falling: 125 (ECR), 129 (ID)

Article 1

Subject matter

This Regulation lays down rules concerning:

(a) the measures to be applied by obliged entities to prevent ~~***and uncover* (253)**~~ money laundering and terrorist financing;

(aa) the preventative measures to be applied by obliged entities to mitigate and manage the risks of non-implementation and evasion of targeted financial sanctions;

(ab) the prevention of money laundering and terrorist financing in Member States which allow for citizenship or residence rights in exchange for any kind of investment, including capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget; (19)

(b) beneficial ownership transparency requirements for legal entities and arrangements;

(c) measures to ***mitigate risks deriving from anonymous instruments and*** limit the misuse of ~~***ban the use of (20)***~~ bearer instruments.

Recital 1

(1) Directive (EU) 2015/849 of the European Parliament and of the Council[23] constitutes the main legal instrument for the prevention of the use of the Union financial system for the purposes of money laundering and terrorist financing. That Directive sets out a comprehensive legal framework, which Directive (EU) 2018/843 of the European Parliament and the Council[24] further strengthened by addressing emerging risks and increasing transparency of beneficial ownership. Notwithstanding ***the*** achievements ***of Directive (EU) 2015/849, divergent practices regarding its enforcement and the lack of correct implementation of minimum standards (123) have led to a fragmented, incomplete and partially inefficient regulatory landscape in the Union. Therefore,*** **(1)** experience has shown that further improvements should be introduced to adequately

mitigate risks, ***tackle divergences regarding its enforcement and implementation (124, 126)*** and to effectively detect criminal attempts to misuse the Union financial system for criminal purposes.

Recital 2

(2) The main challenge identified in respect to the application of the provisions of Directive (EU) 2015/849 laying down obligations for private sector actors, the so-called obliged entities, is the lack of direct applicability of those rules and a fragmentation of the approach along national lines. Whereas those rules have existed and evolved over three decades, ***as a rule*** **(127)** they are still implemented in a manner not fully consistent with the requirements of an integrated internal market. Therefore, it is necessary that rules on matters currently covered in Directive (EU) 2015/849 which may be directly applicable by the obliged entities concerned are addressed in a new Regulation in order to achieve the desired uniformity of application ~~***and to eliminate divergences and inconsistencies of implementation practices within Member States***~~**. (126)**

Recital 2a

(2a) ~~whereas,~~ In the current unstable situation of increased security threats, the EU legal framework for combating money laundering and terrorist financing should be strengthened and harmonised so as to close existing gaps and tighten up current regulations in order to hinder criminal activity in this area; (128)

Recital 2b

(2b) The illegal, unprovoked and unjustified military aggression against Ukraine has been strongly condemned by the Union and has led to a severe embargo on Russian banks and oligarchs by the Member States, while also highlighting schemes of money laundering by Russian banks through EU banks services. It is important in this sense to recognize the potential that long-term maintenance of sanctions has in reducing the risk of Russian money laundering in the Union (167)

Recital 3a

(3a) It is estimated by the United Nations Office of Drugs and Crime (UNODC) that between 2 and 5% of global GDP is laundered each year. In addition, it is estimated that about 1.5% of the European Union's GDP is subject to money laundering and only about 1% of the money is ultimately confiscated[1]. Therefore, it is essential for Member States, apart from reinforcing ~~their~~ rules ~~in order~~ to prevent money laundering and terrorist financing, to devote substantial efforts to recover ill-gotten money~~, to use the money recovered from operations with the purpose to address challenges emerged from current and future crises~~. (130, 131)

COMP B

Article 2 – Definitions

AMs covered: 21 (co-rapporteurs), 22 (co-rapporteurs, 23 (co-rapporteurs), 24 (co-rapporteurs), 25 (co-rapporteurs), 26 (co-rapporteurs), 27 (co-rapporteurs), 28 (co-rapporteurs), 259 (Greens),

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021SC0190

260 (S&D), 262 (S&D/Greens), 263 (S&D/Greens), 265 (EPP), 268 (ECR), 269 (EPP), 271 (The Left), 272 (The Left), 274 (EPP), 275 (Greens), 276 (Greens), 277 (ECR), 279 (Greens), 280 (ID), 281 (S&D/Greens), 283 (The Left), 284 (The Left), 285 (S&D/Greens), 289 (ID), 290 (The Left), 291 (EPP), 294 (ID), 298 (EPP), 302 (ID), 303 (The Left), 305 (The Left), 306 (ECR), 307 (S&D/Greens), 308 (ID), 309 (ECR), 311 (S&D/Greens), 312 (S&D), 313 (EPP), 317 (Renew), 318 (ID), 319 (ID), 320 (EPP), 321 (EPP)

AMs falling: 257 (The Left), 258 (The Left), 261 (EPP), 264 (EPP), 266 (ECR), 267 (EPP), 270 (EPP), 273 (ECR), 278 (ECR), 282 (EPP), 287 (ID), 286 (EPP), 288 (The Left), 292 (The Left), 293 (ID), 295 (ID), 296 (ID), 297 (ID), 299 (ID), 300 (ID), 301 (ID), 304 (ECR), 310 (ECR), 314 (ID), 315 (ECR), 316 (ID), 317 (RN), 318 (ID), 319 (ID), 320 (EPP), 322 (ECR), 323 (ECR), 324 (EPP)

Recital 5
AMs covered: 132 (Renew)
AMs falling:

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) ‘money laundering’ means the conduct as set out in Article 3, paragraphs 1 and 5 of Directive (EU) 2018/1673 including aiding and abetting, inciting and attempting to commit that conduct, whether the activities which generated the property to be laundered were carried out on the territory of a Member State or on that of a third country. Knowledge, intent or purpose required as an element of that conduct may be inferred from objective factual circumstances;

(2) ‘terrorist financing’ means the conduct set out in Article 11 of Directive (EU) 2017/541 including aiding and abetting, inciting and attempting to commit that conduct, whether carried out on the territory of a Member State or on that of a third country. Knowledge, intent or purpose required as an element of that conduct may be inferred from objective factual circumstances;

(3) ‘criminal activity’ means criminal activity as defined in Article 2(1) of Directive (EU) 2018/1673, as well as fraud affecting the Union’s financial interests as defined in Article 3(2) of Directive (EU) 2017/1371, passive and active corruption as defined in Article 4 (2) and misappropriation as defined in Article 4(3), second subparagraph of that Directive;

(4) ***‘funds’ or*** ‘property’ means property as defined in Article 2(2) of Directive (EU) 2018/1673;

~~(4a) ‘funds’ means assets of any kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or an interest in, such assets; (259)~~

(5) ‘credit institution’ means a credit institution as defined in Article 4(1), point (1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[2],

[2] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

including branches thereof, as defined in Article 4(1), point (17) of that Regulation, located in the Union, whether their head office is situated within the Union or in a third country;

(6) 'financial institution' means:

(a) an undertaking other than a credit institution or an investment firm, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council[3], including the activities of currency exchange offices (bureaux de change) ***and creditors as defined in Article 4 point (2) of Directive 2014/17/EU of the European Parliament and of the Council, and in Article 3, point (b) of Directive 2008/48/EC of the European Parliament and of the Council, or an undertaking whose (260), or the*** principal activity ***of which*** is to acquire holdings, including a financial holding company and a mixed financial holding company ***but excluding the activities listed in point (8) of Annex I to Directive 2015/2366/EU [PSD1 now replaced by PSD2]***;

(aa) a central securities depository as defined in Article 2 point (1) of Regulation 909/2014/EU of the European Parliament and of the Council; (262)

~~***(ab) an account information service provider as defined in Article 4 point (19) of Directive (EU) 2015/2366 of the European Parliament and of the Council; (263)***~~

(b) an insurance undertaking as defined in Article 13, point (1) of Directive 2009/138/EC of the European Parliament and of the Council[4], insofar as it carries out life or other investment-related assurance activities covered by that Directive, including insurance holding companies and mixed-activity insurance holding companies as defined, respectively, in Article 212(1), points (f) and (g) of Directive 2009/138/EC;

(c) an insurance intermediary as defined in Article 2(1), point (3) of Directive (EU) 2016/97 of the European Parliament and of the Council[5] where it acts with respect to life insurance and other investment-related services;

(d) an investment firm as defined in Article 4(1), point (1) of Directive 2014/65/EU of the European Parliament and of the Council[6];

(e) a collective investment undertaking, in particular:

(i) an undertaking for collective investment in transferable securities as defined in Article 1(2) of Directive 2009/65/EC and its management company as defined in Article 2(1)(b) of that Directive or an investment company authorised in

---

[3] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

[4] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

[5] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast) (OJ L 26, 2.2.2016, p. 19).

[6] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (OJ L 173, 12.6.2014, p. 349).

accordance with that Directive and which has not designated a management company, that makes available for purchase units of UCITS in the Union;

(ii) an alternative investment fund as defined in Article 4(1)(a) of Directive 2011/61/EU and its alternative investment fund manager as defined in Article 4(1)(b) of that Directive that fall within the scope set out in Article 2 of that Directive;

(f) branches of financial institutions as defined in points (a) to (e), when located in the Union, whether their head office is situated in a Member State or in a third country;

(fa) crypto-asset service providers;

(6a) 'crypto-asset service providers' means a crypto-asset service provider as defined in Article 3(1), point (8), of Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final] where performing one or more crypto-asset services as defined in Article 3(1), point (9), of that Regulation, with the exception of providing advice on crypto-assets as defined in point (9)(h) of that Article.';

(6b) 'bearer share' means negotiable instrument that accords ownership in a legal person to the person who possesses the ~~physical~~ bearer share certificate, and any other similar instruments ~~without traceability~~ which does not allow the identification or traceability of the ownership of the share. It does not refer to dematerialised and/or registered forms of share certificates whose owners are traceable and identifiable ~~can be identified~~. (265)

(6c) 'bearer share warrant' means a negotiable instrument that accords entitlement to ownership in a legal person to whom possesses the ~~physical~~ bearer share warrant, and any other similar warrant or instrument which does not allow the identification or traceability of the ownership of the share ~~without traceability~~. It does not refer to dematerialised and/or registered warrants or other instruments whose owners are traceable and identifiable ~~can be identified~~. It also does not refer to any other instrument that only confers a right to subscribe for ownership in a legal person at specified conditions, but not ownership or entitlement to ownership, unless and until the instruments are exercised. (265)

(7) 'trust or company service provider' means any person that, by way of its business, provides any of the following services to third parties:

(a) the formation of companies or other legal persons;

(b) acting as, or arranging for another person to act as, a director or secretary of a company, ***namely as a nominee, (21)*** a partner of a partnership, ***a president of a management board (268)*** or a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;

(d) acting as, or arranging for another person to act as, a trustee of an express trust or performing an equivalent function for a similar legal arrangement;

(e) acting as, or arranging for another person to act as, a nominee shareholder for another person;

(7a) 'wealth or asset manager' means a natural or legal person that, by way of its business, provides services and offers products designed to grow, protect, utilise and disseminate the wealth of third parties; (22)

(8) 'gambling services' means a service which involves wagering a stake with monetary value, ***also in the form of chargeable communications (269)***, in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services;

(9) 'mortgage creditor' means a creditor as defined in Article 4, point (2) of Directive 2014/17/EU of the European Parliament and of the Council[7];

(10) 'mortgage credit intermediary' means a credit intermediary as defined in Article 4, point (5) of Directive 2014/17/EU;

(11) 'consumer creditor' means a creditor as defined in Article 3, point (b) of Directive 2008/48/EC of the European Parliament and of the Council[8];

(12) 'consumer a credit intermediary' means a credit intermediary as defined in Article 3, point (f) of Directive 2008/48/EC;

(13) 'crypto-asset' means a crypto-asset as defined in Article 3(1), point (2) of Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final] except when falling under the categories listed in Article 2(2) of that Regulation or not otherwise qualifying as funds;

(14) ~~'crypto-asset service provider' means a crypto-assets service provider as defined in Article 3(1), point (8) of Regulation *[please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final]* where performing one or more crypto-asset services as defined in Article 3(1) point (9) of that Regulation~~;

(14a) 'high-level professional football club' means a legal entity established in a Member State which owns or manages a professional football club of which at least one team plays in the championship or championships of the two highest level of competition in that Member States and has an annual turnover of at least EUR 7 000 000. ~~plays in the championship or championships of the highest level of the competition in that Member State or in the championship or championships of the second highest level of the competition in that Member State if the annual revenues of that championship exceed EUR 150 million;~~ (23, 271, 277)

(14b) 'sports agent in the football sector' means a natural person who provides private job placements in the football sector for prospective paid football players or for employers with a view to signing employment contracts for paid football players (24, 272)

---

[7] Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 Text with EEA relevance (OJ L 60, 28.2.2014, p. 34).

[8] Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ L 133, 22.5.2008, p. 66).

(15) ‘electronic money’ means electronic money as defined in Article 2, point (2) of Directive 2009/110/EC[9], but excluding monetary value as referred to in Article 1(4) and (5) of that Directive;

(15a) ***'precious metals' means gold, silver, platinium, iridium, osmium, palladium, rhodium, rhutenium ~~gold, silver, platinum and palladium, sold by jewelleries and precious metal dealers to retail customers;~~***

(15b) ‘precious stones’ means diamond, ruby, sapphire and emerald (321)

(16) ‘business relationship’ means a business, professional or commercial relationship which is ***directly (274)*** connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration, including a relationship where an obliged entity is asked to form a company or set up a trust for its customer, whether or not the formation of the company or setting up of the trust is the only transaction carried out for that customer;

(16a) ‘occasional transaction’ means a transaction that is not carried out as part of a business relationship as defined in point (16) of this Article; (275)

(16b) 'atypical transaction or fact' means a transaction or a fact which does not appear to be consistent with the customer's characteristics and with the purpose and intended nature of the business relationship or the proposed transaction; (276)

(17) ‘linked transactions’ means two or more transactions with either identical or similar origin and destination, over a specific period of time;

(18) ‘third country’ means any jurisdiction, independent state or autonomous territory that is not part of the European Union but that has its own AML/CFT legislation or enforcement regime;

(19) ‘correspondent relationship’ means:

(a) the provision of banking services by one credit institution as the correspondent to another credit institution as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;

(b) the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers ***or relationships established for crypto-asset transactions or crypto-asset transfers; (279)***

(20) ‘shell bank’ means a credit institution or financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group;

(20a) ‘unregistered or unlicenced crypto-asset service provider’ means a crypto-asset service provider that is not established in any jurisdiction or does not have a central

---

[9] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

contact point or substantive management presence in any jurisdiction ~~and that is unaffiliated with a regulated entity or that operates in the Union without authorisation under Regulation (EU) 2021/... [Regulation on Markets in Crypto-assets]~~; (25, 280)

(21) 'Legal Entity Identifier' means a unique alphanumeric reference code based on the ISO 17442 standard assigned to a legal entity;

(22) 'beneficial owner' means any natural person who ultimately owns ***or,*** controls ***~~or benefits from (283, 284)~~*** a legal entity or ***an*** express trust or similar legal arrangement***, or an organisation that has legal capacity under national law (281)***, as well as any natural person on whose behalf or for the benefit of whom a transaction or activity ***or business relationship (285)*** is being conducted;

(23) 'legal arrangement' means an express trust or an arrangement which has a similar structure or function to an express trust, including *fiducie* and certain types of *Treuhand* and *fideicomiso*;

(24) 'formal nominee arrangement' means a contract or ***~~a formal~~ equivalent*** arrangement ***~~with an equivalent legal value to a contract~~, (285)*** between the nominee and the nominator, where the nominator is a legal entity or natural person that issues instructions to a nominee to act on their behalf in a certain capacity, including as a director or shareholder, and the nominee is a legal entity or natural person instructed by the nominator to act on their behalf;

(25) 'politically exposed person' means a natural person who is or has been entrusted with ~~the following~~ prominent public functions ***including***:

(a) in a Member State:

(i) heads of State, heads of government, ministers and deputy or assistant ministers***, ~~regardless their official designation (286)~~;***

(ii) members of parliament or of similar legislative bodies***~~, including at regional level (289, 290, 291)~~***;

(iii) members of the governing bodies of political parties;

(iv) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal***~~, except in exceptional circumstances~~ (294)***;

(v) members of courts of auditors or of the boards of central banks;

(vi) ambassadors, ***~~heads of consular posts (295)~~*** chargés d'affaires and high-ranking officers in the armed forces;

(vii) members of the administrative, management or supervisory bodies of State-owned enterprises;

(viia) heads of regional and local authorities including groupings of municipalities and metropolitan regions of at least 30.000 inhabitants; (26, 298)

(b) in an international organisation:

(i) the highest ranking official, his/her deputies and members of the board or equivalent function of an international organisation;

(ii) representatives to a Member State or to the Union;

(c) at Union level:

(i) functions at the level of Union institutions and bodies that are equivalent to those listed in points (a)(i), (ii), (iv), (v) and (vi);

(d) in a third country:

(i) functions that are equivalent to those listed in point (a);

~~***(ia) other functions falling under the definition of politically exposed person, according to the country of origin; (302)***~~

(ia) other prominent public functions provided for by Member States;

(26) 'family members' means:

(a) the spouse, or the person in a registered partnership or civil union or in a similar arrangement;

(b) the children and the spouses of, or persons in a registered partnership or civil union or in a similar arrangement with, those children;

(c) the parents ***and the siblings (27, 305, 306)***;

(27) 'persons known to be close associates' means:

(a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;

(b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person;

(29a) 'parent undertaking' means :

(a) A parent undertaking of a financial conglomerate, including a 'mixed financial holding company' as defined in Article 2, point (15), of the Directive No 2002/87/CE;

(b) A parent undertaking of a group, other than that mentioned in point a), which is subject to prudential supervision on a consolidated basis, at the highest level of prudential consolidation in the Union, including a 'financial holding company' as defined in Article 4(1), point (20), of Regulation (EU) No 575/2013 and an 'insurance holding company' as defined in Article 212(1), point (f), of Directive 2009/138/EC;

(c) A parent undertaking of a group within the meaning of Article 2 (29) of this Regulation, other than those mentioned in points a) and b), which includes at least two obliged entities as defined in Article 3 of this Regulation, and which is not itself a subsidiary of another undertaking in the Union.

When several parent undertakings are identified within the same group, in accordance with the criteria mentioned above, the parent undertaking is the entity within the group which is not itself a subsidiary of another undertaking in the Union.(311)

(28) 'senior management' means, in addition to executive members of the board of directors or, if there is no board, of its equivalent governing body, an officer or employee with

sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure;

(29) 'group' means a group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU of the European Parliament and of the Council[10];

(30) 'cash' means currency, bearer-negotiable instruments, commodities used as highly-liquid stores of value and prepaid cards, as defined in Article 2(1), points (c) to (f) of Regulation (EU) 2018/1672 of the European Parliament and of the Council[11];

(31) 'competent authority' means:

(a) a Financial Intelligence Unit;

(b) a supervisory authority as defined under point (33);

(c) a public authority that has the function of investigating or prosecuting money laundering, its predicate offences or terrorist financing, or that has the function of tracing, seizing or freezing and confiscating criminal assets;

(d) a public authority with designated responsibilities for ***preventing and*** combating ***(312, 313)*** money laundering or terrorist financing;

(32) 'supervisor' means the body entrusted with responsibilities aimed at ensuring compliance by obliged entities with the requirements of this Regulation, including the Authority for anti-money laundering and countering the financing of terrorism (AMLA) when performing the tasks entrusted on it in Article 5(2) of Regulation *[please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]*;

(33) 'supervisory authority' means a supervisor who is a public body, or the public authority overseeing self-regulatory bodies in their performance of supervisory functions pursuant to Article 29 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*;

(34) 'self-regulatory body' means a body that represents members of a profession and has a role in regulating them, in performing certain supervisory or monitoring functions and in ensuring the enforcement of the rules relating to them;

(35) 'targeted financial sanctions' means both asset freezing and prohibitions to make funds or other assets available, directly or indirectly, for the benefit of designated persons and entities pursuant to Council Decisions adopted on the basis of Article 29 of the Treaty on European Union and Council Regulations adopted on the basis of Article 215 of the Treaty on the Functioning of the European Union;

(36) 'proliferation financing-related targeted financial sanctions' means those targeted financial sanctions referred to in point (35) that are imposed pursuant to Council

---

[10] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 1).

[11] Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 (OJ L 284, 12.11.2018, p. 6).

Decision (CFSP) 2016/849 and Council Decision 2010/413/CFSP and pursuant to Council Regulation (EU) 2017/1509 and Council Regulation (EU) 267/2012.

Recital 5

(5) Since the adoption of Directive (EU) 2015/849, recent developments in the Union's criminal law framework have contributed to strengthening the prevention and fight against money laundering, its predicate offences and terrorist financing. Directive (EU) 2018/1673 of the European Parliament and of the Council25 has led to a common understanding of the money laundering crime and its predicate offences. Directive (EU) 2017/1371 of the European Parliament and of the Council26 defined financial crimes affecting the Union's financial interest, which should also be considered predicate offences to money laundering. Directive (EU) 2017/541 of the European Parliament and of the Council27 has achieved a common understanding of the crime of terrorist financing. As those concepts are now clarified in Union criminal law, it is no longer needed for the Union's AML/CFT rules to define money laundering, its predicate offences or terrorist financing. Instead, the Union's AML/CFT framework should be fully coherent with the Union's criminal law framework ***with the aim to improve public safety and protection of EU citizens. (132)***

COMP C

Article 3 - Obliged entities

AMs covered: 29 (co-rapporteurs), 30 (co-rapporteurs), 31 (co-rapporteurs), 32 (co-rapporteurs), 33 (co-rapporteurs), 34 (co-rapporteurs), 35 (co-rapporteurs), 36 (co-rapporteurs), 37 (co-rapporteurs), 38 (co-rapporteurs), 328 (S&D/Greens), 329 (ECR), 331 (S&D/Greens), 333 (Greens), 334 (S&D), 335 (Greens), 337 (ID), 338 (Greens), 341 (EPP), 342 (Greens), 343 (EPP), 344 (S&D/Greens), 346 (S&D), 347 (Greens), 353 (Greens), 357 (Greens), 359 (EPP), 360 (Renew), 361 (NI), 362 (ECR), 363 (S&D), 364 (The Left), 365 (Greens), 366 (The Left), 367 (ECR), 368 (The Left), 369 (The Left),

AMs falling: 325 (ID), 326 (EPP), 327 (Renew), 330 (ECR), 332 (The Left), 336 (ECR), 339 (S&D), 340 (S&D), 345 (S&D), 348 (ID), 349 (ECR), 350 (S&D), 351 (S&D), 352 (Greens), 354 (ECR), 355 (S&D), 356 (S&D), 358 (EPP), 370 (S&D)

Recitals 6, 6a, 6b, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 18a

AMs covered: 2 (co-rapporteurs), 3 (co-rapporteurs), 4 (co-rapporteurs), 5 (co-rapporteurs), 6 (co-rapporteurs), 135 (EPP), 136 (ECR), 137 (EPP), 138 (S&D), 140 (Greens), 141 (Greens), 142 (Greens), 152 (S&D/Greens), 153 (EPP), 154 (EPP)

AMs falling: 133 (ID), 139 (ID), 143 (ID), 144 (ID), 145 (The Left), 146 (EPP), 147 (Renew), 148 (Renew), 149 (ID), 150 (Greens), 151 (EPP)

Section 2

Scope

Article 3

Obliged entities

The following entities are to be considered obliged entities for the purposes of this Regulation:

(1) credit institutions;

(2) financial institutions;

(3) the following natural or legal persons acting in the exercise of their professional activities:

(a) auditors, ~~***certified debt collectors (329)***~~ external accountants~~***, wealth or asset managers (29, 328)***~~ and tax advisors, and any other natural or legal person that undertakes to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax, ***investment or personal finance*** matters as principal business or professional activity;

(ab) certified debt collectors (329), wealth or asset managers (29, 328);

(b) notaries, ***lawyers (30, 331)*** and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning any of the following:

(i) buying and selling of real ***or virtual (333, 334)*** property or business entities;

(ii) managing of client money, securities or other assets;

(iii) opening or management of bank, savings, securities ***or crypto-assets (335)*** accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies, foundations, or similar structures;

(c) trust or company service providers;

(d) estate agents, including when acting as intermediaries in the letting of immovable property for transactions for which the monthly rent amounts to EUR ***5 000*** ~~10 000~~ ***(31, 338)*** ~~or~~ or the equivalent in national currency ***or other accepted form of payment (337)***;

(da) property developers; (338, 341)

(e) persons trading in precious metals and stones~~***, jewellery and luxury goods, including luxury watches)***~~;

(ea) persons trading in luxury goods other than metals and stones, as listed in Annex X ~~***at least EUR 10 000 or the equivalent in national currency***~~ ***(342, 343, 344)***

[Annex X

A. List of luxury goods referred to in Article 3 (ea)

(1) Jewellery, gold- or silversmith articles of a value exceeding EUR 5 000;

(2) Clocks and watches of a value exceeding EUR 5 000;

(3) Motor vehicles, aircrafts and watercrafts of a value exceeding EUR 50 000;

(4) Garments and clothing accessories of a value exceeding EUR 5 000;(f) providers of gambling services;

(g) crypto-asset service providers;

~~*(ga) undertakings acting as traders in the European Economic Area who accept crypto-assets from self hosted wallets address as means of payment for goods and services whose estimated value is above EUR 1 000 or the equivalent in national currency in situations referred in to Article 59a (346)*~~

(h) crowdfunding service providers ~~*other than those regulated by Regulation (EU) 2020/1503*~~; ***(32, 347)***

(i) persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or linked transactions amounts to at least ***EUR 5 000*** **(33)** ~~10 000~~ or the equivalent in national currency;

(ia) persons ~~*and platforms, other than crypto-asset service providers, trading or acting as intermediaries*~~ ***providing services for*** ~~*importing, minting,*~~ ***the sale and purchase of unique and not fungible crypto-assets*** ~~*that represent ownership of a unique digital or physical asset, including works of art, real estate, digital collectibles and gaming items and any other valuable*~~***; (353)***

(j) persons storing, trading or acting as intermediaries in the trade of works of art ***and luxury goods listed in Annex X*** **(357)** when this is carried out within free zones and customs warehouses, where the value of the transaction or linked transactions amounts to at least ***EUR 5 000*** ~~10 000~~ **(34)** or the equivalent in national currency;

(jb) online platforms within the meaning of Regulation [Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive2000/31/EC] which make it possible for consumers and traders to conclude distance contracts for physical goods in so far as payments of EUR 10 000 or more are made or received, regardless of whether the transaction is carried out in a single operation or in several operations which appear to be linked; (359)

(k) creditors for mortgage and consumer credits, other than credit institutions defined in Article 2(5) and financial institutions defined in Article 2(6), and credit intermediaries for mortgage and consumer credits; **(360)**

(l) investment migration operators permitted to represent or offer intermediation services to third country nationals seeking to obtain ~~*the citizenship of or (35, 361, 362, 363, 364)*~~ residence rights in a Member State in exchange of any kind of investment, including capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity to the public good and contributions to the state budget.

(la) sports agents in the football sector; (36, 366)

(lb) high-level professional football clubs;

(lc) football associations in Member States which are members of the Union of European Football Associations (37, 38, 365, 367, 368, 369)

Recital 6

(6) Technology keeps evolving, offering opportunities to the private sector to develop new products and systems to exchange funds or value. While this is a positive phenomenon, it may generate new money laundering and terrorist financing risks, as criminals

continuously manage to find ways to exploit vulnerabilities in order to hide and move illicit funds around the world. Crypto-assets service providers***, NFT platforms*** and crowdfunding platforms are exposed to the misuse of new channels for the movement of illicit money and are well placed to detect such movements and mitigate risks. The scope of Union legislation should therefore be expanded to cover these entities, in line with the recent developments in FATF standards in relation to crypto-assets. ***NFT platforms are not covered in the current definition of crypto-assets service providers under the MiCA Regulation to the extent they do not provide services in crypto-assets that are fungible and non unique. In order to close this gap and mitigate associated money laundering and terrorist financing risks, NFT platforms should therefore be included in the horizontal AML/CFT framework as a separate category of obliged entities.***

Recital 6a

(6a) Decentralised Autonomous Organisations (DAO) and other Decentralised Finance (DeFi) arrangements should also be subject to Union AML/CFT rules ~~where~~ to the extent they perform or provide for or on behalf of another person crypto-asset services which ~~they~~ are controlled directly or indirectly, including through smart contracts or voting protocols, by identifiable natural and legal persons ~~providing crypto-asset services for or on behalf of another person~~. In such cases, decentralised organisations or arrangements should be considered crypto-asset service providers falling in the scope of Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final] and this Regulation, regardless of the commercial label or their self-identification as DAO or DeFi. Where falling under the scope of this Regulation, developers, owners or operators should assess risks of money laundering and terrorist assessments before launching or using a software or platform and take appropriate measures in order to mitigate money laundering and terrorist financing risks in an ongoing and forward-looking manner. (140)

Recital 6b

(6b) The virtual world offers new opportunities for criminals to hide and channel illicit funds by exploiting it to ~~who can convert cash acquired through illegal activities into non-traceable currencies to~~ purchase and resell virtual items, such as virtual real estate, virtual lands and other high-demand goods. While there is as of today no specific regulatory framework for the metaverse ~~or legal clarity with regard to persons and companies operating in the virtual world~~, as the adoption of the metaverse expands and evolves, the risks of money laundering, terrorist financing and sanctions evasion substantially increase. Obliged entities should be aware of such risks and continue to comply with AML/CFT obligations when operating in virtual worlds, in relation to the activities and operations covered by this Regulation, such as legal professionals with experience in real estate, finance and intellectual property, which may get increasingly involved in such transactions, including when providing legal assistance or ~~tax~~ advice ~~where there is the risk of the services provided being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing~~. (142)

Recital 12

(12) Crowdfunding platforms' vulnerabilities to money laundering and terrorist financing risks are horizontal and affect the internal market as a whole. To date, diverging approaches have emerged across Member States as to the management of those risks. ***While*** Regulation (EU) 2020/1503 of the European Parliament and of the Council harmonises the regulatory approach for business investment and lending-based crowdfunding platforms across the Union and ***sets up some AML/CFT*** requirements ***limited to due diligence of*** crowdfunding ***platforms in respect of project owners and within*** authorisation procedures***, the lack of an harmonised legal framework with robust AML/CFT obligations for crowdfunding platforms creates gaps and weakens the Union AML/CFT*** safeguards. It is therefore ***necessary to ensure that all*** crowdfunding platforms***, including those already*** licensed under Regulation (EU) 2020/1503***, are subject*** to Union AML/CFT legislation. **(141)**

Recital 13

~~(13) Crowdfunding platforms that are not licensed under Regulation (EU) 2020/1503 are currently left either unregulated or to diverging regulatory approaches, including in relation to rules and procedures to tackle anti-money laundering and terrorist financing risks. To bring consistency and ensure that there are no uncontrolled risks in that environment, it is necessary that all crowdfunding platforms that are not licensed under Regulation (EU) 2020/1503 and thus are not subject to its safeguards are subject to Union AML/CFT rules in order to mitigate money laundering and terrorist financing.~~

Recital 15

(15) ***Persons trading in ~~high value goods and services of high value~~*** goods ***~~and services such as gold, silver, platinum, iridium, osmium, palladium, rhodium and ruthenium and other precious stones (153), or high value lifestyle goods, such as cultural artefacts, luxury cars, jewellery, watches, yachts and aircrafts~~ precious metals and stones as well as luxury goods*** are particularly exposed to ***very significant*** money laundering risks, ***regardless of the means of payment (154). Criminal organisations have recurrently used this method, which is easily accessible and does not require specific expertise, to convert criminal proceeds into*** goods ***that are in high demand in foreign markets***. For this reason, persons dealing in precious metals and precious stones ***and luxury goods*** should be subject to AML/CFT requirements. **(152)**

Recital 16

(16) Investment migration operators are private companies, bodies or persons acting or interacting directly with the competent authorities of the Member States on behalf of third-country nationals or providing intermediary services to third-country nationals seeking to obtain residence rights in a Member State in exchange of any kind of investments, including capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget. Investor residence ***and citizenship*** schemes present risks and vulnerabilities in relation to money laundering, corruption and tax evasion. Such risks are exacerbated by the cross-border rights associated with residence in a Member State. Therefore, it is necessary that investment migration operators are subject to AML/CFT obligations. ***In view of the risks***

and vulnerabilities presented by investor schemes, which result in the acquisition of ***either residence rights or*** nationality in exchange for such investments, ***it is necessary to provide for a ban on citizenship by investment schemes and for minimum requirements*** in the ***assessment of applicants by*** Member States***' public authorities with regards to residence by investment schemes, to ensure that enhanced due diligence measures are applied with regard to applicants and to ensure that nationals from countries listed under Articles 23, 24 and 25 are not granted any status on the basis of such schemes. ~~These requirements should be applicable to the extent that no further restrictive measures are enforced against citizenship by investment schemes~~. (5)***

Recital 18a

(18a) According to a report from the FATF of July 2009 entitled 'Money Laundering through the Football Sector', "the professional football market has undergone an accentuated growth due to a process of commercialisation. Money invested in football surged mainly as a result from increases in television rights and corporate sponsorship. Simultaneously, the labour market for professional football players has experienced unprecedented globalisation – with more and more football players contracted by teams outside their country and transfer payments of astounding dimensions. The cross border money flows that are involved may largely fall outside the control of national and supranational football organisations, giving opportunities to move and launder money. At the same time money from private investors is pouring into football clubs to keep them operating and can give the investor long term returns in terms of media rights, ticket sales, proceeds of sales of players and merchandising." In its report of 24 July 2019 to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, the Commission assessed professional football and stated that "whilst it remains a popular sport it is also a global industry with significant economic impact. Professional football's complex organisation and lack of transparency have created fertile ground for the use of illegal resources. Questionable sums of money with no apparent or explicable financial return or gain are being invested in the sport." Professional football is therefore a new sector posing high risks and high-level professional football clubs, along with sports agents in the football sector and football associations in Member States which are members of the Union of European Football Associations, should be considered obliged entities for the purposes of this Regulation. (6)

Recital 27a

27a) Obliged entities may employ staff who by virtue of their professional activities could qualify as obliged entities themselves. As the anti-money laundering/countering the financing of terrorism framework is based on the role of firms or sole practitioners as gatekeepers of the financial system, it does not aim to target such employees. In order to facilitate the implementation of this regulation, it is appropriate to clarify the situation of employees such as in-house lawyers, who should not be subject to the requirements of this act when performing their function as employees of obliged entities. (135)

COMP D

Article 4 - Exemptions for certain providers of gambling services

AMs covered 39 (co-rapporteurs), 372 (The Left), 373 (Renew), 374 (EPP), 375 (ECR), 377 (The Left),
AMs fallen: 371 (Renew), 376 (EPP) 379 (EPP)

Recitals: ---

Article 4
Exemptions for certain providers of gambling services

1. With the exception of casinos, ***online gambling platforms (39, 375), gambling services offered on a cross-border basis (372) and sports betting providers***, Member States may decide to exempt, in full or in part, providers of gambling services ***such as state providers or state-owned and private lotteries,*** from the requirements set out in this Regulation on the basis of the proven low risk posed by the nature the principle of proportionality (374) and, where appropriate, the scale of operations of such services, ***following consultation of AMLA (373).***

2. For the purposes of paragraph 1, Member States shall carry out a risk assessment of gambling services assessing:
   (a) money laundering and terrorist financing vulnerabilities and mitigating factors of the gambling services;
   (b) the risks linked to the size of the transactions and payment methods used;
   (c) the geographical area in which the gambling service is administered.
   When carrying out such risk assessments, Member States shall take into account the findings of the risk assessment drawn up by the Commission pursuant to Article 7 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*.

3. Member States***, in cooperation with AMLA,*** shall establish risk-based monitoring activities or take other adequate measures to ensure that the exemptions granted pursuant to this Article are not abused. (377)

COMP E

Article 4a / 5 – Exemptions

AMs covered 378 (Greens), 379 (EPP)
AMs fallen

Recitals 12, 13
AMs covered 141 (Greens)
AMs fallen: 155 (ID)

Article 4a new

Exemptions for certain providers of crowdfunding services

1. ***With the exception of crowdfunding service providers regulated by Regulation (EU) 2020/1503, Member States may decide to exempt certain providers of crowdfunding services, ~~which are used exclusively for public benefit purposes, shall be exempted~~ from the requirements set out in this Regulation on the basis of an individual risk assessment resulting in a ~~the~~ proven low risk posed by the nature and, where appropriate, the scale of operation of such services, provided that all the following conditions are met:***

a) the provider exclusively promotes projects with a public benefit purpose, it does not have as a primary aim the generation of profits and, where a profit is generated, it is invested in the provider for the pursuit of the objectives of the service and not distributed among members, founders or any other private parties, and

b) the crowdfunding service provider implements minimum due diligence requirements in respect of project owners that propose their projects to be funded through the crowdfunding platform in a manner consistent with Article 5 of Regulation (EU) 2020/1503 and all the natural persons involved in the senior management fulfill the criteria set out in Article 6 of the [AMLD VI Proposal]; and

c) all the natural persons involved in the management of the crowdfunding service provider respect fit and proper requirements consistent with the requirements laid down with Article 12 (3) point (b) of Regulation (EU) 2020/1503; and

d) the crowdfunding service provider sets up and maintains arrangements to ensure that project owners accept funding of crowdfunding projects, or any other payment, only by means of a payment service provider in accordance with Directive (EU) 2015/2366;

e) the crowdfunding service provider is established in the Union.

2. ***Member States, in cooperation with AMLA, shall establish risk-based monitoring activities or take other adequate measures to ensure that the exemptions granted pursuant to this Article are not abused.***

Article 5

Exemptions for certain financial activities

1. With the exception of persons engaged in the activity of money remittance as defined in Article 4, point (22) of Directive (EU) 2015/2366, Member States may decide to exempt persons that engage in a financial activity as listed in Annex I, points (2) to (12), (14) and (15), to Directive 2013/36/EU on an occasional or very limited basis where

there is little risk of money laundering or terrorist financing from the requirements set out in this Regulation, provided that all of the following criteria are met:

(a) the financial activity is limited in absolute terms;

(b) the financial activity is limited on a transaction basis;

(c) the financial activity is not the main activity of such persons;

(d) the financial activity is ancillary and directly related to the main activity of such persons;

(e) the main activity of such persons is not an activity referred to in Article 3, point (3)(a) to (d) or (f);

(f) the financial activity is provided only to the customers of the main activity of such persons and is not generally offered to the public.

1a. Member States ~~and third countries~~ shall require ~~all~~ payment service providers within the meaning of Directive (EU) 2015/2366 to ensure that they do not carry out transactions for gambling service providers which do not possess ~~the~~ a licence in the European Union ~~required in the Member State concerned~~. ~~Member States and third countries shall provide obliged entities with white or black lists for that purpose (379)~~

2. For the purposes of paragraph 1, point (a), Member States shall require that the total turnover of the financial activity does not exceed a threshold which shall be sufficiently low. That threshold shall be established at national level, depending on the type of financial activity.

3. For the purposes of paragraph 1, point (b), Member States shall apply a maximum threshold per customer and per single transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked. That maximum threshold shall be established at national level, depending on the type of financial activity. It shall be sufficiently low in order to ensure that the types of transactions in question are an impractical and inefficient method for money laundering or terrorist financing, and shall not exceed EUR 1 000 or the equivalent in national currency.

4. For the purposes of paragraph 1, point (c), Member States shall require that the turnover of the financial activity does not exceed 5 % of the total turnover of the natural or legal person concerned.

5. In assessing the risk of money laundering or terrorist financing for the purposes of this Article, Member States shall pay particular attention to any financial activity which is considered to be particularly likely, by its nature, to be used or abused for the purposes of money laundering or terrorist financing.

6. Member States shall establish risk-based monitoring activities or take other adequate measures to ensure that the exemptions granted pursuant to this Article are not abused.

COMP F

Article 6 – prior notification of exceptions

AMS covered: 380 (EPP), 381 (ECR), 383 (ECR), 385 (ECR), 387 (ECR)
Ams fallen: 382 (ID), 384 (ID), 386 (ID), 388 (ID)

Recital 19

AMs covered: 156 (EPP)
AMs fallen: 7 (co-rapporteurs); 155 (ID)

Article 6
Prior notification of exemptions

1. Member States shall notify the Commission of any exemption that they intend to grant in accordance with Articles 4 and 5 without delay. The notification shall include a ***detailed*** justification based on the relevant risk assessment ***carried out by the Member State*** (381) to sustain the exemption. ***If deemed appropriate, Member States shall provide further evidence to support the exemption. (380)***

2 The Commission shall within two months from the notification referred to in paragraph 2 take one of the following actions:
(a) confirm that the exemption may be granted ***on the basis of the justification given by the Member State****; (383)*
(b) by reasoned decision, declare that the exemption may not be granted.

3. Upon reception of a decision by the Commission pursuant to paragraph 2(a), Member States may adopt the decision granting the exemption. Such decision shall state the reasons on which it is based. Member States shall review such decisions regularly, **but** ***no later than one year after the exemption has been granted for the first time (385)*** and in any case when they update their national risk assessment pursuant to Article 8 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*.

4. By *[3 months from the date of application of this Regulation]*, Member States shall notify to the Commission the exemptions granted pursuant to Article 2(2) and (3) of Directive (EU) 2015/849 in place at the time of the date of application of this Regulation.

5. The Commission shall publish every year in the *Official Journal of the European Union* the list of exemptions granted pursuant to this Article.
The Commission shall publish every year in the Official Journal of the European Union the list of exemptions granted ***and an analytical and factual overview of the exemptions granted pursuant to this Article. (387, ECR)***

Recital 19

(19) It is important that AML/CFT requirements apply in a proportionate manner and that the imposition of any requirement is proportionate to the role that obliged entities can play in the prevention of money laundering and terrorist financing. To this end, it should be possible for Member States in line with the risk-***based*** approach of this Regulation to exempt certain operators from AML/CFT requirements, where the activities they perform present low money laundering and terrorist financing risks and where the activities are limited in nature. To ensure transparent and consistent application of such exemptions across the Union, a mechanism should be put in place allowing the Commission to verify the necessity of the exemptions to be granted. The Commission should also publish such exemptions on a yearly basis in the Official Journal of the European Union. ***(156, EPP).***

COMP G

Article 6a - Minimum requirements regarding citizenship and residence by investment schemes

AMs covered: 40 (Co-rapporteurs), 389 (S&D, Greens), 390 (S&D), 391 (Renew),
AMs fallen: 392 (The Left)

Article 6a
Ban on citizenship by investment and minimum requirements regarding ~~citizenship and~~ residence by investment schemes

1. ***Member States shall not be permitted to enact schemes under national law which allow for citizenship rights in exchange for any kind of investment, including capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget, and without a genuine link with the Member States concerned.***

2. ***A Member State whose national law grants ~~citizenship or~~ residence rights in exchange for any kind of investment, such as capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget, shall ensure that public authorities that process applications for such ~~citizenship and~~ residence rights carry out at least the following measures before a decision is taken:***

(a) require that transactions are carried out by means of a business relationship with an obliged entity established in that Member State;

(b) request and assess information from involved obliged entities about customer due diligence measures carried out;

(c) obtain and record detailed information, substantiated by verified documents, on the identity of the applicant, on any of the applicant's business interests and employment activities in the previous 10 years and on the applicant's source of funds and source of wealth;

(d) require clearance from law enforcement authorities, substantiated by evidence of the absence of any criminal activities on the part of the applicant.

(e) require that applicants are subject to requirements of minimum physical presence and minimum active involvement in the investment, quality of investment, added value and contribution to the economy; The applicant's presence shall be regularly monitored by relevant authorities and non-compliance with physical presence requirements result in the non-granting or withdrawal of ~~citizenship or~~ residence righ**ts.*** (389, 390, 391)

(f) have in place a monitoring mechanism for ex post control of successful applicants' continued compliance with the legal requirements of the schemes.

3. ***Applicants with documented connections with suspicious activities, including close business relations with persons having a criminal record related to money laundering, terrorist financing or predicate offences, or close personal or business connections with individuals subjected to targeted financial sanctions shall not be granted residency rights under such schemes*.** (389, 390)

4. ***Applicants who are nationals of countries listed in Articles 23, 24 or 25 a~~s referred to in Chapter III Section II~~ shall not be granted residency right under such schemes.***

CHAPTER II
INTERNAL POLICIES, CONTROLS AND PROCEDURES OF OBLIGED ENTITIES

SECTION 1
Internal procedures, risk assessment and staff

COMP H

Article 7 - Scope of internal policies, controls and procedures
AMs covered: 41 (co-rapporteurs), 42 (co-rapporteurs), 393 (Greens), 394 (Renew), 395 (S&D), 396 (EPP), 397 (ID), 398 (ID), 399 (ECR), 400 (ECR), 401 (EPP), 403 (S&D/Greens), 404 (NI), 405 (ID), 406 (S&D/Greens)
AMs falling: 402 (ECR)

Recital 20, 21, 23, 23a, 24
AMs covered: 8 (co-rapporteurs), 157 (EPP), 158 (ID), 159 (ID), 160 (RE), 161 (Greens), 162 (Greens/S&D), 163 (Renew), 164 (Greens), 165 (S&D)

Article 7
Scope of internal policies, controls and procedures

1. Obliged entities shall have in place policies, controls and procedures in order to ensure compliance with this Regulation and in particular to:
(a) mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity;
(b) in addition to the obligation to apply targeted financial sanctions, mitigate and manage the risks of non-implementation, ***divergent implementation*** and evasion of ***all targeted financial sanctions including targeted financial sanctions relating to terrorism and terrorism financing and*** proliferation financing-related targeted financial sanctions. (41, 393, 394, 395)

Those policies, controls and procedures shall be proportionate to the nature, ***activity*** and size of the obliged entity. (396, 397, 398) ***Those policies, controls and procedures shall take into account supranational and national risk assessments and the guidelines of FIUs and supervisors, including the results of controls by the competent authorities.*** (399)

2. The policies, controls and procedures referred to in paragraph 1 shall include:
(a) the development of internal policies, controls and procedures, including risk management practices, customer due diligence, reporting, reliance and record-keeping, the monitoring and management of compliance with such policies, controls and procedures, as well as policies in relation to the processing of personal data pursuant to Article 55;
(b) policies, controls and procedures to identify, scrutinise and manage business relationships or occasional transactions that pose a higher or lower money laundering and terrorist financing risk;
(c) an independent audit function to ***assess whether*** the internal policies, controls and procedures referred to in point (a) ***operate effectively***; (400)
(d) the verification, when recruiting and assigning staff to certain tasks and functions and when appointing its agents and distributors, that those persons are of good

repute, ***have the skills and knowledge*** proportionate to the risks associated with the tasks and functions to be performed; (401)

(e) the internal communication of the obliged entity's internal policies, controls and procedures, including to its agents and distributors;

(f) a policy on the training of employees and, where relevant, its agents and distributors with regard to measures in place in the obliged entity to comply with the requirements of this Regulation.

The internal policies, controls and procedures set out in the first subparagraph, points (a) to (f) shall be recorded in writing. The senior management shall approve those policies controls and procedures.

3. The obliged entities shall keep the policies, controls and procedures up to date, and enhance them where weaknesses are identified.

4. By *[2 years after the entry into force of this Regulation]*, AMLA, ***after consulting the European Banking Authority,*** shall ***develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify*** the elements that obliged entities should take into account when deciding on the extent of their internal policies, controls and procedures ***based on their assessed level of risk***. ***They shall also include guidance on how to determine the number of staff to be entrusted with compliance functions as set out in Article 9, taking into account the nature, activity and size of obliged entities and the inherent risks of the sector in which they operate.*** (42, 403, 404, 405)

4a. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 4 of this Article in accordance with Articles 38 to 41 of Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]. (406)

Recital 20

(20) A consistent set of rules on internal systems and controls that applies to all obliged entities operating in the internal market will strengthen AML/CFT compliance and make supervision more effective. In order to ensure adequate mitigation of money laundering and terrorist financing risks, obliged entities should have in place an internal control framework consisting of risk–based policies, controls and procedures and clear division of responsibilities throughout the organisation. In line with the risk-based approach of this Regulation, those policies, controls and procedures should be proportionate to the nature***, activity*** and size of the obliged entity and respond to the risks of money laundering and terrorist financing that the entity faces. (157, 158, 159)

Recital 21

(21) An appropriate risk-based approach requires obliged entities to identify the inherent risks of money laundering and terrorist financing that they face by virtue of their business in order to mitigate them effectively and to ensure that their policies, procedures and internal controls are appropriate to address those inherent risks. In doing so, obliged entities should take into account the characteristics of their customers, the products, services or transactions offered, the countries or geographical areas concerned and the distribution channels used. In light of the evolving nature of risks, such risk assessment should be regularly updated.

Recital 23

(23) The FATF has developed standards for jurisdictions to identify, and assess the risks of potential non-implementation or evasion of the targeted financial sanctions related to proliferation financing, and to take action to mitigate those risks. Those new standards introduced by the FATF today do not substitute nor undermine the existing strict requirements for countries to implement targeted financial sanctions to comply with the relevant United Nations Security Council Regulations relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. Those existing obligations, as implemented at Union level by Council Decisions 2010/413/CFSP[1] and (CFSP) 2016/849[2] as well as by Council Regulations (EU) No 267/2012[3] and (EU) 2017/1509[4], remain strict rule-based obligations binding on all natural and legal persons within the Union. ***The same approach shall apply with regard to other targeted financial sanctions including targeted financial sanctions relating to terrorism and terrorism financing.*** (160, 161)

Recital 23a

(23a) The Union legislation does not include provisions that describe the systems and controls that credit and financial institutions should have to have in place in order to comply with targeted financial sanctions obligations. In its report on the future EU AML/CFT framework, the European Banking Authority (EBA) noted that, in situations where the legislation provides for exemptions from certain AML/CFT requirements, such as in relation to occasional transactions, there is an apparent conflict between risk-based exemptions and the absolute requirement to comply with applicable sanctions regimes, which is an obligation of result. The EBA also found that there are different interpretations across Member States on the obligations on payment service providers to screen the payer or the payee against sanctions lists. This situation could create regulatory arbitrage and gaps which could weaken the Union targeted financial sanctions regime. It is therefore necessary to establish common standards on the measures that credit and financial institutions should take in order to comply with their financial sanctions obligations. (162)

Recital 24

(24) In order to reflect the latest developments at international level, a requirement has been introduced by this Regulation to identify, understand, manage and mitigate risks of potential non-implementation, ***divergent implementation*** or evasion of ***all targeted financial sanctions including targeted financial sanctions relating to terrorism and terrorism financing and*** proliferation financing-related targeted financial sanctions at obliged entity level. (8, 163, 164, 165)

COMP I

Article 8 – Risk assessment

AMs covered: 407 (Greens), 408 (Renew), 409 (EPP), 410 (ID), 411 (ID), 412 (Greens), 413 (The Left), 414 (Greens), 415 (Greens), 416 (Greens), 417 (Greens)

AMs falling: 418 (EPP)

Article 8
Risk assessment

1. Obliged entities shall take appropriate measures, proportionate to their nature, ***activity*** and size, to identify and assess the risks of money laundering and terrorist financing to which they are exposed, as well as the risks of non-implementation and evasion of ***all targeted financial sanctions including targeted financial sanctions relating to terrorism and terrorism financing and*** proliferation financing-related targeted financial sanctions, taking into account ***at least the following***: (407, 408, 409, 410, 411)

(a) the risk variables set out in Annex I and the risk factors set out in Annexes II and III;

(b) the findings of the supra-national risk assessment drawn up by the Commission pursuant to Article 7 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*;

(c) the findings of the national risk assessments carried out by the Member States pursuant to Article 8 of *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*.

(ca) relevant guidelines, recommendations and opinions issued by AMLA in accordance with Articles 43 and 44 of Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]; (412)

(cb) the conclusions drawn from past infringements of AML/CFT rules by the obliged entity in question or any connection of the obliged entity in question with a case of money laundering or terrorist financing; (413)

(cc) information from Financial Intelligence Units (FIUs) and law enforcement agencies; (414)

(cd) information obtained as part of the initial customer due diligence process and ongoing monitoring; (415)

(ce) own knowledge and professional experience. (416)

1a. Obliged entities may, depending on the level of risk identified and the principle of proportionality, consider at their sole discretion additional sources of information, including:

(a) information from organisations of obliged entities on typologies and on emerging risks;

(b) information from civil society organisations, including corruption perception indices and other country reports;

(c) information from international standard-setting bodies such as mutual evaluation reports or other reports and reviews;

(d) information from credible and reliable open sources and the media;

(e) information from credible and reliable commercial organisations, such as risk reports;

(f) information from statistic organisations and the academia. (417)

2. The risk assessment drawn up by the obliged entity pursuant to paragraph 1 shall be documented, kept up-to-date and made available to supervisors.

3. Supervisors may decide that individual documented risk assessments are not required where the specific risks inherent in the sector are clear and understood.

Recital 22

(22) It is appropriate to take account of the characteristics and needs of smaller obliged entities, and to ensure treatment which is appropriate to their specific needs, and the nature of the business. This may include exempting certain obliged entities from performing a risk assessment where the risks involved in the sector in which the entity operates are well understood.

COMP J

Article 9 – Compliance functions
AMs covered: 43 (co-rapporteurs), 44 (co-rapporteurs), 420 (EPP), 421 (EPP), 422 (ECR), 423 (Renew), 424 (Greens), 425 (EPP), 426 (ECR), 427 (ECR), 428 (EPP), 429 (EPP), 430 (ECR), 431 (Renew), 432 (Greens), 433 (EPP), 435 (EPP), 436 (Greens), 437 (EPP), 438 (Renew), 440 (The Left)
AMs falling: 419 (The Left), 434 (ECR), 439 (S&D)

Article 10 - Awareness of requirements (no AMs)

Recitals 25, 26, 27
AMs covered: 168 (Renew)

Article 9

Compliance functions

1. Obliged entities shall appoint one executive member of their ***management*** body ***in its management function*** who shall be responsible for the implementation ***and monitoring*** of measures to ensure compliance with this Regulation ('compliance manager'). Where the entity has no ***management*** body, the function should be performed by a member of its senior management. ***This paragraph is without prejudice to national provisions on joint civil or criminal liability of management bodies.*** (43, 421, 422, 423, 424, 425, 426)

2. The compliance manager shall ***ensure that*** the obliged entity's policies, controls and procedures ***are fully implemented*** and ***shall receive*** information on significant or material weaknesses in such policies, controls and procedures. The compliance manager shall regularly report on those matters to the ***management*** body. For parent undertakings, that person shall also be responsible for overseeing group-wide policies, controls and procedures. (427, 428, 429, 430, 431, 432)

3. Obliged entities shall have a compliance officer, to be appointed by the ***management*** body ***in its management function***, who shall be in charge of the day-to-day operation of the obliged entity's anti-money laundering and countering the financing of terrorism (AML/CFT) policies ***including being a contact point for competent authorities.*** That person shall also be responsible for reporting suspicious transactions to the Financial

Intelligence Unit (FIU) in accordance with Article 50(6). ***That person shall be independent in its function and responsibilities***. (433, 435, 436, 437, 438, 440).

In the case of obliged entities subject to checks on their senior management or beneficial owners pursuant to Article 6 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]* or under other Union acts, compliance officers shall be subject to verification that they comply with those requirements.

An obliged entity that is part of a group may appoint as its compliance officer an individual who performs that function in another entity within that group, ***provided that that entity is established in the same Member State in which the obliged entity is established***. (44)

3a. ***A compliance officer shall not be penalised in any way in the context of employment for carrying out the duties. A compliance officer shall not be dismissed prior to the end of the term of appointment unless facts emerge that make it unreasonable for the obliged entity concerned to retain the person. Obliged entities shall notify supervisory authorities of the dismissal of compliance officers and the reason thereof.*** (440)

3b. ***'Where verification of the suitability of a compliance manager or compliance officer is performed by a non-AML/CFT authority, the authority performing the suitability verification shall, without undue delay, inform the supervisor in the Member State where the obliged entity concerned is established as to receipt of the application and as to the date by which the decision on the suitability verification needs to be adopted. The supervisor shall, in cooperation with other competent authorities as appropriate, provide the non-AML/CFT authority performing the suitability verification with any input necessary within its supervisory competence, within an appropriate deadline taking into account the date by which the decision on the suitability verification needs to be adopted.***

The input referred to in the first subparagraph shall consist of an assessment as to whether the knowledge, skills and experience of the appointee suffice for the performance of the function of compliance manager or compliance officer for which the appointee was nominated, which shall become a part of the decision of the authority performing the suitability verification.

Where the supervisor concludes, in its input, that the appointee does not have adequate knowledge, skills and experience to perform the tasks set out in the first and second subparagraphs in respect of the function of a compliance manager, or the third subparagraph in respect of the function of a compliance officer, the authority performing the suitability verification shall not issue a decision that would allow the appointee to perform those tasks.

~~***This shall not prevent the non AML/CFT authority performing the suitability verification from issuing a positive decision with respect to any other function for which the appointee was nominated. If the relevant supervisor does not provide, by the deadline referred to in the first subparagraph, the assessment of whether the knowledge, skills and experience of the appointee suffice for the performance of the function of compliance manager or compliance officer for which the appointee was nominated, the non AML/CFT authority performing the suitability verification shall consider the appointee to have the necessary knowledge, skills and experience for the performance of the respective function.***~~

The procedure for identifying the relevant supervisor, specific deadlines for providing the input referred to in this paragraph and other technical modalities of cooperation of supervisors with authorities performing the suitability verification, including the ECB acting in accordance with Regulation (EU) 1024/2013 and other authorities thereunder, shall be set out in the guidelines contained in Article 52 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final].'

4. Obliged entities shall provide the compliance functions with adequate resources, including staff and technology, in proportion to the size, nature, ***activity*** and risks of the obliged entity for the implementation of compliance functions, and shall ensure that ***the access to all information, data, records and systems that might be of relevance in connection with the performance of their duties and*** the powers to propose any measures necessary to ensure the effectiveness of the obliged entity's internal policies, controls and procedures are granted to the persons responsible for those functions. (440)

5. The compliance manager shall submit once a year, or more frequently where appropriate, to the ***management*** body a report on the implementation of the obliged entity's internal policies, controls and procedures, and shall keep the management body informed of the outcome of any reviews. The ***management*** body shall take the necessary actions to remedy any deficiencies identified in a timely manner.

6. Where the size of the obliged entity justifies it, the functions referred to in paragraphs 1 and 3 may be performed by the same natural person. ***The compliance officer may cumulate functions referred to in paragraphs 1 and 3 with other functions.***
Where the obliged entity is a natural person or a legal person whose activities are performed by one natural person only, that person shall be responsible for performing the tasks under this Article.

Article 10
Awareness of requirements

Obliged entities shall take measures to ensure that their employees whose function so requires, as well as their agents and distributors are aware of the requirements arising from this Regulation and of the internal policies, controls and procedures in place in the obliged entity, including in relation to the processing of personal data for the purposes of this Regulation.
The measures referred to in the first subparagraph shall include the participation of employees in specific, ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases. Such training programmes shall be duly documented.

Recital 25

(25) It is important that obliged entities take all measures at the level of their management to implement internal policies, controls and procedures and to implement AML/CFT requirements. While a person at management level should be identified as being responsible for implementing the obliged entity's policies, controls and procedures, the

responsibility for the compliance with AML/CFT requirements should rest ultimately with the ***management*** body of the entity. Tasks pertaining to the day-to-day implementation of the obliged entity's AML/CFT policies, controls and procedures should be entrusted to a compliance officer. (168)

Recital 26

(26) For effective implementation of AML/CFT measures, it is also vital that the employees of obliged entities, as well as their agents and distributors, who have a role in their implementation understand the requirements and the internal policies, controls and procedures in place in the entity. Obliged entities should put in place measures, including training programmes, to this effect.

COMP K

Article 11 - Integrity of employees
AMs covered: 45 (co-rapporteurs), 441 (EPP), 443 (The Left), 444 (EPP), 445 (ID), 446 (ID), 447 (S&D), 448 (The Left), 449 (The Left)
AMs falling: 442 (EPP)

Recital 27 – no AMs

Article 11
Integrity of employees

1. Any employee of an obliged entity entrusted with tasks related to the obliged entity's compliance with this Regulation and Regulation *[please insert reference – proposal for a recast of Regulation (EU) 2015/847 - COM/2021/422 final]* shall undergo an assessment approved by the compliance officer of:
(a) individual skills, knowledge and expertise to carry out their functions effectively;
(b) good repute, honesty and integrity.

2. Employees entrusted with tasks related to the obliged entity's compliance with this Regulation shall inform the compliance officer of any close private or professional relationship established with the obliged entity's customers or prospective customers, ***who have indicated their intention to be legally bound by a contract in their statements or conduct as they were reasonably understood by the other party,*** and shall be prevented from undertaking any tasks related to the obliged entity's compliance in relation to those customers. (441)

2a. Obliged entities shall have in place adequate procedures to ensure that responsibility for a business relationship changes from one employee to another at appropriate intervals. Where the size of the obliged entity or the need for special qualifications does not allow for the establishment of such a procedure, the compliance officer shall carry out, in a risk-based manner, a special examination of the affected business relationships at appropriate intervals. (443)

3. Obliged entities shall have in place appropriate procedures for their employees, or persons in a comparable position, to report breaches of this Regulation internally

through a specific, independent and anonymous channel, proportionate to the nature, ***activity*** and size of the obliged entity concerned. (444, 445, 446)

Obliged entities shall take measures to ensure that employees, managers**,** agents, ***and other persons referred to in Article 4 of Directive (EU) 2019/1937 of the European Parliament and of the Council***[5] who report breaches pursuant to the first subparagraph are protected ***against any ~~from being exposed to threats, hostile action, discrimination, any other unfair treatment and retaliation in accordance with~~ as laid down in that Directive and other applicable legal acts*** (45, 447, 448, 449)

4. This Article shall not apply to obliged entities that are sole traders.

Recital 27

(27) Individuals entrusted with tasks related to an obliged entity's compliance with AML/CFT requirements should undergo assessment of their skills, knowledge, expertise, integrity and conduct. Performance by employees of tasks related to the obliged entity's compliance with the AML/CFT framework in relation to customers with whom they have a close private or professional relationship can lead to conflicts of interests and undermine the integrity of the system. Therefore, employees in such situations should be prevented from performing any tasks related to the obliged entity's compliance with the AML/CFT framework in relation to such customers.

COMP L

Article 12 - Situation of specific employees – no AMs

Article 12a - Minimum requirements for sole traders, single operators or microenterprises
AMs covered: 46 (co-rapporteurs)

Recital 27a
AMs covered: 9 (co-rapporteurs), 169 (EPP)

Article 12
Situation of specific employees

Where a natural person falling within any of the categories listed in Article 3, point (3) performs professional activities as an employee of a legal person, the requirements laid down in this Section shall apply to that legal person rather than to the natural person.

Article 12a
Minimum requirements for sole traders, single operators or microenterprises

1. By ... [2 years from the date of entry into force of this Regulation], AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption concerning minimum requirements and standards for compliance with this Chapter by obliged entities which are sole traders, single operators or microenterprises. In particular, AMLA shall develop requirements and standards in relation to execution of compliance functions.

When developing the draft regulatory technical standards referred to in the first subparagraph, AMLA shall take due account of the inherent levels of risks of the business models of the different types of obliged entities in order to ensure that the requirements and standards for compliance are proportionate to the risks identified.

2. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 1 of this Article in accordance with Articles 38 to 41 of [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]. (46)

Recital 27a

(27a) Given that AML/CFT requirements are applicable to a wide range of obliged entities in both nature and size, AMLA should have the task of developing draft regulatory technical standards concerning minimum requirements and standards by obliged entities which are sole traders, single operators or microenterprises taking due account of the principle of proportionality and alleviation of administrative and financial burden. (9, 169)

SECTION 2
Provisions applying to groups

COMP M
Article 13 - Group-wide requirements
AMs covered: 47 (co-rapporteurs), 450 (S&D/Greens), 451 (S&D), 452 (S&D), 453 (EPP), 454 (ID)

Recitals 28, 29
AMs covered: 170 (EPP), 172 (EPP)
AMs falling: 171 (ID), 173 (ID)

Article 13
Group-wide requirements

1. ***Each*** parent undertaking ***established in the Union*** shall ***put in place group-wide policies, controls and procedures to comply with this Regulation and shall ensure that*** the requirements on internal procedures, risk assessment and staff referred to in Section 1 of this Chapter apply in all branches and subsidiaries of the group in the Member States***. Where a*** parent undertaking is established in the Union***, it shall ensure that those requirements also apply in all branches and subsidiaries of the group*** in third countries. ***To this end, a parent undertaking shall perform a group-wide risk assessment, taking into account the risks identified by all branches and subsidiaries of the group, and use it to establish and implement group-wide policies, controls and procedures.*** The group-wide policies, controls and procedures shall also include data protection policies and policies, controls and procedures for sharing information within the group for AML/CFT purposes. ***Obliged entities that are part of a group shall implement the aforementioned group-wide policies, controls and procedures, taking into account their specificities and risks to which they are exposed.*** (47, 450)

2. The policies, controls and procedures pertaining to the sharing of information referred to in paragraph 1 shall require obliged entities within the group to exchange information when such sharing is relevant for preventing money laundering and terrorist financing**,**

including customer due diligence and risk management. The sharing of information within the group shall cover in particular the identity and characteristics of the customer, its beneficial owners or the person on behalf of whom the customer acts, the nature and purpose of the business relationship and ***of the transactions, as well as, where applicable, the analysis of atypical transactions and*** the suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to FIU pursuant to Article 50, unless otherwise instructed by the FIU.

The group-wide policies, procedures and controls shall require that entities within a group which are not obliged entities according to Article 3 of this Regulation to provide relevant information to obliged entities within the same group for them to comply with requirements set out in this Regulation.

Groups shall put in place group-wide policies, controls and procedures to ensure that the information exchanged pursuant to the first ***and second*** subparagraph is subject to sufficient guarantees in terms of confidentiality, data protection and use of the information, including to prevent its disclosure. (451, 452)

2a. Entities within the same group shall be entitled to use the information received as up-to-date information for the intra-group business relationship, provided that:

(a) the information or documents are provided by another entity within the same group;

(b) the receiving entity within the same group and the providing entity within the same group are not aware that the information is no longer up to date. (453)

3. By *[2 years from the entry into force of this Regulation]*, AMLA***, after consulting the European Banking Authority,*** shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify the minimum requirements of group-wide policies, including minimum standards for information sharing within the group, the role and responsibilities of parent undertakings that are not themselves obliged entities with respect to ensuring group-wide compliance with AML/CFT requirements and the conditions under which the provisions of this Article apply to entities that are part of structures which share common ownership, management or compliance control, including networks or partnerships. (454)

4. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 of this Article in accordance with Articles 38 to 41 of Regulation *[please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]*.

Recitals 28-29

(28) The consistent implementation of group-wide AML/CFT policies and procedures is key to the robust and effective management of money laundering and terrorist financing risks within the group. To this end, group-wide policies, controls and procedures should be adopted and implemented by the parent undertaking. Obliged entities within the group should be required to exchange information when such sharing is relevant for preventing money laundering and terrorist financing. Information sharing should be subject to sufficient guarantees in terms of confidentiality, data protection and use of information. AMLA should have the task of drawing up draft regulatory standards specifying the minimum requirements of group-wide procedures and policies, including minimum standards for information sharing within the group and the role and responsibilities of

parent undertakings that are not themselves obliged entities, ***and taking into account the principle of proportionality***. (170)

(29) In addition to groups, other structures exist, such as networks or partnerships, in which obliged entities might share common ownership, management and compliance controls. To ensure a level playing field across the sectors whilst avoiding overburdening it, AMLA should identify those situations where similar group-wide policies should apply to those structures, ***taking into account the principle of proportionality***. (172)

COMP N
Article 14 - Branches and subsidiaries in third countries
AMs covered: 455 (S&D), 456 (S&D), 457 (NI)
AMs falling: 458 (ID)

Recital 30
AMs covered: 174 (EPP)
AMs falling: 175 (ID)

Article 14
Branches and subsidiaries in third countries

1. Where branches or subsidiaries of obliged entities are located in third countries where the minimum AML/CFT requirements are less strict than those set out in this Regulation, the ***parent undertaking*** shall ensure that those branches or subsidiaries comply with the requirements laid down in this Regulation, including requirements concerning data protection, or equivalent. (455)

2. Where the law of a third country does not permit compliance with the requirements laid down in this Regulation, ***the parent undertaking*** shall take additional measures to ensure that branches and subsidiaries in that third country effectively handle the risk of money laundering or terrorist financing, and shall inform the supervisors of their home Member State ***of those additional measures***. Where the supervisors of the home Member State consider that the additional measures are not sufficient, they shall exercise additional supervisory actions, including requiring the group not to establish any business relationship, to terminate existing ones or not to undertake transactions, or to close down its operations in the third country.(456)

3. By *[2 years after the date of entry into force of this Regulation]*, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify the type of additional measures referred to in paragraph 2, including the minimum action to be taken by obliged entities where the law of a third country does not permit the implementation of the measures required under Article 13 and the additional supervisory actions required in such cases. ***The draft regulatory technical standards shall include a list of third countries where the minimum AML/CFT requirement are deemed equivalent to those laid down in this Regulation. This list shall be regularly updated.*** (457)

4. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 of this Article in accordance

with Articles 38 to 41 of Regulation *[please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]*.

Recital 30

(30) There are circumstances where branches and subsidiaries of obliged entities are located in third countries where the minimum AML/CFT requirements, including data protection obligations, are less strict than the Union AML/CFT framework. In such situations, and in order to fully prevent the use of the Union financial system for the purposes of money laundering and terrorist financing and to ensure the highest standard of protection for personal data of Union citizens, those branches and subsidiaries should comply with AML/CFT requirements laid down at Union level. Where the law of a third country does not permit compliance with those requirements, for example because of limitations to the group's ability to access, process or exchange information due to an insufficient level of data protection or banking secrecy law in the third country, obliged entities should take additional measures to ensure the branches and subsidiaries located in that country effectively handle the risks. AMLA should be tasked with developing draft technical standards specifying the type of such additional measures, ***taking into account the principle of proportionality***. (174)

CHAPTER III

CUSTOMER DUE DILIGENCE

SECTION 1

General provisions

COMP O

Article 15, 16 - Application of customer due diligence / Customer due diligence measures

AMs covered: 48 (co-rapporteurs), 49 (co-rapporteurs), 50 (co-rapporteurs), 51 (co-rapporteurs), 52 (co-rapporteurs), 468 (The Left), 472 (S&D), 473 (S&D), 483 (The Left), 484 (S&D, Greens, Renew), 485 (Renew), 486 (NI), 490 (S&D, Renew, Greens), 491 (S&D), 492 (The Left), 494 (S&D, Renew, Greens)
AMs falling: 459 (Renew), 460 (ECR), 461 (ID), 462 (Renew), 463 (Renew), 464 (NI), 465 (Renew), 466 (Renew), 467 (EPP), 469 (ECR), 470 (EPP), 471 (ID), 474 (ID), 475 (EPP), 477 (Renew, EPP), 478 (ID), 479 (EPP), 481 (EPP), 482 (EPP), 489 (ECR), 493 (ID),

Recitals 33, 34, 34a
AMs covered: 178 (Renew), 181 (EPP), 182 (EPP),
AMs falling: 177 (EPP), 179 (ID), 180 (Renew), 183 (EPP)

Article 15

Application of customer due diligence

1. Obliged entities shall apply customer due diligence measures in any of the following circumstances:

   (a) when establishing a business relationship;

   (b) when involved in or carrying out an occasional transaction that amounts to EUR 10 000 or more, or the equivalent in national currency, whether that transaction is carried out in a single operation or through linked transactions, or a lower threshold laid down pursuant to paragraph 5;

   (c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

   (d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

   ~~By way of derogation from the first subparagraph, point (b), obliged entities shall apply customer due diligence measures when involved in or carrying out an occasional transaction involving crypto-assets that amounts to EUR 1 000 or more, or the equivalent in national currency, whether the transaction is carried out in a single operation or through linked transactions.~~ ~~(48)~~

2. In addition to the circumstances referred to in paragraph 1, credit and financial institutions ***~~and crypto-asset service providers~~*** shall apply customer due diligence when ***~~either~~*** initiating or executing an occasional transaction that constitutes a transfer of funds as defined in Article 3, point (9) of Regulation *[please insert reference – proposal for a recast of Regulation (EU) 2015/847 - COM/2021/422 final]*, ***~~or a transfer of~~***

~~*crypto-assets as defined in Article 3, point (10) of that Regulation, exceeding*~~ ***that amounts to*** EUR 1 000 ***or more*** **(49)** or the equivalent in national currency.

Credit and financial institutions ~~***obliged entities***~~ ***shall also apply customer due diligence measures when involved in or carrying out an occasional transaction involving crypto-assets that amounts to EUR 1 000 or more, or the equivalent in national currency, whether the transaction is carried out in a single operation or through linked transactions.*** (48)

3. Providers of gambling services shall apply customer due diligence upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to at least EUR 2 000 ~~***500***~~ or the equivalent in national currency, ***or, in the case of online gambling services, transactions amounting to at least EUR*** ~~***500***~~ ***1000 or the equivalent in national currency,*** **(468)** whether the transaction is carried out in a single operation or in linked transactions.

3a. By way of derogation from paragraph 1, based on an appropriate risk assessment which demonstrates a low risk, a supervisor ~~***Member State***~~ ***may allow obliged entities not to apply certain customer due diligence measures with respect to s***~~***pecific payment instruments***~~ ***electronic money that can be used only in a limited way, where all of the following risk-mitigating conditions are met:***

a) the maximum amount stored does not exceed EUR 150;

b) the instruments can be used exclusively to purchase, either in store or online, goods or services in a single Member State, from the issuer~~***r, either in the premises of the issuer or online,***~~ ***or within a*** ~~***limited***~~ ***network of service providers under direct commercial agreement with a professional issuer. The instruments should not be linked to a bank account, should not allow for balance top-ups and should not be exchangeable for cash.*** (469, 475, 477, 478, 479)

4. In the case of credit institutions, the performance of customer due diligence shall also take place, ***where necessary,*** **(50)** under the oversight of supervisors, at the moment that the institution has been determined failing or likely to fail pursuant to Article 32(1) of Directive 2014/59/EU of the European Parliament and of the Council[12] or when the deposits are unavailable in accordance with Article 2(1)(8) of Directive 2014/49/EU of the European Parliament and of the Council[13]. Supervisors shall decide on the intensity and scope of such customer due diligence measures having regard to the specific circumstances of the credit institution.

5. By *[2 years from the date of entry into force of this Regulation]*, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify:

   (a) the obliged entities, sectors or transactions that are associated with higher money laundering and terrorist financing risk and which shall comply with thresholds lower than those set in paragraph 1 point (b);

---

12 Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council Text with EEA relevance (OJ L 173, 12.6.2014, p. 190).

13 Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes Text with EEA relevance (OJ L 173, 12.6.2014, p. 149).

(ba) the criteria to be taken into account for identifying occasional transactions, including those involving crypto-assets; (51, 472)

(bb) the criteria to be taken into account to identify business relationships; (473)

(b) the related occasional transaction thresholds;

(c) the criteria to identify linked transactions.

When developing the draft regulatory technical standards referred to in the first sub-paragraph, AMLA shall take due account of the following:

(a) the inherent levels of risks of the business models of the different types of obliged entities;

(b) the supra-national risk assessment developed by the Commission pursuant to Article 7 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*.

6. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 5 of this Article in accordance with Articles 38 to 41 of *[please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]*.

Article 16

Customer due diligence measures

1. For the purpose of conducting customer due diligence, obliged entities shall apply all of the following measures:

(a) identify the customer and verify the customer's identity;

(b) identify the beneficial owner(s) pursuant to Articles 42 and 43 and verify their identity so that the obliged entity is satisfied that it knows who the beneficial owner is and that it understands the ownership and control structure of the customer;

(ba) identify and record the identity of nominee shareholders and nominee directors of a corporate or other legal entity and identify their status as such, where applicable; (52, 483, 486)

(c) assess and, as appropriate, obtain information on the purpose and intended nature of the business relationship;

(ca) ~~obtain and assess information on~~ verify whether the customer or the beneficial owner are subject to targeted financial sanctions relating to terrorism and terrorism financing, proliferation financing and to other applicable Union targeted financial sanctions; (484, 485)

(d) conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds.

When applying the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and shall identify and verify the identity of that person in accordance with Article 18.

2. Obliged entities shall determine the extent of the measures referred to in paragraph 1 on the basis of an individual analysis of the risks of money laundering and terrorist financing having regard to the specific characteristics of the client and of the business relationship or occasional transaction, and taking into account the risk assessment by the obliged entity pursuant to Article 8 and the money laundering and terrorist financing variables set out in Annex I as well as the risk factors set out in Annexes II and III.

Where obliged entities identify an increased risk of money laundering or terrorist financing they shall take enhanced due diligence measures pursuant to Section 4 of this Chapter. Where situations of lower risk are identified, obliged entities may apply simplified due diligence measures pursuant to Section 3 of this Chapter.

2a. Without prejudice to any other measures required to comply with the obligation to apply targeted financial sanctions, for credit and financial institutions ~~and crypto-asset service providers~~ the measures laid down in paragraph 1 (ca) shall include the regular screening of the customer's identity as well as the beneficial owner's identity against the relevant sanctions lists of designated persons in order to verify that the customer is not a designated individual, entity or group subject to targeted financial sanctions. (490)

3. By *[2 years after the date of application of this Regulation]*, AMLA, ***after consulting Europol and the European Supervisory Authorities (491, 492)***, shall issue guidelines on***:***

a) the risk variables and risk factors to be taken into account by obliged entities when entering into business relationships or carrying out occasional transactions;

b) measures to be applied by obliged entities for assessing whether the customer or the beneficial owner is subject to targeted financial sanctions including how to identify entities controlled by persons subject to targeted financial sanctions.(494)

4. Obliged entities shall at all times be able to demonstrate to their supervisors that the measures taken are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

Recital 33

(33) Obliged entities should not be required to apply due diligence measures on customers carrying out occasional or linked transactions below a certain value, unless there is suspicion of money laundering or terrorist financing. Whereas the EUR 10 000 threshold applies to most occasional transactions, obliged entities which operate in sectors or carry out transactions that present a higher risk of money laundering and terrorist financing should be required to apply customer due diligence for transactions with lower thresholds, and ***should, in particular, verify whether those thresholds are met within linked transactions with lower amounts. (178)*** To identify the sectors or transactions as well as the adequate thresholds for those sectors or transactions, AMLA should develop dedicated draft regulatory technical standards.

Recital 34

(34) Some business models are based on the obliged entity having a business relationship with a merchant for offering payment initiation services through which the merchant gets paid for the provision of goods or services, and not with the merchant's customer, who authorises the payment initiation service to initiate ***a single or one-off transaction or several transactions*** to the merchant. In such a business model, the obliged entity's customer for the purpose of AML/CFT rules is the merchant, and not the merchant's customer. Therefore, customer due diligence obligations should be applied by the obliged entity ***only (182)*** vis-a-vis the merchant. ***If the same obliged entity also provides payment services to the merchant, which brings it into the possession of funds, then the obliged entity's customer is also the merchant as regards the combined offering of payment initiation services, account information services and payment services. (181)***

Article 17, 18 - Inability to comply with the requirement to apply customer due diligence measures/ Identification and verification of the customer's identity

AMs covered: 53 (co-rapporteurs), 54 (co-rapporteurs), 55 (co-rapporteurs), 56 (co-rapporteurs), 57 (co-rapporteurs), 58 (co-rapporteurs), 59 (co-rapporteurs), 60 (co-rapporteurs), 480 (ECR), 487 (ECR), 497 (S&D), 498 (Renew), 499 (The Left), 503 (EPP), 504 (EPP), 505 (The Left), 506 (EPP), 507 (EPP), 508 (EPP), 509 (The Left), 514 (Greens), 516 (EPP), 520 (EPP), 521(EPP), 522 (EPP), 523 (EPP), 525 (EPP), 527 (EPP), 528 (ID), 529 (EPP), 530 (S&D), 531 (EPP), 532 (S&D), 533 (EPP), 534 (ECR), 535 (EPP), 536 (S&D), 537 (EPP), 538 (EPP), 539 (EPP), 541 (EPP)

AMs falling: 496 (EPP), 500 (EPP), 501 (ECR), 502 (EPP), 510 (EPP), 511 (ECR), 512 (The Left), 513 (ECR), 515 (The Left), 517 (EPP), 518 (EPP), 519 (ECR), 524 (ECR), 526 (ID), 540 (EPP), 542 (EPP)

Recitals 32a, 36, 40, 41

AMs covered: 135 (EPP), 136 (ECR), 137 (EPP), 138 (S&D), ~~176 (Renew)~~

AMs falling: 184 (EPP), 185 (ID), 186 (ID)

Article 17

Inability to comply with the requirement to apply customer due diligence measures

1. Where an obliged entity is unable to comply with the customer due diligence measures laid down in Article 16(1), it shall ~~***refrain from***~~ ***not*** carry~~***ing***~~ **(497, 498)** out a transaction or establish~~***ing***~~ a business relationship, and shall terminate the business relationship and consider filing a suspicious transaction report to the FIU in relation to the customer in accordance with Article 50. ***Where there is a suspicion of money laundering or terrorist financing, the obliged entity shall file a suspicious transaction report to the FIU. (497, 498, 499)***

1a. ~~***The first subparagraph***~~ ***Paragraph 1*** shall not apply to notaries, lawyers and other independent legal professionals, auditors, external accountants and tax advisors, to the strict extent that those persons

a) ascertain the legal position of their client, ***except where the legal advice~~,~~ ~~including in relation to tax matters,~~ is provided for the purpose of money laundering~~, its predicate offences~~ or terrorist financing, or where those persons know or ~~have a well-grounded suspicion~~ ~~suspect~~ have a well grounded supicion that the client is seeking legal advice~~, including on tax matters,~~ for the purposes of money laundering~~, its predicate offences,~~ or terrorist financing or for the purposes of applying for residence rights or citizenship through investment schemes, and the advice is not sought in relation to judicial proceedings; or***

b) perform the task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings. **(53, 54, 55, 56, 57)**

2. Where obliged entities either accept or refuse to enter in a business relationship, they shall keep record of the actions taken in order to comply with the requirement to apply customer due diligence measures, including records of the decisions taken and the relevant supporting documents. Documents, data or information held by the obliged entity shall be updated whenever the customer due diligence is reviewed pursuant to Article 21.

~~2a. *Member States may adopt or maintain with regard to specific transactions that involve a particular high risk to be used for money laundering or terrorist financing additional reporting obligations customer due diligence obligations for the persons mentioned in paragraph 1a to which the exemption from the requirements laid down in that paragraph may not apply.*~~

Recital 9

(9) ***This Regulation does not aim to regulate independent legal and tax professions, which take different forms across Member States, nor to interfere with the essence of the role of ~~defence~~ these professionals in the administration of justice and the rule of law, which underlays the legal professional privilege. However, independent legal professionals, auditors, external accountants and tax advisors, who, in some Member States, are entitled to defend or represent a client in the context of judicial proceedings or to ascertain a client's legal position, also perform activities that are remote from the role of defence. Therefore, they should be subject to this Regulation when participating in financial or corporate transactions, including when providing tax advice or advice relating to citizenship or residence by investment schemes, where there is the risk of the services provided by those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing. There should, however, be exemptions from any obligation to report information obtained before, during or after judicial proceedings which should be covered by the legal privilege. Exemptions should also be provided for activities performed in the course of ascertaining the legal position of a client, which should also be covered by the legal privilege to the strict extent that such activities aim at establishing the rights and obligations of clients, in contrast to non-legal advice ~~and do not involve economic advice of any type~~. Therefore, legal advice should remain subject to the obligation of professional secrecy, except where the legal professional is taking part in money laundering or terrorist financing, where the legal advice, including in relation to tax matters or citizenship or residence by investment schemes, is provided for the purpose of money laundering ~~its predicate offences~~ or terrorist financing, or where the legal***

professional knows or suspects, on the basis of factual and objective circumstances, ~~has a well-grounded suspicion~~ that the client is seeking legal advice, ~~including on tax matters~~, for the purposes of money laundering, ~~its predicate offences, or~~ terrorist financing or or for the purposes of applying for residence rights or citizenship through investment schemes. Member States may adopt or maintain with regard to specific transactions that involve a particular high risk to be used for money laundering or terrorist financing ~~additional~~ customer due diligence obligations for the persons mentioned in paragraph 1a ~~to which the exemption from the requirements laid down in that paragraph may not apply~~ (135, 136, 137, 138)

Article 18

Identification and verification of the customer's identity ***and the beneficial owner's identity***

1. With the exception of cases of lower risk to which measures under Section 3 apply and irrespective of the application of additional measures in cases of higher risk under Section 4 obliged entities shall obtain at least the following information in order to identify the customer and the person acting on their behalf:

   (a) for a natural person:

   (i) the forename and surname;

   (ii) place and date of birth;

   (iii) nationality or nationalities, or statelessness and refugee or subsidiary protection status where applicable, and the national identification number, where applicable;

   (iv) the usual place of residence or, if there is no fixed residential address ~~***with legitimate residence***~~ **(505)** in the Union, the postal address at which the natural person can be reached and, where ***relevant for the purposes of customer due diligence, ~~possible~~***, **(503, 504)** the occupation, profession, or employment status and the tax identification number;

   (b) for a legal entity:

   (i) legal form and name of the legal entity;

   (ii) address of the registered or official office and, if different, the principal place of business, and the country of incorporation;

   (iii) the names of the legal representatives ~~***and the Legal Entity Identifier***~~ as well as, where ~~***applicable***~~ available, **(509)** the registration number, the tax identification number and the Legal Entity Identifier. ***On a risk sensitive basis,*** obliged entities shall also ***consider the need to verify*** (***506, 507, 508)*** that the legal entity has activities on the basis of accounting documents for the latest financial year or other relevant information;

   (iiia) for a legal entity established in more than one jurisdiction, the Legal Entity Identifier;

   (c) for a trustee of an express trust or a person holding an equivalent position in a similar legal arrangement:

(i) the information referred to in Article 44(1), points (a) and (b), and in point (b) of this paragraph for all the persons identified as beneficial owners;

(ii) the address of residence of the trustee(s) or person(s) holding an equivalent position in a similar legal arrangement, and the powers that regulate and bind the legal arrangements, as well as, where available, the tax identification number and the Legal Entity Identifier;

(d) for other organisations that have legal capacity under national law:

(i) name, address of the registered office or equivalent;

(ii) names of the persons empowered to represent the organisation as well as, where applicable, legal form, tax identification number, register number, Legal Entity Identifier and deeds of association or equivalent.

2. For the purposes of identifying the beneficial owner of a legal entity, obliged entities shall collect the information referred to in Article 44(1), point (a), and the information referred to in paragraph 1, point (b), of this Article.

Where, after having exhausted all possible means of identification pursuant to the first subparagraph, no natural person is identified as beneficial owner, or where there ***~~is any doubt~~ are doubts (516)*** that the person(s) identified is/are the beneficial owner(s), obliged entities shall ***record that no beneficial owner is identified and*** **(514)** identify the natural person(s) holding the position(s) of senior managing official(s) in the corporate or other legal entity and shall verify their identity. Obliged entities shall keep records of the actions taken as well as of the difficulties encountered during the identification process, which led to resorting to the identification of a senior managing official.

3. In the case of beneficiaries of trusts or similar legal entities or arrangements that are designated by particular characteristics or class, an obliged entity shall obtain sufficient information concerning the beneficiary so that it will be able to establish the identity of the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

4. Obliged entities shall obtain the information, documents and data necessary for the verification of the customer ~~and beneficial owner identity~~ through either of the following:

(a) the submission of the identity document, passport or equivalent ***and ~~or~~, where relevant, the acquisition of information from reliable and independent sources, whether accessed directly or provided by the customer, via reliable and trustworthy means, either physically or electronically (58, 520, 521, 522, 523). The extent of the documents consulted for the verification shall be commensurate to the risk.***

(b) the use of electronic identification means and relevant trust services as set out in Regulation (EU) 910/2014, ***in a reliable and trustworthy form via secure authentication processes, where appropriate, or other secure remote or electronic identification procedures regulated, recognised, approved or accepted by competent authorities, provided that the level of security designated is at least 'high' or equivalent. (480, 487, 527, 528, 529, 530)***

(ba) where applicable, the submission of proof of registration in the central register referred to in Article 10 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final] for customers who

are legal entities incorporated outside the Union, in accordance with Article 48 of this Regulation. (59)

Where a customer is a legal entity or a trustee or person in equivalent position acting on behalf of the legal arrangement, obliged entities shall take appropriate measures to verify the identity of the beneficial owner(s) of a legal entity or legal arrangement, including~~,~~ where this is possible, on the basis of identity documents or by means of electronic identification, so that they are satisfied that they know who the beneficial owner is and that they understand the ownership and control structure of the legal entity or legal arrangement. (532)

For the purposes of verifying the information on the beneficial owner(s), obliged entities shall also consult **(531, 532)** the central registers referred to in Article 10 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final],* ***irrespective of the Member State of the central register in which the beneficial ownership information is held (533).***

Where appropriate, and on a risk sensitive basis (534, 535), obliged entities shall also ~~as well as~~ consult additional information ***from the customer or from reliable and independent sources, in particular where the information in central registers does not match the information available to them under Article 18, where they have doubts as to the accuracy of the information or where there is a higher risk of money laundering or terrorist financing***.

Obliged entities shall determine the extent of the additional information to be consulted ***on a risk basis***, having regard to the risks posed by the transaction or the business relationship and the beneficial owner***, or the unusual or complex nature of the ownership structures given the nature of the company's business***.

Obliged entities shall report to the entity in charge of the central registers any discrepancies they find between the beneficial ownership information available therein and the beneficial ownership information available to them pursuant to this Article. National law pertaining to banking secrecy and confidentiality shall not hinder compliance with ~~that~~ the obligation set out in this subparagraph. (60)

Recital 32a

(32a) Obliged entities should take appropriate measures to verify the identity of the beneficial owners of their customers so that they are satisfied that they know who the beneficial owner is and that they understand the ownership and control structure of the customer.
When verifying a beneficial owner's identity, obliged entities should determine the extent and frequency of additional information consulted on a risk-basis. To this end, they should consult the necessary information, documents and data from the customer or reliable and independent sources, such as business register or other relevant corporate documents, and should also consult beneficial owners registers under Article 10 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final].
When verifying a person's identity, the robustness of the evidence provided and the risk of identity theft must be considered. It is therefore important that, when obliged entities suspect that the beneficial ownership information declared by the customer is false or the proof of identity provided is falsified or stolen, or

where there is any related risk that the identity of the beneficial owner may not coincide with the documentation provided, they should take steps to check whether the claimed identity reasonably belongs to the person declared by the customer and whether those persons actually are the beneficial owners of the legal entity or arrangement.

Recital 36

(36) Technological developments and progress in digitalisation enable a secure remote or electronic identification and verification of prospective and existing customers and can facilitate the remote performance of customer due diligence. The identification solutions as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council and the proposal for an amendment to it in relation to a framework for a European Digital Identity enable secure and trusted means of customer identification and verification for both prospective and existing customers and can facilitate the remote performance of customer due diligence. The electronic identification as set out in that Regulation should be taken into account and accepted by obliged entities for the customer identification process. These means of identification may present, where appropriate risk mitigation measures are in place, a standard or even low level of risk.

Recital 40

(40) To ensure the effectiveness of the AML/CFT framework, obliged entities should regularly review the information obtained from their customers, in accordance with the risk-based approach***. This does not mean that the obliged entity should repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An obliged entity may rely on the identification and verification steps that it has already undertaken in low risk situations, provided that there is no suspicion of money laundering or terrorist financing, or reasonable doubt that the information is no longer accurate and up to date and provided that there is no material change in the way that the customer's account is operated, which is not consistent with the customer's business profile. (536, 537, 538, 539, 541)*** Obliged entities should also set up a monitoring system to detect atypical transactions that might raise money laundering or terrorist financing suspicions. To ensure the effectiveness of the transaction monitoring, obliged entities' monitoring activity should in principle cover all services and products offered to customers and all transactions which are carried out on behalf of the costumer or offered to the customer by the obliged entity. However, not all transactions need to be scrutinised individually. The intensity of the monitoring should respect the risk-based approach and be designed around precise and relevant criteria, taking account, in particular, of the characteristics of the customers and the risk level associated with them, the products and services offered, and the countries or geographical areas concerned.**.** AMLA should develop guidelines to ensure that the intensity of the monitoring of business relationships and of transactions is adequate and proportionate to the level of risk.

Recital 41

(41) In order to ensure consistent application of this Regulation, AMLA should have the task of drawing up draft regulatory technical standards on customer due diligence. Those regulatory technical standards should set out the minimum set of information to be obtained by obliged entities in order to enter into new business relationships with customers or assess ongoing ones, according to the level of risk associated with each customer. Furthermore, the draft regulatory technical standards should provide sufficient clarity to allow market players to develop secure, accessible and innovative means of verifying customers' identity and performing customer due diligence, also remotely, while respecting the principle of technology neutrality. The Commission should be empowered to adopt those draft regulatory technical standards. Those specific tasks are in line with the role and responsibilities of AMLA as provided in Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final].

COMP P

<u>Articles 19, 20, 21, 21a:</u> Timing of the verification of the customer and beneficial owner identity/ Identification of the purpose and intended nature of a business relationship or occasional transaction/ Ongoing monitoring of the business relationship and monitoring of transactions performed by customers / Timing of the assessment whether the customer and the beneficial owner is subject to targeted financial sanctions

AMs covered: 543 (ID), 544 (EPP), 557 (Greens), 559 (Renew), 558 (Greens), 566 (S&D, Renew, Greens)

AMs falling: 545 (EPP), 546 (ID), 547(EPP), 548(ID), 549 (ID), 550 (ID), 551 (EPP), 552 (EPP), 553 (ID), 554 (EPP), 555 (EPP), 556 (ID), 560 (The Left), 561 (EPP), 562 (EPP), 563 (ID), 564 (EPP), 565 (ID).

Article 19: Timing of the verification of the customer and beneficial owner identity

1. Verification of the identity of the customer and of the beneficial owner shall take place before the establishment of a business relationship or the carrying out of an occasional transaction. Such obligation shall not apply to situations of lower risk under Section 3 of this Chapter, provided that the lower risk justifies postponement of such verification.

   By way of derogation from the first subparagraph, obliged entities other than credit and financial institutions involved in real estate transactions shall carry out verification of the customer identity, whether the buyer or seller or both, at the point when there is an offer ~~the purchaser's offer is accepted by the seller~~. (543, 544)

2. By way of derogation from paragraph 1, verification of the identity of the customer and of the beneficial owner may be completed during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such situations, those procedures shall be completed as soon as practicable after initial contact.

3. By way of derogation from paragraph 1, a credit institution or financial institution may open an account, including accounts that permit transactions in transferable securities, as may be required by a customer provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the customer due diligence requirements laid down in Article 16(1), first subparagraph, points (a) and (b) is obtained.

4. Whenever entering into a new business relationship with a legal entity or the trustee of an express trust or the person holding an equivalent position in a similar legal arrangement referred to in Articles 42, 43 and 48 and subject to the registration of beneficial ownership information pursuant to Article 10 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*, obliged entities shall collect proof of registration or an excerpt of the register.

Articles 2 (16)

(16) 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration, including a relationship where an obliged entity is asked to form a company or set up a trust for its customer, whether or not the formation of the company or setting up of the trust is the only transaction carried out for that customer. ***In the case of real estate transactions, for entities other than credit and financial institutions, a business relationship means the provision of services which involve the sale or brokerage of more than one property over a period of time.***

Recital 33a

33a) Business relationships are appropriately defined in this Regulation and refer to business, professional or commercial relationships connected with the professional activities of an obliged entity. They are expected, at the time when the contact is established, to have an element of duration. In the case of real estate transactions, for entities other than credit and financial institutions, a business relationship means the provision of services which involve the sale or brokerage of more than one property over a period of time. The sale includes also services of notaries or lawyers where these are required under national law in order to conduct the transactions and/or transfer of immovable property.

Article 20: Identification of the purpose and intended nature of a business relationship or occasional transaction

Before entering into a business relationship or performing an occasional transaction, an obliged entity shall obtain at least the following information in order to understand its purpose and intended nature:

(a) the purpose of the envisaged account, transaction or business relationship;
(b) the estimated amount and economic rationale of the envisaged transactions or activities;
(c) the source of funds;
(d) the destination of funds.

Article 21: Ongoing monitoring of the business relationship and monitoring of transactions performed by customers

1. Obliged entities shall conduct ongoing monitoring of the business relationship, including transactions undertaken by the customer throughout the course of that relationship, to control that those transactions are consistent with the obliged entity's knowledge of the customer, the customer's business activity and risk profile, and where necessary, with the information about the origin ***and destination*** (557) of the funds and to detect those transactions that shall be made subject to a more thorough analysis pursuant to Article 50.

2. In the context of the ongoing monitoring referred to in paragraph 1, obliged entities shall ensure that the relevant documents, data or information of the customer are kept up-to-date.
   The frequency of updating customer information pursuant to the first sub-paragraph shall be based on the risk posed by the business relationship. The frequency of updating of customer information shall ***be established on a risk sensitive basis, particularly taking into account changes of relevant circumstances and shall*** in any case not exceed five years**.** ***In case of high-risk business relationships the frequency for updating customer information shall not exceed two years. (558, 559)***

3. In addition to the requirements set out in paragraph 2, obliged entities shall review and, where relevant, update the customer information where:

   (a) there is a change in the relevant circumstances of a customer;
   (b) the obliged entity has a legal obligation in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owner(s) or to comply with Council Directive 2011/16/EU[1];
   (c) they become aware of a relevant fact which pertains to the customer.

4. By *[2 years after the entry into force of this Regulation]*, AMLA shall issue guidelines on ongoing monitoring of a business relationship and on the monitoring of the transactions carried out in the context of such relationship.

Article 21a: Timing of the assessment whether the customer and the beneficial owner is subject to targeted financial sanctions

1. Obliged entities shall assess whether the customer or the beneficial owner is subject to targeted financial sanctions when verifying the identity of the customer and the beneficial owner pursuant to Article 19.

2. In addition to the requirements set out in paragraph 1, and without prejudice to any other measures required to comply with the obligation to apply targeted financial sanctions, credit and financial institutions shall screen the identity of their existing customers or beneficial owners against the relevant EU sanctions lists of designated

persons on a regular basis, and each time targeted financial sanctions are adopted by the Union.

3. In addition to the requirements set out in Paragraph 1 and without prejudice to any other measures required by Union law relating to targeted financial sanctions, obliged entities other than credit and financial institutions shall assess on a regular basis whether any existing customer or beneficial owner is subject to targeted financial sanctions.

4. In case an obliged entity identifies, in the course of its customer due diligence requirements, that a customer or beneficial owner is subject to targeted financial sanctions, it shall immediately notify the competent authority accordingly.

5. By [2 years after the entry into force of this Regulation], AMLA shall issue guidelines on the measures to be applied by obliged entities for assessing whether the customer or the beneficial owner is subject to targeted financial sanctions. Those guidelines shall include the following elements:

a) risk-based procedures to be established by obliged entities in order to assess whether the customer or the beneficial owner is subject to targeted financial sanctions;
b) the extent, timing and procedures for screening measures to be applied by credit and financial institutions and crypto-asset service providers with regard to existing customers or when entering into a new business relationship;
c) the conditions to be fulfilled for identifying entities controlled by persons subject to targeted financial sanctions;
d) the notification measures to competent authorities in case an obliged entity identifies a customer or a beneficial owner subject to targeted financial sanctions.*(566)*

COMP Q *:*

<u>Article 22, 22a:</u> Regulatory technical standards on the information necessary for the performance of customer due diligence / Special provisions regarding online gambling

AMs covered: 61 (co-rapporteurs), 571 (Renew) 573 (The Left)
AMs falling: 567(EPP), 568 (ID), 569 (The Left), 570 (The Left), 572 (ID)

Article 22: Regulatory technical standards on the information necessary for the performance of customer due diligence

1. By *[2 years after the entry into force of this Regulation]* AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify:

   (a) the requirements that apply to obliged entities pursuant to Article 16 and the information to be collected for the purpose of performing standard, simplified and enhanced customer due diligence pursuant to Articles 18 and 20 and Articles 27(1) and 28(4), including minimum requirements in situations of lower risk ;

(b) the type of simplified due diligence measures which obliged entities may apply in situations of lower risk pursuant to Article 27(1), including measures applicable to specific categories of obliged entities and products or services, having regard to the results of the supra-national risk assessment drawn up by the Commission pursuant to Article 7 of *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*;

(c) the type of exemptions that may apply to certain customer due diligence measures with respect to electronic money, on the basis of an appropriate risk assessment which demonstrates a low risk;

(c) the reliable and independent sources of information that may be used to verify the identification data of natural or legal persons for the purposes of Article 18(4) ***in addition to minimum requirements to be complied with and necessary steps to be taken by obliged entities where discrepancies are found; (61)***

(d) the list of attributes which electronic identification means and relevant trust services referred to in Article 18(4), point (b), must feature in order to fulfil the requirements of Article 16, points (a), (b) and (c) in case of standard, simplified and enhanced customer diligence.

2. The requirements and measures referred to in paragraph 1, points (a) and (b), shall be based on the following criteria:

(a) the inherent risk involved in the service provided;
(b) the nature, amount and recurrence of the transaction;
(c) the channels used for conducting the business relationship or the occasional transaction.
(ca) the residual risk, taking into account a proper risk assessment, the risk mitigating measures put in place by the obliged entities, also considering innovation and technical developments to detect and prevent suspicious transactions. (571)

3. AMLA shall review regularly the regulatory technical standards and, if necessary, prepare and submit to the Commission the draft for updating those standards in order, inter alia, to take account of innovation and technological developments.

4. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraphs 1 and 3 of this Article in accordance with Articles 38 to 41 of Regulation *[please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]*.

Article 22a: Special provisions regarding online gambling

***1. ~~Providers of~** Gambling services, ~~to the extent that they provide a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions~ that are provided by any means at a distance, by electronic means or any other technology for facilitating communication, shall be subject to this Article.*

~~*2. A provider of gambling services may only admit a person as a player to a service as referred to in paragraph 1 provided that it has set up a gambling account for the player in that player's name.*~~

~~*3. Providers of gambling services shall not accept any deposits or other refundable monies from players in gambling accounts that are not used for the immediate purpose of gambling. The balance in a gambling account shall not bear any interest.*~~

2. Providers of gambling services shall ensure that transactions from players to gambling accounts are made only from an account held at a credit or financial institution referred to in Article 3 paragraph 1 and 2 ~~*payment accounts as defined in Article 4, point (12), of Directive (EU) 2015/2366 which were set up in the name of the player concerned with an obliged entity under Article 1, point (1)(a) and (d), of that Directive. Providers of gambling services shall ensure that payment transactions are only executed by means of the following payment services within the meaning of Article 4, point (3), of Directive (EU) 2015/2366:*~~

~~*(a) a direct debit;*~~
~~*(b) a payment transaction through a payment card or similar device; or*~~
~~*(c) a credit transfer.*~~

3. A provider of gambling services shall refund a player only by executing a payment transaction within the meaning of Article 4, point (5), of Directive (EU) 2015/2366 to a payment account set up in the name of that player with a payment service provider as referred to in Article 1, point (1)(a) and (d), of that Directive.
~~*A provider of gambling services shall specify the payment reference in the payment transaction in such a manner that the reason for the payment transaction is transparent to the payment service provider or an outside observer. The competent authorities may designate standard wording to be used by providers of gambling services for the purposes of the payment reference.*~~

4. In addition to the circumstances referred to in Article 15 paragraph 3, providers of gambling services referred to in paragraph 1 shall carry out CDD in the context of a business relationship at the opening of a gambling account ~~*By way of derogation from Article 19, point (1), the provider of gambling services may carry out a provisional identification of a player for whom it sets up a gambling account. The provisional identification may be based on an electronic copy or copy sent by post of a document where there is little risk of money laundering or terrorist financing. Where a provider of gambling services carries out a provisional identification of a player, it shall carry out a full verification of the identity of the player and of the beneficial owner as soon as possible after setting up the gambling account.*~~
(573)

SECTION 2
Third-country policy and ML/TF threats from outside the Union

COMP R

Article 23, 24 - Identification of third countries with significant strategic deficiencies in their national AML/CFT regimes / Identification of third countries with compliance weaknesses in their national AML/CFT regimes

AMs Covered: 62 (Co-rapporteurs), 575 (Left), 576 (EPP), 577 (EPP), 578 (EPP), 579 (EPP), 581 (Left), 583 (EPP), 585 (EPP), 587 (EPP), 588 (S&D), 590 (EPP), 591 (EPP), 592 (EPP), 593 (EPP), 594 (Left), 595 (S&D), 596 (Renew), 597 (EPP), 598 (S&D)

AMs Falling: 574 (Left), 580 (EPP), 582 (EPP), 584 (EPP), 586 (EPP), 589 (Left)

Recitals 49, 50, 51

AMs Covered: 189 (S&D), 190 (Renew), 191 (Left), 192 (EPP), 195 (EPP), 199 (EPP)

AMs Falling: 193 (ID), 194 (ID)

Article 23
Identification of third countries with significant strategic deficiencies in their national AML/CFT regimes

1. Third countries with significant strategic deficiencies in their national AML/CFT regimes shall be identified by the Commission and designated as 'high-risk third countries'.

2. In order to identify the countries referred to in paragraph 1, the Commission is empowered to adopt delegated acts in accordance with Article 60 to supplement this Regulation, where (577):

   (a) significant strategic deficiencies in the legal and institutional AML/CFT framework of the third country have been identified; ***or*** (62)

   (b) significant strategic deficiencies in the effectiveness of the third country's AML/CFT system in addressing money laundering or terrorist financing risks have been identified;

   (c) the significant strategic deficiencies identified under points (a) and (b) are of a persistent nature and no measures to mitigate them have been taken or are being taken.

   Those delegated acts shall be adopted within one month after the Commission has ascertained that the criteria in point (a), (b) or (c) are met. ***This shall mean 1 month after the publication of a public statement or a compliance document concerning the third country by international organisations and standard setters.***

3. For the purposes of paragraph 2, the Commission shall take into account calls for the application of enhanced due diligence measures and additional mitigating measures ('countermeasures') by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, as well as relevant evaluations, assessments, reports or public statements drawn up by them. ***For***

the purposes of establishing whether a third country has significant strategic deficiencies in its national AML/CFT regime, the Commission shall also consider, where appropriate, any relevant assessments by AMLA or other Union institutions, bodies and agencies competent authorities, civil society organisations, and academia. The Commission shall make its assessments of high risk third countries publicly available. (575, 581)

4. Where a third country is identified in accordance with the criteria referred to in paragraph 3, obliged entities shall apply enhanced due diligence measures listed in Article 28(4), points (a) to (g) with respect to the business relationships or occasional transactions involving natural or legal persons from that third country.

5. The delegated act referred to in paragraph 2 shall identify among the countermeasures listed in Article 29 the specific countermeasures mitigating country-specific risks stemming from high-risk third countries (585).

6. The Commission shall review the delegated acts referred to in paragraph 2 on a regular basis, ***within 1 month following any relevant change in the assessment by international organisations and standard setters, and at least every two years*** to ensure that the specific countermeasures identified pursuant to paragraph 5 take account of the changes in the AML/CFT framework of the third country and are proportionate and adequate to the risks (588).

Article 24

Identification of third countries with compliance weaknesses in their national AML/CFT regimes

1. Third countries with compliance weaknesses in their national AML/CFT regimes shall be identified by the Commission.

2. In order to identify the countries referred to in paragraph 1, the Commission is empowered to adopt delegated acts in accordance with Article 60 to supplement this Regulation, where:

   (a) compliance weaknesses in the legal and institutional AML/CFT framework of the third country have been identified***;***

   (b) compliance weaknesses in the effectiveness of the third country's AML/CFT system in addressing money laundering or terrorist financing risks have been identified.

   Those delegated acts shall be adopted within one month after the Commission has ascertained that the criteria in point (a) or (b) are met. ***This shall mean 1 month after the publication of a public statement or a compliance document concerning the third country by international organisations and standard setters.***

3. The Commission, when drawing up the delegated acts referred to in paragraph 2 shall take into account information on jurisdictions under increased monitoring by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, as well as relevant evaluations, assessments, reports or public statements drawn up by them. ***The Commission shall also consider, where appropriate, any relevant assessments by AMLA or other Union institutions, bodies and agencies competent authorities, civil***

society organisations, and academia. The Commission shall make its assessments of high risk third countries publicly available. (594, 595, 596).

4. The delegated act referred to in paragraph 2 shall identify the specific enhanced due diligence measures among those listed in Article 28(4), points (a) to (g), that obliged entities shall apply to mitigate risks related to business relationships or occasional transactions involving natural or legal persons from that third country.

5. The Commission shall review the delegated acts referred to in paragraph 2 on a regular basis, ***within 1 month following any relevant change in the assessment by international organisations and standard setters, and at least every two years*** to ensure that the specific enhanced due diligence measures identified pursuant to paragraph 4 take account of the changes in the AML/CFT framework of the third country and are proportionate and adequate to the risks (598).

(49) In order to protect the proper functioning of the Union financial system from money laundering and terrorist financing, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission to identify third countries, whose shortcomings in their national AML/CFT regimes represent a threat to the integrity of the Union's internal market. The changing nature of money laundering and terrorist financing threats from outside the Union, facilitated by a constant evolution of technology and of the means at the disposal of criminals, requires that quick and continuous adaptations of the legal framework as regards third countries be made in order to address efficiently existing risks and prevent new ones from arising. The Commission should take into account information from ***other EU institutions, bodies and agencies, competent authorities, civil society organisations, academia, and by*** international organisations and standard setters in the field of AML/CFT, such as FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, and adapt its assessments to the changes therein, where appropriate. (189, 190, 191)

(50) Third countries "subject to a call for action" by the relevant international standard-setter (the FATF) present significant strategic deficiencies of a persistent nature in their legal and institutional AML/CFT frameworks and their implementation which are likely to pose a high risk to the Union's financial system. The persistent nature of the significant strategic deficiencies, reflective of the lack of commitment or continued failure by the third country to tackle them, signal a heightened level of threat emanating from those third countries, which requires an effective, consistent and harmonised mitigating response at Union level. Therefore, obliged entities should be required to apply the whole set of available enhanced due diligence measures to occasional transactions and business relationships involving those high-risk third countries to manage and mitigate the underlying risks. Furthermore, the high level of risk justifies the application of additional specific countermeasures, whether at the level of obliged entities or by the Member States. Such approach would avoid divergence in the determination of the relevant countermeasures, which would expose the entirety of Union's financial system to risks. Given its technical expertise, AMLA can provide useful input to the Commission in identifying the appropriate countermeasures.

(51) Compliance weaknesses in both the legal and institutional AML/CFT framework and its implementation of third countries which are subject to "increased monitoring" by the FATF are susceptible to be exploited by criminals. This is likely to represent a risk for the Union's financial system, which needs to be managed and mitigated. The commitment of these third countries to address identified weaknesses, while not

eliminating the risk, justifies a mitigating response, which is less severe than the one applicable to high-risk third countries. In these cases, Union's obliged entities should apply enhanced due diligence measures to occasional transactions and business relationships when dealing with natural persons or legal entities established in those third countries that are tailored to the specific weaknesses identified in each third country. Such granular identification of the enhanced due diligence measures to be applied would, in line with the risk-based approach, also ensure that the measures are proportionate to the level of risk. To ensure such consistent and proportionate approach, the Commission should be able to identify which specific enhanced due diligence measures are required in order to mitigate country-specific risks. Given AMLA's technical expertise, it can provide useful input to the Commission to identify the appropriate enhanced due diligence measures.

Art. 25: Identification of third countries posing a threat to the Union's financial system

AMs Covered: 63 (Co-rapporteurs), 64 (Co-rapporteurs), 65 (Rapporteur), 66 (Co-rapporteurs), 67 (Co-rapporteurs), 68 (Co-rapporteurs), 69 (Co-rapporteurs), 599 (Greens, S&D, Renew), 600 (Left), 601 (EPP), 602 (Left), 603 (Left), 604 (Greens, S&D, Renew), 605 (EPP), 606 (NI), 607 (Renew), 608 (Left), 609 (Left), 610 (EPP), 611 (EPP), 612 (Greens, S&D, Renew), 613 (Renew), 614 (S&D), 617 (S&D), 620 (EPP), 621 (Left), 622 (S&D), 623 (Greens, S&D, Renew), 624 (Renew), 625 (EPP), 626 (EPP), 627 (EPP), 627 (EPP), 628 (S&D), 629 (Greens, S&D, Renew).

AMs Falling: 603 (Left), 618 (Left), 619 (ID)

Recitals: 52, 53

AMs Covered: 196 (EPP), 197 (Renew), 198 (S&D), 199 (EPP), 602 (Left), 617 (S&D), 618 (Left), 621 (Left), 622 (S&D), 624 (Renew), 201 (Left)

AMs Falling: 200 (ID)

Article 25

*Identification of third countries posing **a specific and serious** threat to the Union's financial system*

1. ***In the context of its tasks specified in Article 5 (1) (b) of Regulation [insert reference to AMLA Regulation], AMLA shall monitor and assess, in line with the risk-based approach,*** ~~The Commission is empowered to adopt delegated acts in accordance with Article 60 identifying~~ third countries that pose a specific and serious threat to the financial system of the Union and the proper functioning of the internal market other than those covered by Articles 23 and 24 (600, 601).

AMLA shall carry out the assessment referred to in the first subparagraph on its own initiative, or following a request from the Commission, the European Parliament or the Council.

Following a request from <u>the Commission,</u> the European Parliament or the Council, AMLA shall analyse whether a specific third country poses a specific and serious threat to the financial system of the Union and the proper functioning of the internal market and assess whether specific enhanced due diligence measures or countermeasures should be proposed in

accordance with paragraph 3 in order to mitigate such threat. Where AMLA concludes that the specific third country referred to in the first subparagraph does not pose a specific and serious threat to the financial system of the Union, it shall provide a report to the requesting institution within ~~30~~ 60 days of receipt of the request stating the reasons for its decision. (69, 629)

2. ~~The Commission, when drawing up the delegated acts~~ ***For the purpose of monitoring ~~identifying~~ third countries posing a specific and serious threat to the financial system of the Union and the proper functioning of the internal market*** referred to in paragraph 1, ***and determine the level of threat, AMLA*** shall take into account the following criteria (603, 604) ***where relevant:***

(a) the legal and institutional AML/CFT framework of the third country (605) in particular:

(i) the criminalisation of money laundering ***and its predicate offences*** and terrorist financing; (63, 606)

(ii) measures relating to customer due diligence;

(iii) requirements relating to record-keeping;

(iv) requirements to report suspicious transactions;

(v) ***requirements relating to*** the availability of accurate and timely information of the beneficial ownership of legal persons and arrangements ~~to competent authorities~~ ***held by a public authority or body functioning as a beneficial ownership register, or an alternative mechanism that is as efficient***; (64, 607)

(va) the laws, regulations and administrative provisions of the third country prevent the effective cooperation ~~requirements for competent authorities and judicial authorities to cooperate~~ with competent authorities and judicial authorities of the Member States; (65)

~~(vb) alignment with targeted financial sanctions and proliferation financing-related targeted financial sanctions;~~ ~~(66)~~

(vc) policies in relation to targeted financial sanctions and proliferation financing-related targeted financial sanctions and requirements to mitigate and manage the risks of non-implementation and evasion of targeted financial sanctions and proliferation financing-related targeted financial sanctions. (67)

(vd) whether the third country features on the Union list of non-cooperative jurisdictions for tax purposes; (608)

(ve) whether the third country legal framework provides financial secrecy, ~~as acknowledged by credible sources~~; (609)

(vf) whether the third country's actions run counter to the FATF core principles or represent a gross violation of the commitment to international cooperation;

(b) the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing including appropriately effective, proportionate and dissuasive sanctions, as well as the third country's practice in cooperation and exchange of information with Member States' competent authorities; (610)

(c) the effectiveness of the third country's AML/CFT system in addressing money laundering or terrorist financing risks; (611)

(ca) the quality and effectiveness of financial supervision;

(cb) the existence of a regulatory framework for crypto-assets service providers;

(cc) the extent to which that third country ~~is characterized by high levels of official or institutional corruption~~ is identified as having significant levels of corruption or other criminal activity;
(cd) the recurrence of the involvement of the third country in money laundering or terrorist financing, as reflected in criminal analyses and investigations by Member States' competent authorities, and notably those supported by Europol. (612, 613, 614)

3. For the purposes of determining the level of threat referred to in paragraph 1 ***and identifying mitigating measures ~~specific countermeasures in accordance with Article 29~~, AMLA*** ~~the Commission may~~ ***shall ~~consult~~ take into account any opinion issued by*** ~~request~~ ***EBA, ESMA, EIOPA, ~~as appropriate,~~*** ~~AMLA to adopt an opinion aimed at on assessing~~ concerning the specific impact on the ***orderly functioning and*** integrity of the Union's financial system due to the level of threat posed by a third country. (617, 618, 619, 620)

4. ***When monitoring ~~identifying the~~ third countries posing a specific and serious threat to the Union and determining the level of threat, AMLA shall assess the impact of such threat on the financial system of the Union and on the proper functioning of the internal market.***
~~The Commission, when drawing up the delegated acts referred to in paragraph 1,~~ ***AMLA*** shall take into account***, where appropriate, any*** ~~in particular~~ relevant ***public revelations,*** evaluations***,*** assessments or reports drawn up by ***other Union institutions, bodies and agencies, competent authorities, civil society organisations and academia as well as*** international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing. (621, 622, 624).

~~5. Where the identified specific and serious threat from the concerned third country amounts to a significant strategic deficiency, Article 23(4) shall apply and the delegated act referred to in paragraph 2 shall identify specific countermeasures as referred to in Article 23(5).~~

~~6. Where the identified specific and serious threat from the concerned third country amounts to a compliance weakness, the delegated act referred to in paragraph 2 shall identify specific enhanced due diligence measures as referred to in Article 24(4).~~

7. ***In order to ensure a consistent approach towards AML/CFT threats coming from third countries referred to in paragraph 1, AMLA shall identify specific enhanced due diligence measures that obliged entities shall apply to mitigate risks related to business relationships or occasional transactions involving natural or legal persons from a high third country that poses a specific and serious threat to the Union.***

For that purpose, AMLA shall be empowered to develop draft regulatory technical standards to specify the appropriate enhanced due diligence measures, proportionate to the level of threat, among those listed in Article 28(4), points (a) to (g) that obliged entities shall apply. AMLA shall submit those draft regulatory technical standards to the Commission for adoption (599). ***Those draft regulatory technical standards shall be based on purely technical assessment of ML/TF risks and do not imply strategic decisions or policy choices.***

The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in this paragraph in accordance with

Articles 38 to 41 of Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]. (68, 602, 623)

AMLA ~~The Commission~~ shall review the ~~delegated acts~~ ***regulatory technical standards*** referred to in paragraph ***5*** on a regular basis ***and at least every two years*** to ensure that the measures referred to in ***that paragraph*** take account of the changes in the AML/CFT framework of the third country and are proportionate and adequate to the risks. ***If necessary, AMLA shall prepare and submit to the Commission the draft for updating those standards.*** (628)

7a. ***If the serious threat to the financial system of the Union persists and no effective measures have been taken or are being taken by the third country to mitigate the high risks, the Commission shall identify by means of delegated acts specific countermeasures among those listed in Article 29, where justified by the nature of the threat. For that purpose, the Commission shall request AMLA to adopt an opinion aimed at assessing the measures which may have been taken or are being taken by the third country to mitigate the threat and identifying possible countermeasures.***
In case of significant divergences with the opinion of AMLA, the Commission shall adopt a reasoned analysis, which shall be publicly available. (627)

(52) Countries that are not publicly identified as subject to calls for actions or increased monitoring by international standard setters might still pose a threat to the integrity of the Union's financial system ***and the orderly functioning of the internal market***. ***AMLA should monitor developments third countries and assess related threats and risks for the Union.*** To mitigate those risks, it should be possible for ~~the Commission~~ ***AMLA*** to take action by identifying, based on a clear set of criteria and with the support of ~~AMLA~~ ***other Union institutions, bodies, agencies and competent authorities, analysis by civil society organisations, academia, as well as assessments or reports drawn up by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing***, third countries ***or territories*** posing a specific and serious threat to the Union's financial system, which may be due to either compliance weaknesses or significant strategic deficiencies of a persistent nature in their AML/CFT regime, and the relevant mitigating measures. ***For that purpose, AMLA should develop draft regulatory technical standards to identify specific enhanced due diligence measures to be applied by obliged entities to mitigate risks related to business relationships or occasional transactions involving natural or legal persons from a high third country that poses a specific and serious threat to the Union.*** ~~Those third countries should be identified by the Commission.~~ According to the level of risk posed to the Union's financial system, ~~the Commission~~ ***AMLA*** should require the application of either all enhanced due diligence measures ~~and country-specific countermeasures, as it is the case for high-risk third countries,~~ or country-specific enhanced customer due diligence~~, such as in the case of third countries with compliance weaknesses~~. ***If the threat to the Union's financial system persists and no effective measures have been taken by the third country to mitigate the high risks, the Commission, after consultation of AMLA, should be able to require the application of additional countermeasure.*** (196, 197, 198, 602, 616, 617, 621, 622, 624)

(53) Considering that there may be changes in the AML/CFT frameworks of those third countries ~~***or territories***~~ or in their implementation, for example as result of the country's

commitment to address the identified weaknesses or of the adoption of relevant AML/CFT measures to tackle them, which could change the nature and level of the risks emanating from them, the Commission should regularly review the identification of those specific enhanced due diligence measures in order to ensure that they remain proportionate and adequate. ***The Commission should publish such reviews ~~so that they are open to public scrutiny~~***. (201)

Technical note on revised Article 25

Key elements

Following the concerns expressed by political groups and several exchanges with the legal service, Article 25 was revised as follows:

- AMLA, as the main EU body with AML/CFT competences, is entrusted with the responsibility to carry out an technical assessment of third country ML/TF risks and identify mitigating measures by developing draft RTS, to limit the politicisation of the process;
- AMLA's role in the assessment is strengthened (RTS vs simple opinion) *[in the direction of S&D, Renew, Greens and Left who support a primary role for AMLA in the listing process]*, but it is not binding for the Commission. The Commission's discretion over the adoption of the RTS is preserved *[in line with concerns by EPP and ECR, who want to keep some discretion for Commission]* in line with RTS procedure described in Art 38-41 of AMLA Regulation;
- Co-legislators scrutiny powers over AMLA proposals are preserved; *[to address concerns by legal service over delimitation of agency powers]*

Detailed explanation

The compromise pursue the following policy objectives:

1. Preserve the Union's strategic autonomy to effectively respond to external threats in the field of ML/TF, which may affect the integrity of the Union's financial system and proper functioning of internal market. This objective is consistent with FATF Recommendations 19, which provides that countries should also be able to apply countermeasures independently of any call by the FATF to do so.

2. Ensure that any mitigating measures vis-à-vis high-risk third countries is applied uniformly and in a consistent manner at EU level, given that the nature of the threat to the Union's financial system and orderly functioning of internal market. Council GA preserves the possibility to go beyond FATF only for individual countries, which may not be sufficient or suitable to address threats affecting the Union as a whole.

3. Ensure that the process is based on a solid and independent assessment of ML/TF risks to be carried out by the competent EU Authority, within the legal constraints on delegation of powers to agencies in line with Treaties and relevant case law.

The compromise includes the following key elements:

- AMLA is entrusted with the responsibility to monitor risks and threats coming from third countries. This task has already a basis in the current text of AMLA Regulation, namely Article 1.3(b) (objectives) and Article 5 para 1 (b) (tasks)[14].

- As a response to a threat posed by a third country, AMLA is empowered to adopt draft RTS to identify which enhanced due diligence measures obliged entities should apply to mitigate risks posed by a specific third country.

- No distinction is made between countries with significant strategic deficiency or country with compliance weakness (para 5 and 6 are removed), because the EU process is not intended to replicate, but rather to complement the FATF process and the application of EDD will be risk-based depending on the country specific assessment.

- AMLA's assessment is not binding for the Commission. In accordance with the procedure described in Articles 38-41 of AMLA Regulation, the Commission may decide not to endorse or amend the draft RTS. Nevertheless, deviations from AMLA assessment need to be justified.

- The legal service has expressed reservations about the use of RTS rather than delegated acts in this context, due to the fact that the current text of the AMLA Regulation requires RTS to be technical and not imply strategic decisions or policy choices.

- In order to address those legal concerns, the scope of RTS in Article 25 has now been limited to the definition of EDD measures, whereas the application of additional countermeasures would be a responsibility of the Commission in line with Article 29 AMLR. This is to address the possible concern that countermeasures may go beyond a purely technical assessment and contain an element of political pressure. AMLA would still provide its technical expertise to the Commission with an opinion.

- Moreover, in line with Article 38 AMLA Regulation (*the content of RTS shall be delimited by the legislative acts on which they are based*) the definition of EDD will be based on the list provided in Article 28 of AMLR proposal. The definition of EDD by AMLA to address specific risks is a technical task and should not involve strategic decisions or policy choices.

- The use of RTS in this context is in fact consistent with the approach used in Article 15.5 of this Regulation, which requires AMLA to develop draft RTS to identify high risk sectors or transactions as well as Article 22.1 point (b) of this Regulation, which requires AMLA to define the appropriate mitigating measures for situations of low risk. It is also consistent with Article 23 and 24 since in all cases the measures will ultimately be adopted by means of delegated acts.

[14] Article 1.3b: *The objective of the Authority shall be to protect the public interest, the stability of the Union's financial system and the good functioning of the internal market by:*
[…] contributing to identify and assess risks of money laundering and terrorist financing across the internal market, as well as risks and threats originating from outside the Union that are impacting, or have the potential to impact the internal market;

Art. 5.1 b: *The Authority shall perform the following tasks with respect to money laundering/ terrorist financing ('ML/TF') risks facing the internal market: […]*
(b) monitor developments in third countries and assess threats, vulnerabilities and risks in relation to their AML/CFT systems;

- The assessment required to AMLA for the identification of third country risks and mitigating measures has a precedent in the Capital Requirement Regulation (CRR) which empowers ESMA to develop draft implementing technical standards on main indices and recognized exchanges (link). The ESMA ITS are used to develop a list of main indices and exchanges for the purpose of specifying which collateral can be used by EU banks and investment firms. The CRR requires ESMA to conduct a comprehensive assessment, which has similarities with the AMLA assessment in this context. Similarly to the challenges faced by ESMA under the CRR, AMLA may not be in the position to conduct a comprehensive assessment of the legislative and regulatory framework of all jurisdictions outside the Union. However, the goal is not to replicate the FATF process, but to ensure AMLA has the power to take the appropriate action when it identifies situations of high risk, in the context of its tasks to monitor third countries developments and assess risks and threats for the Union, as provided by the AMLA Regulation.

Article 25a: Identification of credit institutions or financial institutions or crypto-asset service providers not established in the Union posing a specific threat to the Union's financial system

AMs Covered: 70 (Co-rapporteurs), 615 (Greens, S&D, Renew), 616 (Greens, S&D, Renew), 630 (EPP)

Recitals: 47, 53a, 54

AMs Covered: 10 (Co-rapporteurs), 11 (Co-rapporteurs), 202 (S&D)

AMs Falling: 203 (ID)

Article 25a

Identification of credit or financial institutions not established in the Union posing a specific and serious threat to the Union's financial system

1. AMLA shall be empowered to ~~identify~~ assess, in line with the risk-based approach, whether specific credit or financial institutions not established in the Union ~~which~~ pose a specific and serious threat to the financial system of the Union.

AMLA shall ~~also~~ carry out the assessment ~~analysis~~ ~~directed at the identification as~~ referred to in the first subparagraph on its own initiative following information received in the context of its supervisory tasks, or following a request from the European Parliament, the Council, a Member State, or a supervisor.

2. For the purpose of the identification of credit or financial institutions referred to in paragraph 1, AMLA shall take into account in particular the following criteria:

(a) the involvement of such entity in money laundering and terrorist financing;

(b) connections with organized crime and terrorism;

(c) the entity does not comply with customer due diligence procedures;

(d) the entity carries out illegal activities; and

(e) the entity mainly provides products and services prohibited in the Union, such as anonymous accounts~~, privacy wallets~~ and other anonymising tools providing for the anonymization of the customer account or obfuscation of transactions. (615)

3. For the purpose of identifying credit of financial institutions referred to in paragraph 1, AMLA shall take into account, where appropriate, any relevant information, public revelations and relevant evaluations, assessments or reports drawn up by other Union institutions, bodies, agencies and competent authorities, civil society organisations and academia, as well as by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing.

Where relevant, AMLA may launch a public consultation to seek information on the criteria laid down in paragraph 2, and request information to third country supervisory authorities, FIUs and Europol, as deemed appropriate.

~~For the purposes of determining the level of threat referred to in paragraph 1 and identifying specific countermeasures,~~ AMLA ~~may request ECB,~~ shall take into account any opinion issued by EBA, ESMA or EIOPA~~, as appropriate, to adopt an opinion aimed at~~ for the purposes of determining the level of threat referred to in paragraph 1, assessing the degree of exposure of the Union to a specific credit or financial institution not established in the Union, and the specific impact of the concerned credit or financial institution on the orderly functioning and integrity of the Union's financial system. (616)

4. Where AMLA concludes that a specific credit or financial institution not established in the Union poses a specific and serious threat to the financial system of the Union which cannot be eliminated by other means, it shall require selected obliged entities to adopt one or more of the following measures:

- ***(a) the application of elements of enhanced due diligence;***
- ***(b) the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;***
- ***(c) limiting business relationships or transactions with that credit institution or financial institution.***

5. Where a coordinated action by competent authorities is necessary to respond to a specific and serious threat to the integrity of the Union's financial system or the proper functioning of the internal market, AMLA shall be empowered to adopt decisions requiring national competent authorities to ensure that non-selected obliged entities are required to take the necessary mitigating measures with respect to specific credit or financial institutions in accordance with the AMLA decision referred to in paragraph 4.

6. Where the analysis referred to in paragraph 1 is requested by the Commission, the European Parliament, the Council, a Member State, or by a supervisor, and AMLA concludes that a specific credit or financial institution not established in the Union does not pose a specific and serious threat to the financial system of the Union, it shall provide a reasoned justification to the requestor within ~~30~~ 60 days.

AMLA shall publish on its website notice of any decision referred to in paragraph 4.

The notice shall at least specify the measures imposed in accordance with paragraph 4 and the reasons why AMLA is of the opinion that it is necessary to impose the measures including the evidence supporting those reasons.

A measure shall take effect when the notice is published on the AMLA website or at a time specified in the notice that is after its publication. After deciding to impose any measure referred to in paragraph 4, AMLA shall immediately notify the competent authorities. (70, 599, 630)

(53a) Certain credit or financial institutions not established in the Union could also pose a specific and serious threat to the financial system of the Union. To mitigate that threat, AMLA should be able, on its own initiative or at the request of the specific bodies set out in this Regulation, to take action by identifying credit or financial institutions not established in the Union which poses a specific and serious threat to the Union's financial system. Depending on the level of risk posed to the Union's financial system, AMLA should require selected obliged entities to apply concrete measures to mitigate risks and should be able to adopt decisions addressed to financial supervisors to ensure that non-selected obliged entities apply uniform mitigating measures to the ones identified by AMLA. (11)

(54) Potential external threats to the Union's financial system do not only emanate from third countries, but can also emerge in relation to specific customer risk factors or products, services, transactions or delivery channels which are observed in relation to a specific geographical area outside the Union. There is therefore a need to identify money laundering and terrorist financing trends, risks and methods to which Union's obliged entities may be exposed. AMLA***, with the support of other EU bodies and agencies already involved in the AML/CFT framework, competent authorities and Europol,*** is best placed to detect any emerging ML/TF typologies from outside the Union, to monitor their evolution with a view to providing guidance to the Union's obliged entities on the need to apply enhanced due diligence measures aimed at mitigating such risks. (202)

Technical note on revised Article 25a

Key elements

The revised compromise on Article 25a empowers AMLA to: a) require selected obliged entities to adopt mitigating measures vis-à-vis individual non-EU institutions; b) adopt decisions addressed to financial supervisors to ensure that non-selected obliged entities adopt uniform mitigating measures in line with those identified by AMLA.

N.B. the powers granted to AMLA would ideally require an adaptation to the list of supervisory powers foreseen in AMLA Regulation, notably in Article 20, as well as in AMLD6, notably in Article 41, for supervisors towards non-selected obliged entities. Coordination with the AMLA NT would also be desirable to establish the mechanism foreseen in paragraph 5.

Detailed explanation

- Article 25a pursues the policy objective to preserve the Union's strategic autonomy to respond to specific ML/TF which may be posed by individual institutions established in countries which per

se do not present any strategic deficiencies or compliance weakness, nor they pose any specific threat to the Union at country level.

Differently from the US, the EU does not have as of today the tools to mitigate ML/TF risk from third countries at the level of the entity.

Under the US Patriot Act, financial institutions are required to apply enhanced due diligence measures to correspondent accounts established or maintained in the U.S with respect to other jurisdictions as well as financial institutions operating outside of the United States, in case of primary money laundering concern for the United States[15]. This power has been used in 2018 towards the Latvian bank ABLV, to prohibit the opening or maintaining of a correspondent account in the United States for, or on behalf of, ABLV[16]. See section 311 – with staged approach with draft proposed rulemaking on EDD re. third countries financial institutions https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

The lack of a similar tool in the Union legal order was highlighted by the European Court of Auditors in its 2021 Special Report. [See comparison between EU and US at page 55]

- In particular, Recommendation 1: The Commission should: (a) use greater prioritisation of sectors based on risk throughout the whole supranational risk assessment exercise [..]; (b) implement the new methodology to generate an autonomous EU third-country list; working in liaison with the EEAS and Member States to ensure integration of intelligence, and early communication with listed third countries; (c) put in place tools to mitigate ML/TF risk from third countries at the level of the entity or sector.

- The responsibility for assessing the risks posed by individual institutions is given to AMLA, rather than Commission, because AMLA will be the main EU body competent for monitoring ML/TF risks and threats emerging either from within the internal market or from outside the Union. The assessment of individual entities is based on specific criteria defined in level 1.

- Under paragraph 5, AMLA is empowered to adopt decisions addressed at national supervisors to ensure "non-selected obliged entities" are required to apply uniform mitigating measures in a coordinated manner. This power is crucial to ensure that AMLA and competent authorities are able to take effective action in coordinated manner at EU level, in exceptional situations where there is a specific and serious ML/TF threat that may affect the integrity of the Union's financial system and the functioning of the internal market.

- A similar mechanism to the one envisaged in paragraph 5 for AMLA is foreseen for the European Supervisory Authorities (EBA, ESMA, EIOPA) under the ESAs Regulation (Article 18 "Action in emergency situations"), whereby the ESAs are granted the power to adopt decisions addressed

[15] List of US rulemakings (see BPA or ABLV): https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures

[16] "FinCEN has reasonable grounds to believe that ABLV executives, shareholders, and employees have institutionalized money laundering as a pillar of the bank's business practices. [..] ABLV management permits the bank and its employees to orchestrate and engage in money laundering schemes; solicits the high-risk shell company activity that enables the bank and its customers to launder funds; maintains inadequate controls over high-risk shell company accounts; and seeks to obstruct enforcement of Latvian anti-money laundering and combating the financing of terrorism (AML/CFT) rules in order to protect these business practices. In addition, illicit financial activity at the bank has included transactions for parties connected to U.S. and UN-designated entities, some of which are involved in North Korea's procurement or export of ballistic missiles."

to national competent authorities to ensure a coordinated approach in case of adverse developments which may affect the integrity and orderly functioning of the Union's financial system.

- In particular, Article 18 of ESAs Regulation provides that: [...]"*in exceptional circumstances, where coordinated action by competent authorities is necessary to respond to adverse developments which may seriously jeopardise the orderly functioning and integrity of financial markets or the stability of the whole or part of the financial system in the Union or customer and consumer protection, the Authority may adopt individual decisions requiring competent authorities to take the necessary action in accordance with the legislative acts referred to in Article 1(2) to address any such developments by ensuring that financial institutions and competent authorities satisfy the requirements laid down in those legislative acts".*

- Moreover, the possibility for AMLA to adopt decisions addressed to national supervisors avoids the legal risks of the initial version of this compromise, which would have empowered AMLA to directly require measures with general applicability for all obliged entities in the Union.

Article 26: Guidelines on ML/TF risks, trends and methods

AMs Covered: 634 (S&D), 635 (Renew)

AMs Falling: 631 (Left), 632 (ID), 633 (ID), 636 (ID)

Article 26
Guidelines on ML/TF risks, trends and methods

1. By *[3 years from the date of entry into force of this Regulation]*, AMLA shall adopt guidelines defining the money laundering and terrorist financing trends, risks and methods involving any geographical area outside the Union to which obliged entities are exposed. AMLA shall take into account, in particular, the risk factors listed in Annex III. Where situations of higher risk are identified, the guidelines shall include enhanced due diligence measures that obliged entities shall consider applying to mitigate such risks.

2. AMLA shall review the guidelines referred to in paragraph 1 at least every two years.

3. In issuing and reviewing the guidelines referred to in paragraph 1, AMLA shall take into account evaluations, assessments or reports of ***EU bodies and agencies, and competent authorities,*** international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing (634, 365).

COMP S

Article 27 - Simplified customer due diligence measures,
Article 28 - Scope of application of enhanced customer due diligence measures

AMs covered: 71 (Rapporteurs), 72 (Rapporteurs), 73 (Rapporteurs), 639 (EPP), 640 (EPP), 641 (S&D), 644 (S&D), 645 (ID), 646 (ID), 647 (S&D), 648 (ID), 649 (ID), 650 (S&D, Greens), 651 (Renew), 652 (Greens), 654 (S&D), 662 (NI)

AMs falling: 637 (EPP), 638 (ID), 642 (ID), 643 (ID), 653 (ID), 655 (The Left), 656 (ID), 657 (EPP), 658 (EPP), 659 (EPP), 660 (ID), 661 (ID), 663 (EPP)

Recitals 45, 46

AMs covered:

AMs falling: 187 (ID)

Article 27

Simplified customer due diligence measures

1. Where, taking into account the risk factors set out in Annexes II and III, the business relationship or transaction present a low degree of risk, obliged entities may apply the following simplified customer due diligence measures:

   (a) verify the identity of the customer and the beneficial owner after the establishment of the business relationship, provided that the specific lower risk identified***, in the business-wide risk assessment and the customer risk assessment*** **(639),** justified such postponement but in any case no later than [~~30~~ ***60***] **days (640, 641)** of the relationship being established.

   (b) reduce the frequency of customer identification updates;

   (c) reduce the amount of information collected to identify the purpose and intended nature of the business relationship, or inferring it from the type of transactions or business relationship established ;

   (d) reduce the frequency or degree of scrutiny of transactions carried out by the customer;

   (e) apply any other relevant simplified due diligence measure identified by AMLA pursuant to Article 22.

   The measures referred to in the first subparagraph shall be proportionate to the nature**,** ***type of activity*** **(644, 645, 646**) and size of the business and to the specific elements of lower risk identified. However, obliged entities shall carry out sufficient monitoring of the transactions and business relationship to enable the detection of unusual or suspicious transactions.

   2. Obliged entities shall ensure that the internal procedures established pursuant to Article 7 contain the specific measures of simplified verification that shall be taken in relation to the different types of customers that present a lower risk. Obliged entities shall document decisions to take into account additional factors of lower risk.

3. For the purpose of applying simplified due diligence measures referred to in paragraph 1, point (a), obliged entities shall adopt risk management procedures with respect to the conditions under which they can provide services or perform transactions for a customer prior to the verification taking place, including by limiting the amount, number or types of transactions that can be performed or by monitoring transactions to ensure that they are in line with the expected norms for the business relationship at hand.

4. Obliged entities shall verify on a regular basis that the conditions for the application of simplified due diligence continue to exist. The frequency of such verifications shall be commensurate to the nature, ***type of activity*** **(647, 648, 649)** and size of the business and the risks posed by the specific relationship.

5. Obliged entities shall refrain from applying simplified due diligence measures in any of the following situations:

   (a) the obliged entities have doubts as to the veracity of the information provided by the customer or the beneficial owner at the stage of identification, or they detect inconsistencies regarding that information;

   (b) the factors indicating a lower risk are no longer present;

   (c) the monitoring of the customer's transactions and the information collected in the context of the business relationship exclude a lower risk scenario;

   (d) there is a suspicion of money laundering or terrorist financing.

   ~~(da) any of the circumstances set out in Articles 28, 31b, 32, 36 and 36a apply.~~ **~~(71)~~**

   (db) ~~there is a risk that~~ the customer~~,~~ or the beneficial owner is subject~~ed~~ to targeted financial sanctions or

   (dc) the customer is a family member~~s~~ or ~~any associated~~ a person known to be a ~~their~~ close associate~~s~~ of persons subject to targeted financial sanctions. **(650)**

Enhanced customer due diligence

Article 28

Scope of application of enhanced customer due diligence measures

1. In the cases referred to in Articles 23, 24, 25 and 30 to ***36b*** (651) as well as in other cases of higher risk that are identified by obliged entities pursuant to Article 16(2), second subparagraph ('cases of higher risk'), obliged entities shall apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.

2. Obliged entities shall examine the origin and destination of funds involved in, and the purpose of, all transactions that ***are atypical and may*** **(652)** fulfil at least one of the following conditions:

   (a) the transactions are of a complex nature;

   (b) the transactions are unusually large;

   (c) the transactions are conducted in an unusual pattern;

   (d) the transactions do not have an apparent economic or lawful purpose.

3. With the exception of the cases covered by Section 2 of this Chapter, when assessing the risks of money laundering and terrorist financing posed by a business relationship or occasional transaction, obliged entities shall take into account at least the factors of potential higher risk set out in Annex III and the guidelines adopted by AMLA pursuant to Article 26.

4. With the exception of the cases covered by Section 2 of this Chapter, in cases of higher risk, obliged entities ~~may~~ ***shall*** apply ~~any~~ ***at least one*** **(72, 654)** of the following enhanced customer due diligence measures, proportionate to the higher risks identified:

(a) obtain additional information on the customer and the beneficial owner(s);

(b) obtain additional information on the intended nature of the business relationship;

(c) obtain additional information on the source of funds, and source of wealth of the customer and of the beneficial owner(s);

(d) obtain information on the reasons for the intended or performed transactions and their consistency with the business relationship;

(e) obtain the approval of senior management for establishing or continuing the business relationship;

(f) conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;

(g) require the first payment to be carried out through an account in the customer's name with a credit institution subject to customer due diligence standards that are not less robust than those laid down in this Regulation.

5. With the exception of the cases covered by Section 2 of this Chapter, where Member States identify pursuant to Article 8 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final] cases of higher risk, they may require obliged entities to apply enhanced due diligence measures and, where appropriate, specify those measures. Member States shall notify to the Commission and AMLA the enhanced due diligence requirements imposed upon obliged entities established in their territory within one month of their adoption, accompanied by a justification of the money laundering and terrorist financing risks underpinning such decision.

Where the risks identified by the Member States pursuant to the first subparagraph are likely to affect the financial system of the Union, AMLA shall, upon a request from the Commission or on its own initiative, consider updating the guidelines adopted pursuant to Article 26 or, ***if deemed more appropriate, issue draft regulatory technical standards to impose*** enhanced due diligence requirements upon obliged entities ***uniformly in the EU and submit them to the Commission for adoption***.

5a. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 of this Article in accordance with Articles 38 to 41 of Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final].

~~6. Enhanced customer due diligence measures shall not be invoked automatically with respect to branches or subsidiaries of obliged entities established in the Union which are located third countries referred to in Articles 23, 24 and 25 where those branches or subsidiaries fully comply with the group-wide policies, controls and procedures in accordance with Article 14.~~ (73, 662)

COMP T

Article 29 - Countermeasures to mitigate ML/TF threats from outside the Union

AMs covered: 74 (Rapporteurs), 75 (Rapporteurs), 664 (S&D), 668 (EPP), 669 (EPP), 670 (EPP), 671 (EPP), 675 (ECR)

AMs falling: 665 (EPP), 666 (EPP), 667 (EPP), 672 (Greens/EFA), 673 (EPP), 674 (Left)

Article 29

Countermeasures to mitigate ML/TF threats from outside the Union

1. For the purposes of Articles 23 and 25, the Commission ***shall*** choose from among the following countermeasures: (74, 664)

   (a) countermeasures that obliged entities are to apply to persons and legal entities involving high-risk third countries and, where relevant, other countries posing a threat to the Union's financial system consisting in:

   (i) the application of additional elements of enhanced due diligence;

   (ii) the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;

   (iii) the limitation of business relationships or transactions with natural persons or legal entities from those third countries;

   (b) countermeasures that Member States are to apply with regard to high-risk third countries and, where relevant, other countries posing a threat to the Union's financial system consisting in:

   (i) refusing the establishment of subsidiaries or branches or representative offices of obliged entities from the country concerned, or otherwise taking into account the fact that the relevant obliged entity is from a third country that does not have adequate AML/CFT regimes;

   (ii) prohibiting obliged entities from establishing branches or representative offices of obliged entities in the third country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a third country that does not have adequate AML/CFT regimes;

   (iii) requiring increased supervisory examination or increased external audit requirements for branches and subsidiaries of obliged entities located in the third country concerned;

   (iv) requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the third country concerned;

   (v) requiring credit and financial institutions to review and amend, or if necessary terminate, correspondent relationships with respondent institutions in the third country concerned.

1a. In addition to the countermeasures chosen under this Article for the purposes of Articles 23 and 25, Member States shall not grant residence status to nationals of countries designated under Article 23, 24 or 25 on the basis of national schemes that

grant citizenship or residence rights in exchange for any kind of investments, including capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget. **(75, 675)**

COMP U

Article 30 - Specific enhanced due diligence measures for cross-border correspondent relationships

Article 30a - Specific enhanced due diligence measures for correspondent relationships with non-EU entities providing crypto-asset services

Article 30b - Specific enhanced due diligence regarding transactions involving self hosted wallets

AMs covered: 76 (Rapporteurs), 77 (Rapporteurs), 78 (Rapporteurs), 134 (Greens/EFA), 676 (EPP), 677 (Greens/EFA, S&D), 695 (Greens/EFA)

Article 30

Specific enhanced due diligence measures for cross-border correspondent relationships

1. With respect to cross-border correspondent relationships, including relationships established for securities transactions or fund transfers , involving the execution of payments with a third-country respondent institution, in addition to the customer due diligence measures laid down in Article 16, credit institutions and financial institutions shall be required, when entering into a business relationship, to: (76)

   (a) gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

   (b) assess the respondent institution's AML/CFT controls;

   (c) obtain approval from senior management before establishing new correspondent relationships;

   (d) document the respective responsibilities of each institution;

   (e) with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent institution, and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

   Where credit institutions and financial institutions decide to terminate cross-border correspondent relationships for reasons relating to anti-money laundering and counter-terrorist financing policy, they shall document their decision.

Article 30a

Specific enhanced due diligence measures for correspondent relationships with non-EU entities providing crypto-asset services

1. With respect to correspondent cross-border relationships involving the execution of crypto-asset services as defined in MiCA with a respondent entity not established in the EU and providing similar services, including transfers of crypto-assets, crypto-asset service providers shall, in addition to the customer due diligence measures laid down in Article 16, be required when entering into a business relationship, to:

> ***(a) determine that the respondent entity is registered or licenced under the law of a third country;***
> ***(b) gather sufficient information about the correspondent entity to understand fully the nature of the respondent institution's business and to determine from publicly available information the reputational risk of the entity and the quality of supervision;***
> ***(c) assess the respondent entity's AML/CFT controls;***
> ***(d) obtain approval from senior management before establishing the correspondent relationship;***
> ***(e) document the respective responsibilities of each party to the correspondent relationship;***
> ***(f) with respect to payable-through crypto-asset accounts, be satisfied that the respondent entity has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent entity, and that it is able to provide relevant customer due diligence data to the correspondent entity, upon request. Where crypto-asset service providers decide to terminate correspondent relationships for reasons relating to anti-money laundering and counter-terrorist financing policy, they shall document and record their decision.***

Crypto-asset service providers shall update the due diligence information for the correspondent relationship on a regular basis or when new risks emerge in relation to the respondent entity.

2. Crypto-asset service providers shall take into account the information referred to in the first paragraph in order to determine, on a risk sensitive basis, the appropriate enhanced due diligence measures required to mitigate the risks associated with the respondent entity.

3. By [2 years from the date of entry into force of this Regulation], AMLA shall, after consulting the EBA, adopt guidelines specifying the criteria and elements that crypto-asset services providers shall take into account for conducting the assessment referred to in paragraph 1 and the risk mitigating measures referred to in paragraph 2, including the variables and risk factors criteria to be taken into account to assess the level of risk associated with a particular category of crypto-asset service provider. **(677)**

Article 30b

Specific enhanced due diligence regarding crypto-assets transactions involving a self-hosted address

1. In addition to the customer due diligence measures laid down in Article 16, and without prejudice to the measures required by Regulation [please insert reference – proposal for a recast of Regulation (EU) 2015/847 - COM/2021/422 final], crypto-asset service providers

shall have in place appropriate risk management systems, including risk-based procedures, to identify and assess the risk of money laundering and financing of terrorism as well as the risk of non-implementation or evasion of targeted financial sanctions associated with crypto-assets transactions directed to or originating from a self-hosted address.

2. With respect to such transactions, crypto-asset service providers shall apply mitigating measures commensurate with the risks identified. Those mitigating measures shall include:

> ***(a) taking risk-based measures to verify through suitable technical means whether the self-hosted address is owned or controlled by their customers;***
>
> ***(b) taking risk-based measures to identify, and verify the identity of the person who owns or controls or benefits from a self-hosted address, to the extent possible outside the framework of a customer relationship, including through reliance on third party verification;***
>
> ***(c) requiring additional information on the origin and destination of the crypto-assets, in accordance with a risk based approach;***
>
> ***(d) conducting enhanced monitoring of those transactions, in accordance with a risk based approach;***
>
> ***(e) any other risk-based measure to mitigate and manage the risks of money laundering and financing of terrorism as well as the risk of non-implementation and evasion of targeted financial sanctions and proliferation financing-related targeted financial sanctions.***

Where the identification and verification is not technically feasible, crypto-asset service providers shall apply appropriate alternative measures to mitigate and manage the risks of money laundering and financing of terrorism as well as the risk of non-implementation or evasion of targeted financial sanctions, in accordance with regulatory technical standards referred to in paragraph 3.

3. By [2 years from the date of entry into force of this Regulation], AMLA shall issue draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall be developed taking into account of technological developments and shall specify the following:

> ***(a) the criteria and means for the identification and verification of a self-hosted address, whether or not it is owned or controlled by a customer, including criteria for secure and trusted means of electronic identification and verification performed by third parties;***
>
> ***(b) alternative risk-mitigating measures to be applied where the verification of a self-hosted address owned or controlled by a third party is not technically feasible outside of a customer relationship;***
>
> ***(c) other enhanced due diligence measures associated with the level of risk posed by transactions with a self-hosted address.***

4. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 of this Article in accordance with Articles 38 to 41 of Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]. (695)

Recital 48a

(48a) Self-hosted addresses ~~wallets~~ enable their users to receive, send and exchange crypto-assets across the world, without revealing their identity or being subject to any customer due diligence measures. While transactions recorded on the distributed ledger can be traced back to a particular self-hosted address, it may be very difficult or impossible to link such address to a real person. For this reason, self-hosted addresses ~~wallets~~ may be misused to conceal criminal activities or circumvent targeted financial sanctions. In order to manage and mitigate those risks appropriately, crypto-asset service providers should be required to establish, to the extent possible, the identity of the originator or beneficiary of a transaction made from or to a self-hosted wallet and apply any additional enhanced due diligence measures adequate to the level of risk identified. Crypto-asset service providers can rely on secure and trusted means of verification performed by third parties. The verification requirement should not be interpreted as implying onboarding the person who owns or controls the self-hosted address as customer. In order to ensure consistent application of this Regulation, AMLA should be tasked with drawing up draft regulatory technical standards to specify, taking into account of the latest technological developments, the criteria and means for the identification and verification of the originator or beneficiary of a transaction with a self-hosted wallet.

COMP V

Article 31 - Prohibition of correspondent relationships with shell banks

Article 31a - Prohibition of correspondent relationships with unregistered and unlicensed entities providing crypto-asset services
Article 31b - Public register on shell banks and unregistered and unlicensed entities providing crypto-asset services
Article 31c - Specific provisions regarding applicants for citizenship and residence by investment schemes

AMs covered: 79 (Rapporteurs), 80 (Rapporteurs), 81 (Rapporteurs), 678 (Greens/EFA, S&D), 679 (ID), 680 (ID), 681 (ID), 682 (ID), 683 (ID)

Recital 47
AMs covered: 10 (Rapporteurs), 188 (S&D)

Article 31
Prohibition of correspondent relationships with shell banks
Credit institutions and financial institutions shall not enter into, or continue, a correspondent relationship with a shell bank. Credit institutions and financial institutions shall take appropriate measures to ensure that they do not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank.

Article 31a

Prohibition of correspondent relationships with unregistered or unlicensed entities providing crypto-asset services

Credit and financial institutions shall not enter into or continue a correspondent relationships with unregistered and unlicensed entities providing crypto-asset services. Credit and financial institutions shall take appropriate measures to ensure that they do not engage in or continue correspondent relationships with an entity that is known to allow its accounts or distributed ledger addresses to be used by an unregistered or unlicensed entity providing crypto-asset services. **(79, 678, 679, 680)**

[to be added to ***Article 2 (20a):***
'unregistered or unlicenced entity providing crypto-asset services' means an entity which provides crypto-asset services and that is not established in any jurisdiction or does not have a central contact point or substantive management presence in any jurisdiction (25, 280)]

Article 31b

Public register on shell banks and unregistered and unlicensed entities providing crypto-asset services

1. Where competent authorities, supervisors or obliged entities become aware of shell banks and unregistered and unlicensed crypto-asset service providers operating within or outside the Union, they shall inform AMLA.

2. AMLA shall set up and maintain an indicative and non-exhaustive public register of shell banks and unregistered and unlicensed entities providing crypto-asset services based on information which may be provided by competent authorities, supervisors, obliged entities and any additional information at its disposal. The register shall be publicly available in machine-readable format.

3. AMLA shall update the public register referred to in paragraph 2 on a regular basis, taking into account any changes in circumstances concerning the entities included in the list or any information brought to its attention. **(80, 678, 681, 682, 683)**

Article 31c

Specific provisions regarding applicants for citizenship and residence by investment schemes

In addition to the customer due diligence measures laid down in Article 16, with respect to customers who are third-country nationals who apply for residence rights in a Member State in exchange for any kind of investment, including transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget, obliged entities shall, as a minimum, carry out enhanced customer due diligence measures as set out in Article 28 (4), points (a) (c) (e) and (f). **(81)**

[*agreed at technical level to introduce a ban on CBI schemes in Chapter 1*]

Recital 47

(47) Cross-border correspondent relationships with a third-country's respondent institution are characterised by their on-going, repetitive nature. Moreover, not all cross-border correspondent banking services present the same level of money laundering and terrorist financing risks. Therefore, the intensity of the enhanced due diligence measures should be determined by application of the principles of the risk based approach. However, the risk based approach should not be applied when interacting with third-country's respondent institutions that have no physical presence where they are incorporated ***or with unregistered and unlicensed entities providing crypto-asset services***. Given the high risk of money laundering and terrorist financing inherent in shell banks ***and unregistered and unlicensed entities***, credit institutions and financial institutions should refrain from entertaining any correspondent relationship with such shell banks ***and with unregistered and unlicensed entities providing crypto-asset services. In order to facilitate compliance by obliged entities, AMLA should establish and maintain a non-exhaustive public register of entities identified as shell banks or unregistered or unlicensed crypto-asset service providers on the basis of information submitted by competent authorities, supervisors and other obliged entities. The inclusion of a specific entity in the public register is merely indicative and should not replace the obligation on obliged entities to take adequate and effective measures to comply with the prohibition on entering into a correspondent relationship with those entities.*** (10, 188)

COMP W
Articles 32, 33, 35 - Specific provisions regarding politically exposed persons

AMs covered: 82 (Co-rapporteurs), 690 (Renew), 691 (EPP), 701 (EPP), 703 (S&D, Greens)

AM falling: 686 (EPP), 692 (ID), 694 (Greens), 696 (ID), 697 (EPP), 698 (Renew), 699 (ID), 700 (ID), 702 (ID)

Recitals 55, 57, 59

AMs covered: 205 (S&D), 206 (ID), 207 (ID)

AMs falling: 204 (ID), 208 (ID)

Article 32

Specific provisions regarding politically exposed persons

1. In addition to the customer due diligence measures laid down in Article 16, obliged entities shall have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a politically exposed person.

2. With respect to transactions or business relationships with politically exposed persons, obliged entities shall apply the following measures:

(a) obtain senior management approval for establishing or continuing business relationships with politically exposed persons**;**

(b) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or ***occasional*** **(690, 691)** transactions with politically exposed persons***;***

(c) conduct enhanced, ongoing monitoring of those business relationships.

3. By *[~~3~~ **2** (**82**) years from the date of entry into force of this Regulation]*, AMLA shall issue guidelines on the following matters:

(a) the criteria for the identification of persons falling under the definition of persons known to be a close associate;

(b) the level of risk associated with a particular category of politically exposed person, their family members or persons known to be close associates, including guidance on how such risks are to be assessed after the person no longer holds a prominent public function for the purposes of Article 35.

Article 33

List of prominent public functions

1. Each Member State shall issue and keep up to date a list indicating the exact functions which, in accordance with national laws, regulations and administrative provisions, qualify as prominent public functions for the purposes of Article 2, point (25). Member States shall request each international organisation accredited on their territories to issue and keep up to date a list of prominent public functions at that international organisation for the purposes of Article 2, point (25). These lists shall also include any function which may be entrusted to representatives of third countries and of international bodies accredited at Member State level. Member States shall notify those lists, as well as any change made to them, to the Commission and to AMLA.
2. The Commission shall draw up and keep up to date the list of the exact functions which qualify as prominent public functions at the level of the Union. That list shall also include any function which may be entrusted to representatives of third countries and of international bodies accredited at Union level.
3. The Commission shall assemble, based on the lists provided for in paragraphs 1 and 2 of this Article, a single list of all prominent public functions for the purposes of Article 2, point (25). The Commission shall publish that single list shall in the *Official Journal of the European Union*. AMLA shall make the list public on its website.

Article 34

Politically exposed persons who are beneficiaries of insurance policies

Obliged entities shall take reasonable measures to determine whether the beneficiaries of a life or other investment-related insurance policy or, where relevant, the beneficial owner of the beneficiary are politically exposed persons. Those measures shall be taken no later than at the time of the payout or at the time of the assignment, in whole or in part, of the policy. Where there are higher risks identified, in addition to applying the customer due diligence measures laid down in Article 16, obliged entities shall:

(a) inform senior management before payout of policy proceeds;
(b) conduct enhanced scrutiny of the entire business relationship with the policyholder.

Article 35

Measures towards persons who cease to be politically exposed persons

1. Where a politically exposed person is no longer entrusted with a prominent public function by the Union, a Member State, third country or an international organisation, obliged entities shall take into account the continuing risk posed by that person in their assessment of money laundering and terrorist financing risks in accordance with Article 16.
2. Obliged entities shall apply one or more of the measures referred to in Article 28 (4) to mitigate the risks posed by the business relationship. ***Obliged entities shall apply these measures in a manner proportionate to the risks identified*** until such time as that person is deemed to pose no further risk, but in any case for not less than ***24*** ~~12~~ months following the time when the individual is no longer entrusted with a prominent public function. ***(700, 701, 702, 703)***
3. The obligation referred to in paragraph 2 shall apply accordingly where an obliged entity enters into a business relationship with a person who in the past was entrusted with a prominent public function by the Union, a Member State, third country or an international organisation.

Recitals 55, 57, 59

(55) Relationships with individuals who hold or who have held important public functions, within the Union or internationally, and particularly individuals from countries where corruption is widespread, may expose the financial sector to significant reputational and legal risks. The international effort to combat corruption also justifies the need to pay particular attention to such persons and to apply appropriate enhanced customer due diligence measures with respect to persons who are or who have been entrusted with prominent public functions and with respect to senior figures in international organisations. Therefore, it is necessary to specify measures which obliged entities should apply with respect to transactions or business relationships with politically exposed persons. To facilitate the risk-based approach, AMLA should be tasked with issuing guidelines on assessing the level of risks associated with a particular category of politically exposed persons, their family members or persons known to be close associates.

(57) When customers are no longer entrusted with a prominent public function, they can still pose a higher risk, for example because of the informal influence they could still exercise, or because their previous and current functions are linked. It is essential that obliged entities take into consideration those continuing risks and apply one or more enhanced due diligence measures until such time that the individuals are deemed to pose no further risk, and in any case for not less than ***24*** ~~***12***~~ months following the time when they are no longer entrusted with a prominent public function. ***(205, 206, 207)***

(59) Close private and professional relationships can be abused for money laundering and terrorist financing purposes. For that reason, measures concerning politically exposed persons should also apply to their family members and persons known to be close associates. Properly identifying family members and persons known to be close associates may depend on the socio-economic and cultural structure of the country of the politically exposed person. Against this background, AMLA should have the task of issuing guidelines on the criteria to use to identify persons who should be considered as close associate.

COMP X

Article 36a - Specific provisions regarding certain high-net-worth customers

AMs covered: 83 (Co-rapporteurs), 684 (The Left), 685 (The Left), 687 (The Left), 688 (The Left), 689 (The Left), 693 (The Left), 705 (S&D, Greens), 706 (ID)

Article 36b- Specific provisions regarding offshore financial centres

AM covered: 694 (Greens)

Recitals 60a
AMs covered: 12 (Co-rapporteurs), 209 (Renew), 210 (ID)

Article 36a

Specific provisions regarding certain high-net-worth customers

1. In addition to the customer due diligence measures laid down in Article 16, obliged entities shall have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a high risk high-net-worth ~~customer~~ individual ~~who ostensibly presents high risk factors referred to in Annex III, Article 1 (ba)~~.

2. ~~Obliged entities other than those referred to in Article 3 (3) (b)~~, A customer whose wealth derives from the extractive industry ~~the extraction of natural resources~~, or from ~~reported~~ links with politically exposed persons, or from the exploitation of monopolies in third countries identified by credible sources/acknowledged processes as having significant levels of corruption or other criminal activity (120, 122) shall be considered to be a high-risk high-net-worth individual ~~in accordance with~~ where ~~shall determine whether the customer is a high risk high-net-worth customer individual in accordance with taking into account the following~~:

a) obliged entities other than those referred to in Article 3 (3) (b):

i) have a business relationship with that customer that exceeds EUR 1 000 0000, calculated on the basis of the customer's financial or investable wealth or assets either under management by the obliged entity or relating to which the obliged entity offers material aid, assistance or advice, excluding the customer's main

private residence, regardless of whether that amount is reached at the time of establishment of the business relationship or ~~after~~ in the course of one year; or

ii) perform an occasional transaction, or offer material aid, assistance or advice relating to an occasional transaction for that customer that exceeds-EUR 1 000 0000;

b) obliged entities referred to in Article 3 (3) (b):

(i) act on behalf of and for that customer in any business relationship or occasional transaction which exceeds EUR 1 000 000; or

(ii) when they assist in the planning or carry out transactions for those customers which, alone or combined in the course of a business relationship which extends over one year, exceeds EUR 1 000 000.

4. Without prejudice to paragraphs 2 and 3, for the purposes of paragraph 1, obliged entities shall also consider information obtained as part of the customer due diligence process and ongoing monitoring of transactions in accordance with this Chapter or any other relevant information at their disposal.

5. For the purpose of this Article, ~~extraction of natural resources~~ extractive industry means any activity involving the exploration, prospection, discovery, development, and extraction of minerals, oil, natural gas deposits or other materials, within the economic activities listed in Section B, Divisions 05 to 08 of Annex I to Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Revision 2, as referred to in Article 41 (1) of Directive 2013/34.

6. With respect to transactions or business relationships with high risk high-net-worth customers who present high risk factors as referred to in paragraph 1, obliged entities shall apply the following enhanced due diligence measures:

(a) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or occasional transactions with those customers and determine to the extent possible ~~be satisfied~~ that the business relationships or transactions are not linked to money laundering, predicate offences or terrorist financing in accordance with EU law, whether committed ~~practiced~~ in the EU or in third countries;

(b) obtain senior management approval for establishing or continuing business relationships with those customers as well as for carrying out occasional transactions with those customers;

(c) conduct enhanced, ongoing monitoring of business relationships with those customers. (83, 684, 685, 687, 688, 689, 693, 705, 706)

[definition to be included in Chapter 1, Article 2 (27a):]

Article 2 (27a)

(27a) 'high-net-worth customer' means a customer who is a natural person or the beneficial owner of a legal entity that holds in total a minimum of EUR 1 000 000 in financial or investable wealth or assets, excluding that person's main private residence, in accordance with the criteria laid down in this Regulation.]

Recital 60a

(60a) Business relationships and occasional transactions involving high-net-worth customers who present one or several factors of high risk could seriously compromise the integrity of the Union's financial system and cause serious vulnerabilities in the internal market. Obliged entities should therefore determine on a risk-sensitive basis whether the customer or the beneficial owner of the customer is a high-risk high net worth individual in the course of due diligence procedures. Where an obliged entity identifies that a customer or the beneficial owner of a customer is a high-risk high net worth individual, it shall apply specific enhanced customer due diligence measures as laid down in this Regulation with respect to those customers. (12, 209, 210)

Article 36b
Specific provisions regarding offshore financial centres

1. In addition to the customer due diligence measures laid down in Article 16 and without prejudice to any stricter measures applicable under Section 2, obliged entities shall have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a ~~company~~ legal entity established or having a substantial link with ~~an~~ a jurisdiction designated by AMLA as an offshore financial centre.

2. With respect to transactions or business relationships with legal entities ~~companies~~ established or having a substantial link with ~~registered in~~ an offshore financial centre, obliged entities shall apply the following measures, on a risk sensitive basis:

(a) gather sufficient information about the ~~company~~ legal entity to understand fully the nature of the ~~company's~~ business of that entity;

b) obtain senior management approval for establishing or continuing business relationships with that ~~company~~ legal entity;

(c) take adequate measures to establish the source of funds that are involved in business relationships or transactions with the ~~company~~ legal entity;

(c) conduct enhanced, ongoing monitoring of those business relationships.

3. AMLA shall develop draft ~~implementing~~ regulatory technical standards to specify what constitutes a substantial link as referred to in paragraph 1 and further specify ~~the offshore financial centres referred to in paragraph 1 and further specify the criteria for their identification,~~ the criteria for the identification of offshore financial centres as defined in Article 2, taking into account:

a) the inclusion in the Annex I of the Council conclusions on the EU list of non-cooperative jurisdictions for tax purposes;
~~a~~b) ~~the level~~ the provision of financial secrecy, as identified by credible sources/ acknowledged processes;
~~b) the lack of effective exchange of information;~~
c) the absence of minimum substance requirements for legal entities ~~a requirement for substantial activities~~;
~~d) the lack of due diligence on the creation of companies;~~
~~e) the lack of availability of accurate and timely information on beneficial ownership of legal persons and arrangements to competent authorities;~~
~~f) the level of risk of anti-money laundering and terrorist financing risk associated with different types of offshore jurisdictions.~~

AMLA shall develop draft <u>implementing</u> technical standards to specify the offshore financial centres identified in accordance with the criteria referred to in paragraph 3.

AMLA shall adopt those <u>draft implementing</u> technical standards and submit them to the Commission for adoption by [2 years from the date of entry into force of this Regulation].

Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulation (EU) No 1095/2010. (694)

AMLA shall review list of offshore financial centres regularly the regulatory technical standards on a regular basis and at least every two years and submit proposals for amendments to the Commission.

4. For the purpose of paragraph 3, AMLA shall also take into account the relevant lists and definitions of offshore financial centres adopted by international organisations and standard setters as well as relevant evaluations, assessments, reports or public statements drawn up by them.

AMLA shall adopt those technical standards by [2 years from the date of entry into force of this Regulation] and submit them to the Commission for adoption.
Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulation (EU) No 1095/2010. (694)

Technical Note to shadows:

This provision intends to increase attention towards companies operating in offshore financial centres. The inclusion in the list does not trigger any countermeasure, such as the limitation of business relationship or systematic reporting which may be required under third country policy. It would instead trigger some elements of enhanced due diligence measures, on a risk basis, such as gathering information on the nature of the business, approval of senior management, understanding the source of funds (to detect any illicit financial flows) and monitoring.

The provisions would only apply to legal companies and arrangements, not to natural persons based in the offshore centres.

Various lists and definitions of offshore financial centres have been developed at international and European level (IMF, BIS, FSB, Eurostat). Such lists have a different scope compared to the FATF blacklist/grey list although they may overlap in specific cases. An offshore financial centre may indeed not qualify per se as a high-risk jurisdiction. Nevertheless, companies linked with offshore financial centres often pose higher risks of money laundering and other illegal activities.

This was exposed in particular by a series of investigations from Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers and Offshore Leaks.

The PANA Committee of the European Parliament had published a study addressing the link between money laundering and offshore financial centres (link).

Europol called for introducing specific provisions in the AMLR to address the risks of companies located in offshore financial centres.

COMP Y

Annex I - Indicative list of risk variables

Annex II - Lower risk factors

Annex III - Higher risk factors

AMs covered: 120 (co-rapporteurs), 121 (co-rapporteurs), 122 (co-rapporteurs), 166 (S&D, Renew, Greens), 962 (Greens), 965 (Greens), 966 (S&D), 968 (Greens), 969 (Greens), 970 (Greens), 971 (EPP), 972 (Greens), 974 (Greens), 976 (Greens), 980 (Greens)

AMs falling: 118 (co-rapporteurs), 119 (co-rapporteurs), 952 (The Left), 953 (The Left), 954 (The Left), 955 (The Left), 956 (EPP), 957 (EPP), 958 (The Left), 959 (The Left), 960 (The Left), 961 (The Left), 963 (The Left), 964 (EPP), 967 (ID), 973 (EPP), 975 (The Left), 977 (The Left), 978 (Greens), 979 (The Left), 981 (The Left), 982 (The Left),

ANNEX I

Indicative list of risk variables

The following is a non-exhaustive list of risk variables that obliged entities shall take into account when drawing up their risk assessment in accordance with Article 8 determining to what extent to apply customer due diligence measures in accordance with Article 16:

(a) Customer risk variables:

(i) the customer's and the customer's beneficial owner's business or professional activity;

(ii) the customer's and the customer's beneficial owner's reputation;

(iii) the customer's and the customer's beneficial owner's nature and behaviour;

(iv) the jurisdictions in which the customer and the customer's beneficial owner are based;

(v) the jurisdictions that are the customer's and the customer's beneficial owner's main places of business;

(vi) the jurisdictions to which the customer and the customer's beneficial owner have relevant personal links;

(b) Product, service or transaction risk variables:

(i) the purpose of an account or relationship;

(ii) the regularity or duration of the business relationship;

(iii) the level of assets to be deposited by a customer or the size of transactions undertaken;

(iv) the level of transparency, or opaqueness, the product, service or transaction affords;

(v) the complexity of the product, service or transaction;

(vi) the value or size of the product, service or transaction.

(c) Delivery channel risk variables:

(i) the extent to which the business relationship is conducted on a non-face-to-face basis;

(ii) the presence of any introducers or intermediaries that the customer might use and the nature of their relationship with the customer;

(d) Risk variable for life and other investment-related insurance:

(i) the risk level presented by the beneficiary of the insurance policy.

ANNEX II

Lower risk factors

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Article 16:

(1) Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

(b) public administrations ~~or enterprises~~ **(118)**;

(c) customers that are resident in geographical areas of lower risk as set out in point (3);

(2) Product, service, transaction or delivery channel risk factors:

(a) life insurance policies for which the premium is low;

(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;

(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);

(3) Geographical risk factors — registration, establishment, residence in:

(a) Member States;

(b) third countries having effective AML/CFT systems;

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;

(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

ANNEX III

Higher risk factors

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 16:

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;

(b) customers that are resident in geographical areas of higher risk as set out in point (3);

(ba) customers who are high-net-worth individuals or whose beneficial owner is a high-net-worth individual whose wealth derives prominently from the extractive industry ~~extraction of natural resources~~, or from links with politically exposed persons or from the exploitation of monopolies in third countries identified by credible sources/ acknowledged processes as having significant levels of corruption or other criminal activity; (120, 122)

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies ***or other legal entities*** that have nominee shareholders or shares in bearer form ***or fiduciary deposits***; **(962)**

(e) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex or ***~~constructed in such a way to conceal beneficial ownership~~,*** given the nature of the company's business; **(965)**

(g) customer is a third country national who applies for ***~~citizenship or~~*** **(121, 966)** residence rights in a Member State in exchange of any kind of investment, including capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget;

(d) customer is subject to sanctions, embargos or similar measures issued by international organisations, such as the United Nations;

(d) third countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

Recital 24a (new)

(24a) Sanctions adopted by the Union Nations are relevant risk factors for money laundering, predicate offences and terrorism financing since they aim to address threats of terrorism and terrorism financing, crimes related to human rights violations and proliferation of nuclear weapon of mass destruction. Therefore, appropriate risk-mitigating measures need to be taken in high-risk situations in that regard, without prejudice to the application of rule-based obligations imposed under the EU targeted financial sanctions regime; (166)

Technical note
Addition of a customer factor in relation to UN sanctions, mirroring the geographical risk factor in point (3) to take into account the element of risk/suspicion emanating from the listing grounds which relate to ML/TF, terrorism or predicate offences. This would ensure that there is a clear basis in Union legislation for introducing a reporting obligations in relation to persons subject to UN sanctions, in accordance with Article 36c as redrafted.

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity, ***including crypto-assets which have inbuilt anonymisation*** ~~***anonymity-enhanced cryptocurrency (AEC) or privacy coins***~~ **(968);**

(ba) ~~***use of anonymising services and tools, including***~~ ***privacy wallets, mixers and tumblers*** ~~***as well as Internet Protocol (IP) anonymizers such as The Onion Router (Tor), the Invisible Internet Project (I2P)***~~ ***and other anonymizing software or techniques used for obfuscating transactions; (969)***

(bc) ***crypto-ATMs (974)***

(c) payment ***or transfers of assets (970)*** received from unknown or unassociated third parties;

~~(d) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;~~ **(971)**

(e) transactions related to oil, arms, precious metals ***and stones,*** **(972)** tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species;

(2a) Counterpart risk factors:

(a) transactions in crypto assets from or to self-hosted ~~***wallets***~~ ***address whose owner cannot be identified, unregistered or unlicensed entities providing crypto assets services and decentralised applications or*** ~~***other***~~ ***similar arrangements to the extent they do not*** ~~***perform***~~ ***qualify as crypto-assets service providers covered under the MiCA Regulation;***

(b) entities identified as not applying minimum customer due diligence procedures;

(c) entities identified by credible sources/acknowledged process, as having strong connections and links to money laundering, terrorist financing and other illegal activities, including dark-net marketplaces, ransomware and hacking;

Technical note

Decentralised applications or organisations can be easily misused for money laundering and sanctions evasion.

The COM Supranational Risk Assessment addresses the higher risk of Defi.

In addition, a study by Chainalysis revealed that the total annual value of laundered cryptocurrency jumped 30% in 2021 for DeFI and there is evidence AML risk is on a rising trend.

These are the main reasons why they should be considered high risk:

there are no intermediaries, meaning none is conducting KYC/AML checks;

there are many regulatory challenges, no jurisdiction in the world has yet managed to come up with a regulatory framework;

very easy to cash out - the application can be accessed by anyone, anywhere, anytime;

DeFI is used to obfuscate source of funds from blockchain analytics.

DeFI does not fall under the scope of crypto-assets services providers to the extent it is fully decentralised and operated without any intermediary. Therefore there is no identified body that is responsible for compliance and checks. There won't be any regulation soon for DeFI.

(3) Geographical risk factors:

(a) third countries subject to increased monitoring or otherwise identified by the FATF due to the compliance weaknesses in their AML/CFT systems;

(aa) third countries included in the Annex I ~~and Annex II~~ of the EU list of non-cooperative jurisdictions for tax purposes; (976)

(b) third countries identified by credible sources/ acknowledged processes, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

(c) third countries identified by credible sources/ acknowledged processes as having significant levels of corruption or other criminal activity;

(ca) third countries identified by credible sources/acknowledged and verifiable processes as ~~favouring~~ offering high levels of financial secrecy ~~such as offshore centres~~; (980)

(d) third countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

(e) third countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

COMP Z

Article 36c - Persons subject to restrictive measures by international organisations

Article 37a - Monitoring of transactions with regard to risks posed by targeted financial sanctions

AMs covered: 704 (S&D, Renew, Greens), 707 (S&D, Renew, Greens)

Article 36c

Persons subject to restrictive measures by international organisations

1. Obliged entities shall report to the ~~competent~~ FIUs where they detect any business relationship or occasional transaction with persons subject to UN sanctions as referred in Annex III point (1) (d) in the temporary period between the moment the UN designation is made publicly available and the moment targeted financial sanctions adopted by the Union become applicable.

In the circumstances referred to in the first subparagraph, obliged entities shall refrain from carrying out any transaction related to a person subject to UN sanctions until they have notified the ~~competent~~ FIU and have complied with any further specific instruction from the FIU.

2. When the FIU receives such a notification referred to in paragraph 1, it may ~~shall decide to~~ suspend any transaction or ~~withhold its consent or suspend~~ any account in accordance with Article 20 of Directive [insert reference to AMLD6] ~~up to 10 calendar days or until the adoption of targeted financial sanctions by the Union.~~

3. This Article is without prejudice to the possibility of Member States to apply temporary measures which ensure a higher level of protection of the financial system of the Union such as temporary measures applying directly UN designations pending the adoption of EU targeted financial sanctions. **(704)**

Article 37a

Monitoring of transactions with regard to risks posed by targeted financial sanctions

1. Without prejudice to any other measures required by Union law relating to targeted financial sanctions, credit and financial institutions ~~and crypto-asset service providers~~ shall screen the information accompanying a transfer of funds or crypto-assets pursuant to [please insert reference – Regulation on information accompanying transfers of funds and certain crypto-assets (Recast)] in order to assess whether the payee or the payer of a funds transfer, or the originator or the beneficiary of a transfer of crypto-assets, are subject to targeted financial sanctions.

By [2 years after the entry into force of this Regulation] AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption.

Those draft regulatory technical standards shall specify:

(a) which information shall be screened by the credit or financial institution of the payer as well as the relevant obligations of this institution;

(b) which information shall be screened by the credit or financial institution of the payee as well the relevant obligations of this institution;

~~***(c) which information shall be screened by the crypto-asset service provider of the originator as well the relevant obligations of this provider;***~~

~~***(d) which information shall be screened by the crypto-asset service provider of the beneficiary as well the relevant obligations of this provider.***~~

The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in ~~***paragraphs 1 and 3 of***~~ ***this Article in accordance with Articles 38 to 41 of Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final].*** **(707)**

Technical note

Under the Transfer of Funds Regulation (Article 18ad), obliged entities should apply internal policies, procedures and controls to ensure the implementation of targeted financial sanctions with respect to all kind of transfers. Recital 16 provides further clarity on sanctions screening obligations to be applied for all transfers of funds and crypto-assets.
Upon CONS request, it was agreed to negotiate the details of sanctions screening in the AMLR to make it applicable horizontally to obliged entities (including – but not limited to – processing of transactions).

A similar approach was adopted by the COM proposal for a Regulation on instant payment (Article 5d).

COMP AA

Articles 38, 39, 40; 41, 41 a - Performance by third parties

AMs Covered: 84, 85, 86, 87, 88, 89 (Rapporteurs), 476, 488, 495 (Left), 708 (EPP), 709 (EPP), 711 (Renew), 712 (EPP), 713 (S&D), 715 (Renew), 717 (EPP), 718, 719 (Renew), ~~720 (Renew), 721 (EPP),~~ 726 (Left), 731 (EPP), 732 (Renew), 733 (EPP), 734 (Left), 736 (EPP), 737 (Left), 738 (Renew), 739 (EPP), 740 (Renew), 742 (Renew),

AMs Falling: 710 (ID), 714 (S&D), 716 (ECR), 720 (Renew), 721 (EPP), 722, 723, 724 (EPP), 725 (Renew), 727 (EPP), 728 (Renew), 729 (EPP), 730 (ID), 731 (EPP), 732 (Renew), 733 (EPP), 734 (Left), 735 (EPP), 736 (EPP), 737 (Left), 738 (Renew), 741 (ID), 743 (ID)

Article 38
General provisions relating to reliance on other obliged entities

1. Obliged entities may rely on other obliged entities, whether situated in a Member State or in a third country, to meet the customer due diligence requirements laid down in Article 16(1), points (a), (b)***, (c)*** and (***d), and Article 21 (2) and (3***), provided that: (708,709)

   (a) the other obliged entities apply customer due diligence requirements and record-keeping requirements laid down in this Regulation, or equivalent when the other obliged entities are established or reside in a third country;

   (b) compliance with AML/CFT requirements by the other obliged entities is supervised in a manner consistent with Chapter IV of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*.

   The ultimate responsibility for meeting the customer due diligence requirements shall remain with the obliged entity which relies on another obliged entity.

2. When deciding to rely on other obliged entities situated in third countries, obliged entities shall take into consideration the geographical risk factors listed in Annexes II and III and any relevant information or guidance provided by the Commission, or by AMLA or other competent authorities.

3. In the case of obliged entities that are part of a group, compliance with the requirements of this Article and with Article 39 may be ensured through group-wide policies, controls and procedures provided that all the following conditions are met:

   (a) the obliged entity relies on information provided solely by an obliged entity that is part of the same group;

   (b) the group applies AML/CFT policies and procedures, customer due diligence measures and rules on record-keeping that are fully in compliance with this Regulation, or with equivalent rules in third countries;

   (c) the effective implementation of the requirements referred to in point (b) is supervised at group level by the supervisory authority of the home Member State in accordance with Chapter IV of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]* or of the third country in accordance with the rules of that third country.

4. Obliged entities shall not rely on obliged entities established in third countries identified pursuant to Section 2 of this Chapter. ~~However, obliged entities established in the Union whose branches and subsidiaries are established in those third countries may rely on those branches and subsidiaries, where all the conditions set out in paragraph 3, points (a) to (c), are met.~~ (84)

4a. Reliance on other obliged entities may also include the re-use of relevant customer due diligence information and documentation obtained and processed by that entity. (711, 712)

Article 40
Outsourcing

1. Obliged entities may outsource tasks deriving from requirements under this Regulation for the purpose of performing customer due diligence to an agent or external service provider***. These tasks can be outsourced to***~~, whether~~ a natural or legal person, with the exception of natural or legal persons residing or established in third countries identified pursuant to Section 2 of this Chapter. (713, 715)

   The obliged entity shall remain fully liable for any action of agents or external service providers to which activities are outsourced.

2. The tasks outsourced pursuant to paragraph 1 shall not be undertaken in such way as to impair materially the quality of the obliged entity's measures and procedures to comply with the requirements of this Regulation and of Regulation *[please insert reference – proposal for a recast of Regulation (EU) 2015/847 - COM/2021/422 final]*. The following tasks shall not be outsourced under any circumstances:

   (a) the approval of the obliged entity's risk assessment;

   (b) the internal controls in place pursuant to Article 7;

   (c) the ~~drawing up and~~ approval of the obliged entity's policies, controls and procedures to comply with the requirements of this Regulation; (85, 717, 718, 726)

   (d) the ~~attribution of a risk profile to a prospective client and the entering~~ ***decision to enter*** into a business relationship with ~~that~~ a client ***based on the attribution of a risk profile***; (86)

   (e) the ~~identification~~ ***approval*** of criteria for the detection of suspicious or unusual transactions and activities; (87)

   (f) the reporting of suspicious activities or threshold-based declarations to the FIU pursuant to Article 50, ***unless such activities are outsourced to a service provider belonging to the same group as the obliged entity and which is established in the same Member State as the obliged entity***.

3. Where an obliged entity outsources a task pursuant to paragraph 1, it shall ensure that the agent or external service provider applies the measures and procedures adopted by the obliged entity. The conditions for the performance of such tasks shall be ***clearly specified and*** laid down in a written agreement between the obliged entity and the outsourced entity. The obliged entity shall perform regular controls to ascertain the effective implementation of such measures and procedures by the outsourced entity. The frequency of such controls shall be determined on the basis of the critical nature of the tasks outsourced. ***The obligation to lay down in a written agreement the conditions for the performance of customer due diligence tasks by the outsourced entity shall be without prejudice to any obligation of the obliged entity under Regulation (EU) 2016/679. Any subsequent outsourcing of tasks by the outsourced entity to other third party service providers ~~is not allowed. This prohibition does not prevent the outsourced entity from using services of other third parties for the purposes of performing outsourced tasks~~ shall be foreseen in the written agreement with the obliged entity, provided that the outsourced entity maintains full responsibility for applying the measures and procedures agreed with the obliged entity.*** (739, 740, 742)

3a. ***Where an obliged entity outsources a task pursuant to paragraph 1 which requires the consultation of beneficial ownership registers referred to in Article 10 of Directive [insert reference to AMLD6] and in accordance with the rules laid down in Article 11 of Directive [insert reference to AMLD6], the obliged entity shall notify the respective supervisor of the outsourcing agreement.***

4. Obliged entities shall ensure that outsourcing is not undertaken in such way as to impair materially the ability of the supervisory authorities to monitor and retrace the obliged entity's compliance with all of the requirements laid down in this Regulation.

Article 41
Guidelines on the performance by third parties

By *[~~3~~ **3** years after the entry into force of this Regulation]*, AMLA***, in cooperation with the European supervisory authorities,*** shall issue guidelines addressed to obliged entities on: (88)

(a) the conditions which are acceptable for obliged entities to rely on information collected by another obliged entity, including in case of remote customer due diligence;
(b) the establishment of outsourcing relationships in accordance with Article 40, their governance and procedures for monitoring the implementation of functions by the outsourced entities, and in particular those functions that are to be regarded as critical;
(c) the roles and responsibility of each actor, whether in a situation of reliance on another obliged entity or of outsourcing;
(d) supervisory approaches to reliance on other obliged entities and outsourcing.

Article 41a
Unwarranted de-risking, non-discrimination and financial inclusion

1. ***~~Member States shall ensure that c~~Credit and financial institutions shall have in place~~, in the implementation of~~ internal policies, controls and procedures ~~referred to in Article 7~~ to ensure that ~~and in~~ the application of customer due diligence requirements provided under this Chapter does not result in the unwarranted refusal, or termination, of business relationships with entire categories of customers and that obliged entities comply with Article 15 and Article 16(2) of Directive 2014/92/EU.***
The internal policies, controls and procedures of credit and financial institutions shall include options for mitigating the risks of money laundering and terrorist financing that obliged entities will consider applying before deciding to reject a customer on ML/TF risk grounds.

~~Obliged entities~~ The internal policies and procedures of credit and financial institutions shall include options and criteria to adjust the features of products or services offered to a given customer on an individual and risk-sensitive basis and, where applicable, ~~shall ensure that the customer due diligence measures under this Chapter apply proportionately,~~ in accordance with the level of services offered under Directive 2014/92/EU. (476) (488) (495)

2. ***Without prejudice to paragraph 1, ~~Member States shall ensure that, obliged entities~~ credit and financial institutions shall have in place internal policies, controls and***

procedures to ensure that the application of customer due diligence requirements provided under this Chapter does not result in the undue exclusion of ~~*obliged entities do not deny access to basic financial services to civil society*~~ *non-profit organisations and their representatives and associates from access to financial services* ~~*and activists solely*~~ *exclusively on the basis of geographical risk.* ~~*Obliged entities shall not rely exclusively on information provided by public authorities from the countries under authoritarian regimes or political systems with weak democratic institutions in the risk assessment concerning civil society organisations and activists.*~~

3. Obliged entities shall not rely exclusively on information provided by public authorities from the third countries covered by Articles 23, 24 and 25, as well as from the third countries covered by a decision adopted in accordance with Chapter 2 of Title V of the Treaty on European Union providing for the interruption or reduction, in part or completely, of economic and financial relations.

4. By ... [~~*2*~~ *3 years after the entry into force of this Regulation], AMLA and the European Banking Authority shall jointly issue guidelines on the clarification of the relationship between requirements in this Chapter and access to financial services, including in relation to the interactions between this Chapter and Directive (EU) 2014/92 and Directive (EU) 2015/2366.*
Those guidelines shall include guidance on how to maintain a balance between financial inclusion of ~~*certain*~~ *the categories of customers particularly affected by de-risking*~~*, such as those deemed high risk,*~~ *and AML/CFT requirements*~~*,*~~*. The guidelines shall clarify how risk can be mitigated in relation to those customers and* ~~*in particular ways to mitigate risk and ensure that basic financial products and services can be offered, in addition to practices to*~~ *ensure transparent and fair processes for customers.*
(89)

Recitals 32a, 62, 63

AMs Covered: 176 (Renew), 211 (Renew), 213 (S&D), 214 (S&D)
AMs Falling: 212 (ECR), 215 (ECR), 216 (ID)

(32a)
Credit and financial institutions should ensure that the application of due diligence measures is carried out on the basis of an individual risk assessment and does not result in unduly denying legitimate customers access to financial services, in particular with regard to specific categories of individual customers associated with higher risk, such as refugees and asylum seekers as well as human rights defenders and non-governmental organisations and their representatives and associates. To this end, credit and financial institutions should ensure that their internal policies, controls and procedures are commensurate to the risks identified and do not unduly undermine financial inclusion. Access to basic financial products and services allows refugees and people seeking temporary or international protection to participate in the economic and social life of the Union, in line with the right to protection enshrined in Article 18 of the Charter of Fundamental Rights. At the same time, financial inclusion avoids that transactions are driven underground through informal channels, thereby making the detection and reporting of suspicious transactions more difficult. As such, financial

inclusion contributes significantly to the fight against money laundering and terrorist financing. This Regulation provides sufficient flexibility to financial institutions to perform the identification and verification of prospective clients who are refugees or seek protection and to adopt, in line with the risk-based approach, proportionate and effective measures to manage and mitigate risks linked to these clients. To ensure such flexibility is exploited to the fullest, credit and financial institutions should accept documents issued by Member States stating legal residence as a valid means for the purposes of customer identity verification. In order to ensure the effective implementation of anti-money laundering/countering the financing of terrorism rules, financial institutions should address the situation of refugees and persons seeking temporary or international protection within their internal policies and procedures of refugees and persons seeking temporary or international protection within their internal policies and procedures (176)

AMLA and EBA should issue joint guidelines to specify how to maintain a balance between the financial inclusion of the categories of customers particularly affected by de-risking and AML/CFT requirements and clarify how risk can be mitigated in relation to these customers and ensure transparent and fair processes for customers.

(62) Obliged entities may outsource tasks relating to the performance of customer due diligence to an agent or external service provider ~~***that fully comply with GDPR, such as an AML compliance entity,***~~ unless they are established in third countries that are designated as high-risk, as having compliance weaknesses or as posing a threat to the Union's financial system. ***These outsourcing activities should support obliged entities, to obtain complete, timely and accurate information by using decision-making tools, such as global news, business, regulatory and legal databases***. In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external service providers not covered by AML/CFT requirements, any AML/CFT obligations upon those agents or outsourcing service providers could arise only from the contract between the parties and not from this Regulation. Therefore, the responsibility for complying with AML/CFT requirements should remain entirely with the obliged entity itself. The obliged entity should in particular ensure that, where an outsourced service provider is involved for the purposes of remote customer identification, the risk-based approach is respected. ***The outsourcing of tasks deriving from requirements under this Regulation for the purpose of performing customer due diligence to an agent or external service provider should not exempt the obliged entity from any obligation under Regulation (EU) 2016/679, including Article 28 thereof.*** (211, 213)

(63) In order for third party reliance and outsourcing relationships to function efficiently, further clarity is needed around the conditions according to which reliance takes place. AMLA should have the task of developing guidelines on the conditions under which third-party reliance and outsourcing can take place, as well as the roles and responsibilities of the respective parties. To ensure that consistent oversight of reliance and outsourcing practices is ensured throughout the Union, the guidelines should also provide clarity on how supervisors should take into account such practices and verify compliance with AML/CFT requirements when obliged entities resort to those practices. ~~***These guidelines must ensure that third-party reliance and outsourcing can only take place when third-parties fully comply with GDPR.***~~ (214)

CHAPTER IV

BENEFICIAL OWNERSHIP TRANSPARENCY

COMP AB

Article 42 - Identification of Beneficial Owners for corporate and other legal entities

AMs covered: 13 (co-rapporteurs), 90 (co-rapporteurs), 91 (co-rapporteurs), 744 (Greens), 745 (S&D), 746 (S&D, Greens), 747 (The Left), 748 (The Left), 749 (EPP), 753 (The Left), 763 (S&D), 765 (EPP), 766 (S&D), 771 (EPP), 773 (EPP), 778 (NI), 779 (Renew), 780 (S&D; Greens), 781 (The Left), 783 (The Left), 785 (Renew), 789 (S&D), 791 (S&D, Greens)

AMs falling: 750 (Renew), 751 (Greens), 752 (S&D), 753 (NI), 754 (Left), 755 (S&D), 756 (ID), 757 (EPP), 758 (EPP), 759 (S&D), 760 (EPP), 761 (EPP), 762 (The Left), 764 (EPP), 767 (The Left), 768 (The Left), 769 (S&D, Greens), 770 (The Left), 772 (EPP), 774 (S&D, Greens), 775 (The Left), 776 (The Left),777 (EPP), 782 (The Left), 784 (NI), 786 (S&D, Greens), 787 (Greens), 788 (The Left), 790 (The Left), 792 (The Left), 793 (The Left), 794 (The Left), 795 (The Left)

Recitals 65, 66

AMs covered: 13 (co-rapporteurs), 223 (The Left), 225 (The Left)

AMs falling: 217 (S&D), 218 (S&D, Greens), 219 (S&D), 220 (NI), 221 (ID), 222 (EPP), 224 (ECR)

Article 42

Identification of Beneficial Owners for corporate and other legal entities

1. In case of corporate ***and other legal*** entities ***regardless of form or structure***, the beneficial owner(s) as defined in Article 2(22) shall be the natural person(s) who ***owns, or*** control(s), directly or indirectly***, ~~or benefits from~~***, the corporate ***or other legal*** entity, either through an ownership interest or through control via other means. **(744, 745, 746, 747, 748, 749)**

For the purpose of this Article, ***~~where~~*** '~~control through~~ an ownership interest' ***~~is based on a threshold, it~~*** shall mean an ***~~be determined based on an~~ ~~maximum~~*** ownership of ~~25%~~ ***~~5%~~*** ***~~[10%]~~*** ***15%*** plus one of the shares or voting rights or other ***direct or indirect*** ownership interest in the corporate entity, including through bearer shareholdings, on every level of ownership.

In assessing whether there is an ownership interest in the corporate entity, shareholdings on ~~each~~ every level of ownership shall ~~should~~ be taken into account. Indirect ownership shall be calculated by multiplying the shares or voting rights or other ownership interests held by the intermediate entities in the chain and by adding together the results from the various chains.

***For the purpose of this Article, 'control of the corporate or legal entity' shall mean the possibility to exercise, directly or indirectly, significant influence and impose relevant decisions within the corporate or legal entity. The 'indirect control of the corporate or legal entity' shall mean control of intermediate entities in the chain or in various chains of the structure, where the direct control is identified on each level of the structure, insofar the control over intermediate entities allows for a natural person to control the legal entity*. (763, 765)**

For the purpose of this Article, ~~***any of the following situations shall mean***~~ 'control ***of the corporate or legal entity' exists, including control*** via other means' ~~***shall include at least the following***~~ include at least one of the following **(766)**:

(a) the right to appoint or remove more than half of the members of the board or similar officers of the corporate entity;

(b) the ~~***ability to exert a significant***~~ ***exercise of dominant*** influence ~~***on***~~ ***over*** the decisions taken by the corporate entity, including veto rights, decision rights and any decisions regarding profit distributions or leading to a shift in assets; **(771)**

(c) control, whether shared or not, through formal or informal agreements with owners, members or the corporate entities, provisions in the articles of association, partnership agreements, syndication agreements, or equivalent documents depending on the specific characteristics of the legal entity, as well as voting arrangements;

(d) control through informal means, such as ***close personal connections*** ~~links~~ with ~~***family members first-degree***~~ ***relatives or associates*** **(773)** of managers or directors/those owning or controlling the corporate entity;

(e) use of formal or informal nominee arrangements, ***including powers to manage or dispose of the corporate entity's assets or income, in particular its bank or financial accounts***;

(ea) control through debt instruments or other financing arrangements.

~~***(ea)***~~ ~~a power of attorney to manage or dispose of the corporate entity's assets or income, in particular its bank or financial accounts~~**. (774, 775, 776)**

Control via other means may be determined also in accordance with the criteria of Article 22(1) to (5) of Directive 2013/34/EU.

2. In case of legal entities other than corporate entities, the beneficial owner(s) as defined in Article 2(22) shall be the natural person identified according to paragraph 1 of this Article, except where Article 43(2) applies.

3. Member States shall notify to the Commission by *[3 months from the date of application of this Regulation]* a list of the types of corporate and other legal entities existing under their national laws with beneficial owner(s) identified in accordance with paragraph 1. The notification shall include the specific categories of entities, description of characteristics, names and, where applicable, legal basis under the national laws of the Member States. It shall also include an indication of whether, due to the specific form and structures of legal entities other than corporate entities, the mechanism under Article 45(3) applies, accompanied by a detailed justification of the reasons for that. ***In this notification, Member States shall also include other legal entities or vehicles to which, under national law, identification of beneficial ownership information is not deemed applicable, in particular if that is the case for investment vehicles such as special purpose vehicles or entities, protected cell companies or series limited liability companies. (780, 781, 783)***

4. The Commission shall ~~***make recommendations to Member States***~~ ***determine*** ~~***decide via implementing delegated acts***~~ ~~**on the**~~ specific rules and criteria to identi***f***y **(91, 789)** the beneficial owner(s) of legal entities other than corporate entities ***through the adoption of a delegated act*** by *[~~**1**~~ **6 months** ~~***year***~~ from the date of application of this Regulation]*. ~~***In the event that Member States decide not to apply any of the recommendations, they shall notify the Commission thereof and provide a justification for such a decision***~~. **(785)**

5. The provisions of this Chapter shall not apply to:

(a) companies listed on a regulated market that is subject to disclosure requirements consistent with Union legislation or subject to equivalent international standards, ***except for undertakings active in the extractive industry ~~and forestry~~ as defined in Article 41 (1) ~~and (2)~~ of Directive 2013/34;***

~~provided that:~~

~~(i) control over the company is exercised exclusively by the natural person with the voting rights; and~~

~~(ii) no other legal persons or legal arrangements are part of the company's ownership or control structure; (791);~~ and

(b) bodies governed by public law as defined under Article 2(1), point (4) of Directive 2014/24/EU of the European Parliament and of the Council[1].

5a. By way of derogation from paragraph 1 of this Article, ~~the~~ an ownership interest ~~of the following legal entities~~ shall mean an ownership of ~~at least~~ 5% plus one share or voting right or other ownership interest in the corporate entity, for the following legal entities:

i) ~~legal entities~~ undertakings active in the extractive industry ~~and forestry~~ as defined in Article 41 (1) ~~and (2)~~ of Directive 2013/34;

ii) legal entities that are exposed to a higher risk of money laundering and terrorist financing as identified by the Commission in accordance with paragraph 5b.

5b. ~~Member States shall conduct a comprehensive risk assessment of all categories of legal entities and legal arrangements in their territory and of the cases in which national or foreign legal entities have been misused for money laundering, predicate offences or terrorist financing purposes.~~

~~For the purposes of conducting such assessment, Member States shall take into account the typical ownership and control structure of different types of legal entities, including the number of layers of ownership and the type of legal entity in each layer. The assessment shall also include the exposure to risks deriving from the sector of operation, the involvement of intermediaries, the use of nominee shareholders or directors and concealment techniques, as well as the exposure to risks deriving from foreign legal persons and legal arrangements, in particular those which have a multi-layered control structure involving several jurisdictions. Member States shall submit their findings by [2 years after the entry into force of this Regulation] to the Commission and AMLA. On the basis of the information collected by Member States in accordance with the first subpragraph, and after consultation with AMLA, the~~

Member States shall notify to the Commission by [3 months from the date of application of this Regulation] a list of all categories of corporate and other legal entities exising in their territory.

The Commission shall be empowered to identify, by means of delegated acts, the categories of legal entities or sectors that are associated with higher money laundering and terrorist financing risk and predicate offences for which a ~~lower~~ threshold ~~of 5% than that set out in paragraph 1,~~ shall be an ownership interest.~~and specify the corresponding thresholds.~~

For the purpose of the first subpragraph, the Commission shall consult AMLA and take into account the national risk assessment carried out in accordance with Article 8 of Directive and any additional information provided by the Member States. ***[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final].***

In order to identify the categories of legal entities or sectors of higher risk in accordance with this paragraph, the Commission shall, where relevant, consult experts from the private sector, civil society and academia.
The Commission shall review the delegated acts on a regular basis to ensure that the categories of corporate entities identified as associated with higher risks are correct, and that the lower thresholds imposed are proportionate and adequate to ~~those~~ the risks identified.

(65) Detailed rules should be laid down to identify the beneficial owners of corporate and other legal entities and to harmonise definitions of beneficial ownership. While a specified percentage shareholding or ownership interest does not automatically determine the beneficial owners, it should be one factor among others to be taken into account. ~~***Member States should be able, however, to decide that a percentage lower than 25% may be an indication of ownership or control***~~. Control through ownership interest ~~of 5% 25% plus one of the shares or voting rights or other ownership interest,~~ should be assessed on every level of ownership, meaning that ~~this~~ ***the specific*** threshold should apply to every ~~link~~ ***level*** in the ownership structure and that every link in the ownership structure and the combination of them should be properly examined. **(13, 223)** ***In case of indirect shareholding, the beneficial owners should be identified by multiplying the shares in the ownership chain. To this end, all shares directly or indirectly owned by the same natural person should be added together.***

(66) A meaningful identification of the beneficial owners requires a determination of whether control is exercised via other means. The determination of control through an ownership interest is necessary but not sufficient and it does not exhaust the necessary checks to determine the beneficial owners. The test on whether any natural person exercises control via other means is not a subsequent test to be performed only when it is not possible to determine an ownership interest. The two tests, namely that of control through an ownership interest and that of control via other means, should be performed in parallel. Control through other means may include the right to appoint or remove more than half of the members ~~***any member***~~ of the board of the corporate entity; the ability to exert a significant influence on the decisions taken by the corporate entity; control through formal or informal agreements with owners, members or the corporate entities, as well as voting arrangements; links with family members ~~***close relatives or associates***~~ of managers or directors or those owning or controlling the corporate entity; use of formal or informal nominee arrangements ***or control through debt instruments or other financing arrangements*** ~~***or the possibility to use the power of attorney to manage or dispose of the corporate entity's assets or income, particularly its bank or financial accounts***~~. (225)

[1] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance (OJ L 94, 28.3.2014, p. 65).

COMP AC

Article 43 - Identification of beneficial owners for express trusts and similar legal entities or arrangements

Article 44 - Beneficial ownership information

Article 45 - Obligations of legal entities

AMs included: 92 (co-rapporteurs), 93 (co-rapporteurs), 94 (co-rapporteurs), 797 (S&D, Greens), 798 (Greens), 800 (S&D, Greens), 803 (EPP), 804 (EPP), 810 (EPP), 814 (EPP), 818 (Renew), 820 (NI), 821 (Renew),

AMs falling: 796 (EPP), 799 (The Left), 801 (ID), 802 (The Left), 805 (The Left), 806 (Greens), 807 (EPP), 808 (S&D), 809 (Greens), 811 (EPP), 812 (EPP), 813 (The Left), 815 (The Left), 816 (Renew), 817 (The Left), 819 (The Left), 822 (NI), 823 (The Left), 824 (NI), 825 (NI), 826 (The Left), 827 (EPP),

Recitals 70, 71, 72

AMs covered: 230 (Renew), 228 (EPP)

AMs falling: 226 (The Left), 227 (The Left), 229 (Renew)

Article 43

Identification of beneficial owners for express trusts and similar legal entities or arrangements

1. In case of express trusts, the beneficial owners shall be all the following natural persons:

   (a) the ***economic and legal*** settlor(s); **(797, 798)**

   (b) the trustee(s);

   (c) the protector(s), if any;

   (d) the beneficiaries or where there is a class of beneficiaries, the individuals within that class that receive a benefit from the legal arrangement or entity , irrespective of any threshold, as well as the class of beneficiaries. However, in the case of pension schemes within the scope of Directive (EU) 2016/2341 of the European Parliament and of the Council[17] and which provide for a class of beneficiaries, only the class of beneficiaries shall be the beneficiary;

   (e) any other natural person exercising ultimate control over the express trust by means of direct or indirect ownership or by other means, including through a chain of control or ownership.

[17] Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (OJ L 354, 23.12.2016, p. 37).

2. In the case of legal entities and legal arrangements similar to express trusts, the beneficial owners shall be the natural persons holding equivalent or similar positions to those referred to under paragraph 1. ***In the case where the parties of the express trust laid down in paragraph 1 point (a), (b), (c), or (d) are corporate or legal entities or arrangements themselves, the beneficial owner shall be the natural person who owns, directly or indirectly, ~~is the beneficial owner of~~ those entities or arrangements, through an ownership of at least one share or voting right or other ownership interest in the corporate entity or the ultimate natural person(s) who exercises control through a chain of control or ownership of corporate or legal entities or arrangements (800) or through control via other means.***

   Member States shall notify to the Commission by *[3 months from the date of application of this Regulation]* a list of legal arrangements and of legal entities, similar to express trusts, where the beneficial owner(s) is identified in accordance with paragraph 1.

3. The Commission is empowered to adopt, by means of an implementing act, a list of legal arrangements and legal entities governed under the laws of Member States which should be subject to the same beneficial ownership transparency requirements as express trusts. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 61(2) of this Regulation.

Article 44

Beneficial ownership information

1. For the purpose of this Regulation, beneficial ownership information shall be adequate, accurate, and current and include the following:

   (a) the first name and surname, full place and date of birth, residential address, country of residence and nationality or nationalities of the beneficial owner, national identification number and source of it, such as passport or national identity document, ***~~and, where applicable, the tax identification number or other equivalent number assigned to the person by his or her country of usual residence;~~ (803, 804)***

   (b) the nature and extent of the beneficial interest held in the legal entity or legal arrangement, whether through ownership interest or control via other means, as well as the date of acquisition of the beneficial interest held;

   (c) information on the legal entity or legal arrangement of which the natural person is the beneficial owner in accordance with Article 16(1) point (b), as well as the description of the control and ownership structure.

2. ***Entities referred to in Articles 42 and 43 shall ~~obtain~~ hold adequate, accurate, and current*** beneficial ownership information ***~~shall be obtained~~*** within ***~~14~~ 21*** calendar days from ***their creation ~~of legal entities or legal arrangements~~***. It shall be updated promptly, and in any case no later than ***~~14~~ 21*** calendar days following any change of the beneficial owner(s), and on an annual basis. **(92, 810)**

Article 45

Obligations of legal entities

1. All corporate and other legal entities incorporated in the Union shall obtain and hold adequate, accurate and current beneficial ownership information.

   Legal entities shall provide, in addition to information about their legal owner(s), information on the beneficial owner(s) to obliged entities where the obliged entities are taking customer due diligence measures in accordance with Chapter III.

   The beneficial owner(s) of corporate or other legal entities shall provide those entities with all the information necessary for the corporate or other legal entity ***and shall inform obliged entities without undue delay about all changes relating to beneficial ownership***. **(814)**

2. Where, after having exhausted all possible means of identification pursuant to Articles 42 and 43, no person is identified as beneficial owner, or where there is any doubt that the person(s) identified is the beneficial owner(s), the corporate or other legal entities shall keep records of the actions taken in order to identify their beneficial owner(s) ***and ~~provide~~ hold additional information available on a risk-sensitive basis, and promptly provide it to competent authorities where required, including resolutions of the board of directors and minutes of their meetings, partnership agreements, trust deeds, informal arrangements determining powers equivalent to powers of attorney or other contractual agreements and documentation***. **(93, 818, 820)**

3. In the cases referred to in paragraph 2, when providing beneficial ownership information in accordance with Article 16 of this Regulation and Article 10 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*, corporate or other legal entities shall provide the following ***information, which shall be clearly stated in the register referred to in Article 10 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]***: **(94)**

   (a) a statement, accompanied by a justification ***and supporting documents (821)***, that there is no beneficial owner or that the beneficial owner(s) could not be identified and verified;

   (b) the details on the natural person(s) who hold the position of senior managing official(s) in the corporate or legal entity equivalent to the information required under Article 44(1), point (a).

4. Legal entities shall make the information collected pursuant to this Article available, upon request and without delay, to competent authorities.

5. The information referred to in paragraph 4 shall be maintained for five years after the date on which the companies are dissolved or otherwise ceases to exist, whether by persons designated by the entity to retain the documents, or by administrators or liquidators or other persons involved in the dissolution of the entity. The identity and contact details of the person responsible for retaining the information shall be reported to the registers referred to in Article 10 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*.

(70) Underpinning an effective framework on beneficial ownership transparency is the knowledge by corporate and other legal entities of the natural persons who are their beneficial owners. Thus, all corporate and other legal entities in the Union should obtain and hold adequate, accurate and current beneficial ownership information. That information should be retained for five years and the identity of the person responsible

for retaining the information should be reported to the registers. That retention period is equivalent to the period for retention of the information obtained within the application of AML/CFT requirements, such as customer due diligence measures. In order to ensure the possibility to cross-check and verify information, for instance through the mechanism of discrepancy reporting, it is justified to ensure that the relevant data retention periods are aligned.

(71) Corporate and other legal entities should take all necessary measures to identify their beneficial owners. There may however be cases where no natural person is identifiable who ultimately owns or exerts control over an entity. In such exceptional cases, provided that all means of identification are exhausted, the senior managing officials can be reported when providing beneficial ownership information to obliged entities in the course of the customer due diligence process or when submitting the information to the central register. Corporate and legal entities should keep records of the actions taken in order to identify their beneficial owners, especially when they rely on this last resort measure, which should be duly justified and documented.

(72) There is a need to ensure a level playing field among the different types of legal forms and to avoid the misuse of trusts and legal arrangements, which are often layered in complex structures to further obscure beneficial ownership. Trustees of any express trust administered in a Member State should thus be responsible for obtaining and holding adequate, accurate and current beneficial ownership information regarding the trust and for disclosing their status and providing this information to obliged entities carrying out costumer due diligence, ***taking into account the specificities and risks of different legal systems, including common law jurisdictions (228)***. Any other beneficial owner of the trust should assist the trustee in obtaining such information.

(73) In view of the specific structure of certain legal entities such as foundations, and the need to ensure sufficient transparency about their beneficial ownership, such entities and legal arrangements similar to trusts should be subject to equivalent beneficial ownership requirements as those that apply to express trusts, ***with due account to the specificities inherent to the different legal entities, in particular civil society organisations***. **(230)**

COMP AD

Article 46 - Trustees obligations relating to the identification of beneficial owners of express trusts or similar legal arrangements

Article 47 - Measures to mitigate risks relating to nominee shareholders and nominee directors

Article 48 - Foreign legal entities and arrangements

Article 49 - Sanctions

AMs included: 95 (co-rapporteurs), 96 (co-rapporteurs), 828 (S&D), 829 (S&D), 830 (Greens), 832 (The Left), 833 (NI), 834 (The Left), 835 (S&D, Greens), 836 (S&D, Greens), 841 (S&D),

AMs falling: 97 (co-rapporteurs), 831 (Renew), 837 (S&D), 838 (The Left), 839 (The Left), 840 (Renew),

Article 46

Trustees obligations ***relating to the identification of beneficial owners of express trusts or similar legal arrangements (828)***

1. Trustees of any express trust administered in a Member State and persons holding an equivalent position in a similar legal arrangement shall obtain and hold adequate, accurate and current beneficial ownership information regarding the legal arrangement. Such information shall be maintained for five years after their involvement with the express trust or similar legal arrangement ceases.

2. The persons referred to in paragraph 1 shall disclose their status and provide the information on the beneficial owner(s) to obliged entities when the obliged entities are taking customer due diligence measures in accordance with Chapter III.

3. The beneficial owner(s) of an express trust or similar legal arrangement other than the trustee or person holding an equivalent position, shall provide the trustee or person holding an equivalent position in a similar legal arrangement with all the information necessary to comply with the requirements of this Chapter.

4. Trustees of an express trust and persons holding an equivalent position in a similar legal arrangement shall make the information collected pursuant to this Article available, upon request and without delay, to competent authorities.

4a. ***Where the trustee or person holding an equivalent position in a similar legal arrangement is not established or resides in the Union, beneficial ownership information shall be obtained and held in the conditions laid down in paragraph 1 by ~~either~~ the settlor ~~or the beneficiary~~, provided that:***

1) the express trust or legal arrangement is governed under the law of one Member State; or

2) either the settlor, the protector or the beneficiary are residents in one Member State. (829)

Article 47

Measures to mitigate risks relating to nominee shareholders and nominee directors ***~~Nominees obligations~~***

Nominee shareholders and nominee directors of a corporate or other legal entities shall ***be ~~prohibited, except where nominee shareholders and nominee directors of a corporate or other legal entities are~~ granted a licenced ~~under national law to offer nominee services. In addition, nominee shareholders and nominee directors~~ and*** shall maintain adequate, accurate and current information on the identity of their nominator and the nominator's beneficial owner(s) and disclose them, as well as their status, to the corporate or other legal entities, ***regardless of whether the nominee arrangements are formal or informal***. Corporate or other legal entities shall report this information to the registers set up pursuant to Article 10 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final].

Corporate and other legal entities shall also report this information to obliged entities when the obliged entities are taking customer due diligence measures in accordance with Chapter III. (**830)**

Article 48

Foreign legal entities and arrangements

1. Beneficial ownership information of legal entities incorporated outside the Union or of express trusts or similar legal arrangements administered outside the Union shall be held in the central register referred to in Article 10 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]* set up by the Member State where such entities or trustees of express trusts or persons holding equivalent positions in similar legal arrangements:

   (a) enter into ***or hold*** **(95, 832)** a business relationship with an obliged entity;

   (b) ***own or*** **(96, 833, 834)** acquire ***land or*** real estate in their territory.

   ba) own or acquire ~~relevant high value~~ goods ~~assets~~ referred to in Article 16b and Article 16c of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final], unless Member States make the beneficial ownership information available in other registers or electronic data retrieval systems in accordance with Articles 16b or 16c of that Directive;

   (bd) own or acquire a majority or minority stake in bodies governed by public law, as defined under Article 2(1), point (4) of Directive 2014/24/EU of the European Parliament and of the Council (835)

   (bc) are ~~or have been~~ awarded a public procurement for goods, services or concessions or have been awarded a public procurement for goods, services or concessions that is ongoing. (836)

   2. Where the legal entity, the trustee of the express trust or the person holding an equivalent position in a similar legal arrangement enters into multiple business relationships or acquires ***land or*** real estate ***other relevant high value goods or assets referred to in point (ba)*** in different Member States, a certificate of proof of registration of the beneficial ownership information in a central register held by one Member State shall be considered as sufficient proof of registration.

2a. With regard to already existing business relationships ~~with an obliged entity~~ referred in paragraph 1 (a), (ba) and (bd) or real estate owned as of ... [the date of application of this Regulation], obliged entities and legal entities as referred to in paragraph 1 shall comply with the requirements set out in paragraphs 1 and 2 by ... [six months after the date of application of this Regulation].

Article 49

Sanctions

Member States shall lay down the rules on sanctions applicable to infringements of the provisions of this Chapter and shall take all measures necessary to ensure that they are implemented. The sanctions provided for must be effective, proportionate and dissuasive.

Member States shall notify those rules on sanctions by *[6 months after the entry into force of this Regulation]* to the Commission together with their legal basis and shall notify it without delay of any subsequent amendment affecting them.

By [2 years after the date of entry into force of this Directive], AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall define indicators to classify the level of gravity of infringements and criteria to be taken into account when setting the level of administrative sanctions, including ranges of pecuniary sanctions relative to the turnover of the entity that shall be applied as references for effective, proportionate and dissuasive sanctions.

The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 1a of this Article in accordance with Articles 38 to 41 of Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]. (841)

CHAPTER V

REPORTING OBLIGATIONS

COMP AE
Articles 50, 51, 52, 53, 54 - Reporting Obligations
AMs Covered: 98, 99, 100, 101, 102, 103 (Rapporteurs), 842 (S&D), 843 (Greens), 844 (EPP), 848 (Greens), 849 (EPP), 850 (S&D), 852 (Renew), 853 (Greens), 854 (EPP), 856 (S&D), 857 (S&D), 858 (Left), 859 (Greens), 860 (Greens), 862 (Renew), 864 (Left), 865 (S&D), 866 (Renew), 873 (ECR), 874 (EPP), 876 (Renew), 877 (EPP), 878 (EPP), 879 - partly covered (EPP), 880 (S&D),
AMs Falling: 845, 846, 847 (Renew), 851 (EPP), 855 (Renew), 861 (Left), 863 (ID), 867 (ID), 868 (Renew), 869, 870 (ID), 871 (NI), 872 (EPP), 875 (Left), 881, 882 (Renew), 883 (EPP), 884 (RE)

Article 50

Reporting of ***suspicions*** ~~*suspicious transactions*~~

1. Obliged entities shall report to the FIU ~~***[via the FIU.net one-stop-shop]***~~ all ***suspicions of money laundering, predicate offences and terrorist financing***, including ***on*** attempted transactions. (842, 843, 844)

   Obliged entities, and, where applicable, their directors and employees, shall cooperate fully by promptly:

   (a) reporting to the FIU, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds***, assets or activities***, regardless of the amount involved, ***are related to*** the proceeds of criminal activity or ~~are related~~ to terrorist financing, and by responding to requests by the FIU ~~***[via the FIU.net one-stop-shop]***~~ for additional information in such cases; (848, 849, 850)

   (b) providing the FIU directly ~~***[via the FIU.net one-stop-shop]***~~, at its request, with all necessary information. (852)

   For the purposes of points (a) and (b), obliged entities shall reply to a request for information by the FIU within ~~***the appropriate deadline set by the FIU, depending on the complexity and urgency of the request***~~ 5 ***working*** days***, unless the FIU determines a different deadline***. In justified and urgent cases, ~~FIUs shall be able to shorten~~ such ~~a deadline to 24 hours~~ ***as where transactions are in progress or a prompt action is required, FIUs may require the information to be provided ~~immediately~~ as soon as possible, and within a deadline that shall not be longer than ~~24 hours~~ one working day.*** (853, 854, 856)

2. For the purposes of paragraph 1, obliged entities shall assess transactions identified pursuant to Article 20 as atypical in order to detect those that can be suspected of being linked to money laundering or terrorist financing.

   A suspicion ~~is~~ ***may be*** based on the characteristics of the customer ***and their counterparts***, the size and nature of the transaction or activity, ***the methods, techniques and patterns of execution of the transaction or activity***, ***the use of anonymising tools***, the link between several transactions or activities and any other circumstance known to

the obliged entity, including ***the origin of funds or assets and*** the consistency of the transaction or activity with the risk profile of the client ***and the characteristics of the transaction or customer when linked to patterns highlighted by the risk assessments conducted in accordance with Articles 7 and 8 of Directive [please insert reference proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]***. (857, 858, 859)

3. By *[two years after entry into force of this Regulation]*, AMLA shall develop draft implementing technical standards and submit them to the Commission for adoption. Those draft implementing technical standards shall specify the ***means and*** format to be used for the reporting of ***suspicions*** ~~suspicious transactions~~ pursuant to paragraph 1 ***The technical standards shall include appropriate formats for the reporting of specific indicators that may be associated with crypto-asset transactions~~, including distributed ledger wallet addresses and transaction hashes~~***. (860, 862)

4. The Commission is empowered to adopt the implementing technical standards referred to in paragraph 3 of this Article in accordance with Article 42 of Regulation *[please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final]*.

5. AMLA shall issue and periodically update***, with the assistance of other EU bodies, offices and agencies involved in the AML/CFT framework,*** guidance on indicators of unusual or suspicious activity or behaviours. (864, 865, 866)

6. The person appointed in accordance with Article 9(3) shall transmit the information referred to in paragraph 1 of this Article to the FIU of the Member State in whose territory the obliged entity transmitting the information is established.

6 a. Within [3 years from the entry into force of this Regulation], the ~~Commission~~ AMLA shall develop an electronic filing system (FIU.net one-stop-shop) to be used by obliged entities to submit to the ~~competent FIUs~~ to the FIU of the Member State in whose territory the obliged entity transmitting the information is established, and to any other concerned FIU, reports of suspicion of money laundering, predicate offences and terrorist financing, including on attempted transactions.

The FIU.net one-stop-shop shall provide a single access point for reporting of suspicions ~~in a secure manner~~ through protected channels of communications and via a standardised form, as well for communication between the competent FIUs and obliged entities, and for information and intelligence sharing between FIUs on submitted reports of suspicions. The FIU.net one-stop-shop shall be managed by AMLA, and shall be hosted by the FIU.net.

The FIU.net one-stop-shop shall become fully operational by [5 years from the entry into force of this Regulation], and its use for the submission of reports of suspicion and the transmission of information between obliged entities and competent FIUs shall become mandatory as of [6 years after entry into force of this Regulation].

The FIU.net one-stop-shop shall be established as a decentralised system. Information transmitted by obliged entities via such system shall be controlled and stored by the competent FIUs, in full compliance with the Union data protection acquis.

When establishing the FIU.net one-stop-shop~~, the Commission, after having consulted~~ AMLA shall specify the conditions for operational management of the system ~~by AMLA~~, its composition, and digital procedural standards enabling the interconnection through the single access points.

Article 51

Specific provisions for reporting of suspicious transactions by certain categories of obliged entities

1. By way of derogation from Article 50(1), Member States may allow obliged entities referred to in Article 3, point (3)(a), (b) ~~and (d)~~ to transmit the information referred to in Article 50(1) to a self-regulatory body designated by the Member State. The designated self-regulatory body shall forward the information referred to in the first sub-paragraph to the FIU promptly and unfiltered.

2. Notaries, lawyers and other independent legal professionals, auditors, external accountants and tax advisors shall be exempted from the requirements laid down in Article 50(1) to the extent that such exemption relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client ***except where the legal advice is provided for the purpose of money laundering or terrorist financing, or where those persons know or ~~suspect~~ have a well grounded supicion that the client is seeking legal advice for the purposes of money laundering or terrorist financing and the advice is not sought in relation to judicial proceedings***, or performing their task of defending or representing that client in, or concerning, judicial proceedings ***~~related to suspicions~~***, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

Member States may adopt or maintain with regard to specific transactions that involve a particular high risk to be used for money laundering or terrorist financing additional reporting obligations for the professionals mentioned in this paragraph to which the exemption from the requirements laid down in Article 50(1) does not apply. For this purpose, Member States may introduce specific provisions in national law on the application of requirements applicable to such professionals under Article 17. (98, 99, 100, 101, 102, 873, 874, 876)

Article 52

Consent by FIU to the performance of a transaction

1. Obliged entities shall refrain from carrying out transactions which they know or suspect to be related to proceeds of criminal activity or to terrorist financing until they have completed the necessary action in accordance with Article 50(1), second subparagraph, point (a), and have complied with any further specific instructions from the FIU or other competent authority in accordance with the applicable law. ***Obliged entities may carry out the transaction concerned after a proper risk assessment if they have not received instructions to the contrary from the FIU within three days.*** (877)

2. Where refraining from carrying out transactions referred to in paragraph 1 is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected transaction, the obliged entities concerned shall inform the FIU immediately afterwards.

Article 53

Disclosure to FIU

Disclosure of information in good faith by an obliged entity or by an employee or director of such an obliged entity in accordance with Articles 50 and 51 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether illegal activity actually occurred.

Article 54

Prohibition of disclosure

1. Obliged entities and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted in accordance with Article 50 or 51 or that a money laundering or terrorist financing analysis is being, or may be, carried out.

2. Paragraph 1 shall not apply to disclosures to competent authorities and to self-regulatory bodies where they perform supervisory functions, or to disclosure for the purposes of investigating and prosecuting money laundering, terrorist financing and other criminal activity.

3. By way of derogation from paragraph 1, disclosure may take place between the obliged entities that belong to the same group, or between those entities and their branches and subsidiaries established in third countries, provided that those branches and subsidiaries fully comply with the group-wide policies and procedures, including procedures for sharing information within the group, in accordance with Article 13, and that the group-wide policies and procedures comply with the requirements set out in this Regulation.

4. By way of derogation from paragraph 1, disclosure may take place between the obliged entities as referred to in Article 3, point (3)(a) and (b), or entities from third countries which impose requirements equivalent to those laid down in this Regulation, who perform their professional activities, whether as employees or not, within the same legal person or a larger structure to which the person belongs and which shares common ownership, management or compliance control, including networks or partnerships.

5. For obliged entities referred to in Article 3, points (1), (2), (3)(a) and (b), in cases relating to ~~the same customer and~~ the same transaction involving two or more obliged entities, and by way of derogation from paragraph 1, disclosure may take place between the relevant obliged entities provided that they are located in the Union, or with entities in a third country which imposes requirements equivalent to those laid down in this Regulation, and that they are from the same category of obliged entities and are subject to professional secrecy and personal data protection requirements***, in line with the Union acquis on data protection*** ***~~[comparable to those laid down in Regulation (EU) 2016/679]~~.*** (103, 878, 879 - partly covered, 880)

6. Where the obliged entities referred to in Article 3, point (3)(a) and (b), seek to dissuade a client from engaging in illegal activity, that shall not constitute disclosure within the meaning of paragraph 1.

Recitals 10; 77 - 84
AMs Covered: 3 (Rapporteurs) 15 (Rapporteurs), 231 (Renew),

AM Falling: 232 (ID)

Recital 10

(10) In order to ensure respect for the rights guaranteed by the Charter of Fundamental Rights of the European Union (the 'Charter'), in the case of auditors, external accountants and tax advisors, who, in some Member States, are entitled to defend or represent a client in the context of judicial proceedings or to ascertain a client's legal position, the information they obtain in the performance of those tasks should not be subject to reporting obligations, except ***where the auditors, external accountants or tax advisors are taking part in money laundering or terrorist financing, the*** legal advice, is provided for the ***purposes*** of money laundering ***or terrorist financing, or where the auditor, external accountant or tax advisor knows or ~~has reasonable grounds to suspects~~ has a well-grounded suspicion, on the basis of factual and objective circumstances, (138) that the client is seeking legal advice, including in relation to tax matters or citizenship or residence by investment schemes, for the purposes of money laundering*** or terrorist financing ***and the legal advice sought is not connected to judicial proceedings***. ***(3) Member States should be able to adopt or maintain with regard to specific transactions that involve a particular high risk to be used for money laundering or terrorist financing additional reporting obligations to which the exemption from the requirements to transmit information does not apply. For this purpose, Member States may introduce specific provisions in national law on the application of requirements applicable to such professionals under this Regulation.***

Recital 77

(77) ***Suspicions,*** suspicious transactions, including attempted transactions, and other information relevant to money laundering, its predicate offences and terrorist financing, should be reported to the FIU, which should serve as a single central national unit for receiving and, analysing reported suspicions and for disseminating to the competent authorities the results of its analyses. ***FIU's shall strengthen cooperation with other competent authorities to ensure that meaningful information is exchanged in a timely and constructive manner in accordance with the applicable legal framework (231)***. All suspicious transactions, including attempted transactions, should be reported, regardless of the amount of the transaction. Reported information may also include threshold-based information. The disclosure of information to the FIU in good faith by an obliged entity or by an employee or director of such an entity should not constitute a breach of any restriction on disclosure of information and should not involve the obliged entity or its directors or employees in liability of any kind.

Recital 78

(78) Differences in suspicious transaction reporting obligations between Member States may exacerbate the difficulties in AML/CFT compliance experienced by obliged entities that have a cross-border presence or operations. Moreover, the structure and content of the suspicious transaction reports have an impact on the FIU's capacity to carry out analysis and on the nature of that analysis, and also affects FIUs' abilities to cooperate and to exchange information. In order to facilitate obliged entities' compliance with their reporting obligations and allow for a more effective functioning of FIUs' analytical activities and cooperation, AMLA should develop draft regulatory standards specifying a common template for the reporting of ~~suspicious transactions~~ ***suspicions*** to be used as

a uniform basis throughout the Union. ***To simplify and accelerate reporting of suspicions by obliged entities and communications and exchange of information between FIUs, ~~the Commission~~ AMLA should establish a secure and reliable electronic filing system ("FIU.net one-stop-shop") for reporting ~~of~~ suspicions of money laundering, predicate offences and terrorist financing, including on attempted transactions via a standardised form to the FIU of the Member State in whose territory the obliged entity transmitting the information is established. Such interface should also allow for the immediate transmission of this information to any other FIU which is concerned by a suspicious transaction report. The FIU.net one-stop-shop should also enable communication between the competent FIUs and obliged entities, and for information and intelligence sharing between FIUs on submitted reports of suspicions. The FIU.net one-stop-shop should be established ~~by the Commission~~ within 3 years from the entry into force of this Regulation. The use of the FIU.net one-stop-shop should be introduced gradually over time in order to allow a smooth and uninterrupted reporting of suspicion transaction reports and to leave sufficient time for FIUs and obliged entities to implement the necessary technical changes. FIUs may therefore decide to instruct obliged entities to report information via the FIU.net one-stop-shop as of [5 years after entry into force of this Regulation]. The use of FIU.net one-stop-shop should be mandatory for obliged entities as of [6 years after entry into force of this Regulation].***

Recital 79

(79) FIUs should be able to obtain swiftly from any obliged entity all the necessary information relating to their functions. Their unfettered and swift access to information is essential to ensure that flows of money can be properly traced and illicit networks and flows detected at an early stage. The need for FIUs to obtain additional information from obliged entities based on a suspicion of money laundering or financing of terrorism might be triggered by a prior suspicious transaction report reported to the FIU, but might also be triggered through other means such as the FIU's own analysis, intelligence provided by competent authorities or information held by another FIU. FIUs should therefore be able, in the context of their functions, to obtain information from any obliged entity, even without a prior report being made. Obliged entities should reply to a request for information by the FIU as soon as possible and, in any case, within ***5 working days, unless the FIU determines a different deadline*** ~~five days of receipt of the request~~ ***~~the appropriate deadline set up by the FIU~~***. In justified and urgent cases, the obliged entity should be able to respond to the FIU's request ~~within 24 hours~~ ***~~immediately~~ as soon as possible, and within a deadline that should not be longer than one working day ~~24 hours~~***. This does not include indiscriminate requests for information to the obliged entities in the context of the FIU's analysis, but only information requests based on sufficiently defined conditions. An FIU should also be able to obtain such information on a request made by another Union FIU and to exchange the information with the requesting FIU.

Recital 80

(80) For certain obliged entities, Member States should have the possibility to designate an appropriate self-regulatory body to be informed in the first instance instead of the FIU. In accordance with the case-law of the European Court of Human Rights, a system of first instance reporting to a self-regulatory body constitutes an important safeguard for upholding the protection of fundamental rights as concerns the reporting obligations

applicable to lawyers. Member States should provide for the means and manner by which to achieve the protection of professional secrecy, confidentiality and privacy.

Recital 81

(81) ~~Where a Member State decides to designate such a self-regulatory body, it may allow or require that body~~ ***Notaries, lawyers and other independent legal professionals, auditors, external accountants and tax advisors should be allowed*** not to transmit to the FIU ***or a self-regulatory body*** any information obtained from persons where such information has been received from, or obtained on, one of their clients, in the course of ascertaining the legal position of their client ***except where the legal advice is provided for the purpose of money laundering or terrorist financing, or where those persons know or suspect, on the basis of factual and objective circumstances, that the client is seeking legal advice, including in relation to tax matters or citizenship or residence by investment schemes, for the purposes of money laundering or terrorist financing and the advice is not sought in relation to judicial proceedings***, or in performing their task of defending or representing that client in, or concerning, judicial proceedings ***~~related to suspicions~~***, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings. ***Member States should be able to adopt or maintain with regard to specific transactions that involve a particular high risk to be used for money laundering or terrorist financing additional reporting obligations to which the exemption from the requirements to transmit information does not apply.***

Recital 82

(82) Obliged entities should exceptionally be able to carry out suspicious transactions before informing the competent authorities where refraining from doing so is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, ***including in duly justified cases, where this is provided in national law***. However, this exception should not be invoked in relation to transactions concerned by the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.

Recital 83

(83) Confidentiality in relation to the reporting of suspicious transactions and to the provision of other relevant information to FIUs is essential in order to enable the competent authorities to freeze and seize assets potentially linked to money laundering, its predicate offences or terrorist financing. A suspicious transaction is not an indication of criminal activity. Disclosing that a suspicion has been reported may tarnish the reputation of the persons involved in the transaction and jeopardise the performance of analyses and investigations. Therefore, obliged entities and their directors and employees should not inform the customer concerned or a third party that information is being, will be, or has been submitted to the FIU, whether directly or through the self-regulatory body, or that a money laundering or terrorist financing analysis is being, or may be, carried out. The prohibition of disclosure should not apply in specific circumstances concerning, for example, disclosures to competent authorities and self-regulatory bodies when performing supervisory functions, or disclosures for law enforcement purposes or when the disclosures take place between obliged entities that belong to the same group.

Recital 84

(84) Criminals move illicit proceeds through numerous intermediaries to avoid detection. Therefore it is important to allow obliged entities to exchange information not only between group members, but also in certain cases between credit and financial institutions and other entities that operate within networks, with due regard to data protection rules.

CHAPTER VI
DATA PROTECTION AND RECORD-RETENTION

COMP AF

Article 55 - Processing of certain categories of personal data
Article 56 - Record retention
Article 57 - Provision of records to competent authorities
Recitals 85, 86, 87, 88, 89, 90
AMs covered: 16 (Rapporteurs), 105 (Rapporteurs), 106 (Rapporteurs), 107 (Rapporteurs), 885 (Renew), 886 (EPP, Renew), 888 (EPP, Renew), 890 (S&D), 891 (S&D), 893 (Left), 894 (Left), 895 (Left), 897 (Left), 900 (Renew), 901 (EPP), 903 (Renew),908 (Left)
AMs falling: 233 (S&D), 104 (Rapporteurs), 887 (Left), 889 (Left), 892 (Left), 896 (ID), 898 (Left), 899 (Renew), 902 (EPP), 904 (Left), 905 (EPP), 906 (EPP), 907 (Left)

Article 55

Processing of certain categories of personal data

1. To the extent that it is strictly necessary for the purposes of preventing money laundering and terrorist financing ***and in accordance with the principle of proportionality***, obliged entities may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679 and personal data relating to criminal convictions and offences referred to in Article 10 of that Regulation subject to the safeguards provided for in paragraphs 2 and 3.

2. Obliged entities shall be able to process personal data covered by Article 9 ***and 10*** (893, 894) of Regulation (EU) 2016/679 provided that:

   (a) obliged entities inform their customers or prospective customers that such categories of data may be processed for the purpose of complying with the requirements of this Regulation;

   (b) the data originate from reliable sources, are accurate***, adequate, relevant*** and up-to-date; (105, 890)

   (ba) the processing of the data does not lead to biased and discriminatory outcomes; (106)

   (bb) obliged entities ensure the possibility of human intervention on the part of the controller by appropriately trained staff to verify automated individual decision-making; (107, 891, 895, 897)

   (bc) obliged entities ensure verification, where ~~of the any~~ a higher risk is identified solely on the basis of special categories of data; ~~(107)~~

   (c) the obliged entity adopts measures of a high level of security in accordance with Article 32 of Regulation (EU) 2016/679, in particular in terms of confidentiality.

3. In addition to paragraph 2, obliged entities shall be able to process personal data covered by Article 10 of Regulation (EU) 2016/679 provided that:

   (a) such personal data relate to money laundering, its predicate offences or terrorist financing;

   (b) the obliged entities have procedures in place that allow the distinction, in the processing of such data, between allegations, investigations, proceedings and

convictions, taking into account the fundamental right to a fair trial, the right of defence and the presumption of innocence.

4. Personal data shall be processed by obliged entities on the basis of this Regulation only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Regulation for commercial purposes shall be prohibited.

Article 55~~b~~a

Exchange of data under ~~Public Private Partnerships~~ partnerships for information sharing in AML/CFT field

1. For the purpose of combating money laundering and terrorist financing and related predicate offences, including for the fulfilment of their obligations under Chapter V of this Regulation, obliged entities and ~~competent~~ public authorities may ~~together with competent authorities,~~ participate in ~~cooperation arrangements~~ partnerships for information sharing in AML/CFT field established under national law in one or across several Member States.

~~2. Without prejudice to Regulation 2016/679, for no other purposes than those specifically mentioned in the arrangements pursuant to this Article and to the extent it is necessary to exchange information referred to in Article 54, by way of derogation from Article 54(1) of this Regulation, obliged entities participating in such arrangements may exchange the necessary information with other participating obliged entities and the competent authorities.~~

2. Without prejudice to Article 54, each Member State may lay down in its national law that, to the extent that is necessary and proportionate, obliged entities, and where applicable, public authorities that are party to the partnership for information sharing in AML/CFT field, may share personal data collected in the course of performing customer due diligence obligations under Chapter III, and process that data within the partnership for the purposes of the prevention of money laundering and terrorist financing, provided that at a minimum:

(a) obliged entities concerned inform their customers or prospective customers that they may share their personal data under this paragraph;

(b) personal data shared originate from reliable sources, are accurate and up-to-date;

(c) the obliged entities concerned adopt measures of a high level of security in accordance with Article 32 of Regulation (EU) 2016/679, in particular in terms of confidentiality, including secure channels for exchange of information;

(d) each instance of sharing of personal data is recorded by obliged entities, and where applicable, public authorities, concerned; the records shall be made available, without prejudice to Article 54(1), to data protection authorities and authorities responsible for protection of customers from undue tipping-off upon request;

(e) obliged entities and, where applicable, public authorities, that are party to the partnership for information sharing in AML/CFT field implement appropriate measures for protection of justified interests of the customer concerned. Further processing of personal data under this paragraph for other,

in particular commercial purposes, shall be prohibited. (885, 886, 888, 900, 901, 903)

Article 56

Record retention

1. Obliged entities shall retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:

   (a) a copy of the documents and information obtained in the performance of customer due diligence pursuant to Chapter III, including information obtained through electronic identification means, and the results of the analyses undertaken pursuant to Article 50;

   (b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions.

2. By way of derogation from paragraph 1, obliged entities may decide to replace the retention of copies of the information by a retention of the references to such information, provided that the nature and method of retention of such information ensure that the obliged entities can provide immediately to competent authorities the information and that the information cannot be modified or altered.

   Obliged entities making use of the derogation referred to in the first subparagraph shall define in their internal procedures drawn up pursuant to Article 7, the categories of information for which they will retain a reference instead of a copy or original, as well as the procedures for retrieving the information so that it can be provided to competent authorities upon request.

3. The information referred to in paragraphs 1 and 2 shall be retained for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction. Upon expiry of that retention period, obliged entities shall delete personal data.

   The retention period referred to in the first subparagraph shall also apply in respect of the data accessible through the centralised mechanisms referred to in Article 14 of Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]*.

4. Where, on *[the date of application of this Regulation]*, legal proceedings concerned with the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing are pending in a Member State, and an obliged entity holds information or documents relating to those pending proceedings, the obliged entity may retain that information or those documents, in accordance with national law, for a period of five years from *[the date of application of this Regulation]*.

   Member States may, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings, allow or require the retention of such information or documents for a further period of five years where the necessity and proportionality of such further retention have been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing.

Article 57

Provision of records to competent authorities

Obliged entities shall have systems in place that enable them to respond fully and speedily to enquiries from their FIU or from other competent authorities, in accordance with their national law, as to whether they are maintaining or have maintained, during a five-year period prior to that enquiry a business relationship with specified persons, and on the nature of that relationship, through secure channels and in a manner that ensures full confidentiality of the enquiries. ***Such system shall also provide for the authentication of competent authorities.*** (908)

Recital 85

(85) Regulation (EU) 2016/679 of the European Parliament and of the Council[18] applies to the processing of personal data for the purposes of this Regulation. The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States.

Recital 86

(86) It is essential that the alignment of the AML/CFT framework with the revised FATF Recommendations is carried out in full compliance with Union law, in particular as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter. Certain aspects of the implementation of the AML/CFT framework involve the collection, analysis, storage and sharing of data. Such processing of personal data should be permitted, while fully respecting fundamental rights, only for the purposes laid down in this Regulation, and for carrying out customer due diligence, ongoing monitoring, analysis and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person and sharing of information by credit institutions and financial institutions and other obliged entities. The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with AML/CFT requirements and personal data should not be further processed in a way that is incompatible with that purpose. In particular, ***processing of special categories of personal data and of personal data relating to criminal convictions and offences should be subject to appropriate safeguards laid down in this Regulation.*** (15), Further processing of personal data for commercial purposes should be strictly prohibited.

Recital 87

(87) The revised FATF Recommendations demonstrate that, in order to be able to cooperate fully and comply swiftly with information requests from competent authorities for the purposes of the prevention, detection or investigation of money laundering and terrorist financing, obliged entities should maintain, for at least five years, the necessary information obtained through customer due diligence measures and the records on transactions. In order to avoid different approaches and in order to fulfil the requirements

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

relating to the protection of personal data and legal certainty, that retention period should be fixed at five years after the end of a business relationship or an occasional transaction.

Recital 88

(88) When the notion of competent authorities refers to investigating and prosecuting authorities, it shall be interpreted as including the central and decentralised levels of the European Public Prosecutor's Office (EPPO) with regard to the Member States that participate in the enhanced cooperation on the establishment of the EPPO.

Recital 89

(89) For the purpose of ensuring the appropriate and efficient administration of justice during the period between the entry into force and application of this Regulation, and in order to allow for its smooth interaction with national procedural law, information and documents pertinent to ongoing legal proceedings for the purpose of the prevention, detection or investigation of possible money laundering or terrorist financing, which have been pending in the Member States on the date of entry into force of this Regulation, should be retained for a period of five years after that date, and it should be possible to extend that period for a further five years.

Recital 90

(90) The rights of access to data by the data subject are applicable to the personal data processed for the purpose of this Regulation. However, access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Exceptions to and restrictions of that right in accordance with Article 23 of Regulation (EU) 2016/679 may therefore be justified. The data subject has the right to request that a supervisory authority referred to in Article 51 of Regulation (EU) 2016/679 checks the lawfulness of the processing and has the right to seek a judicial remedy referred to in Article 79 of that Regulation. The supervisory authority may also act on an ex-officio basis. Without prejudice to the restrictions to the right to access, the supervisory authority should be able to inform the data subject that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question.

CHAPTER VII
Measures to mitigate risks deriving from anonymous instruments

COMP AG

Article 58 - Anonymous accounts and bearer shares and bearer share warrants
Recital 92, 93
AMs covered: 108 (Rapporteurs), 237 (Greens, S&D), 910 (Renew), 911 (Greens, S&D), 912 (ID), 913 (EPP),
AMs falling: 109 (Rapporteurs), 234 (S&D), 235 (ID), 909 (EPP), 914 (Renew), 915 (NI), 236 (ID)

Article 58

Anonymous accounts and bearer shares and bearer share warrants

1. Credit institutions, financial institutions and crypto-asset service providers shall be prohibited from keeping anonymous ***bank and payment*** accounts, anonymous passbooks, anonymous safe-deposit boxes or anonymous crypto-asset ***accounts*** as well as any account ~~***or instruments***~~ otherwise allowing for the anonymisation of the customer account holder ***or the increased obfuscation of transactions***. (108, 911, 913)

   Owners and beneficiaries of existing anonymous ***bank and payment*** accounts, anonymous passbooks, anonymous safe-deposit boxes or crypto-asset ***accounts*** shall be subject to customer due diligence measures before those accounts, passbooks, deposit boxes or crypto-asset ***accounts*** are used in any way.

2. Credit institutions and financial institutions acting as acquirers shall not accept payments carried out with anonymous prepaid cards issued in third countries, unless otherwise provided in the regulatory technical standards adopted by the Commission in accordance with Article 22 on the basis of a proven low risk.

3. Companies shall be prohibited from issuing bearer shares, and shall convert all existing bearer shares into registered shares by *[2 years after the date of application of this Regulation]*. However, companies with securities listed on a regulated market or whose shares are issued as intermediated securities shall be permitted to maintain bearer shares. ~~(109, 915)~~

   Companies shall be prohibited from issuing bearer share warrants that are not in intermediated form.

(92) Obliged entities should obtain and hold adequate and accurate information on the beneficial ownership and control of legal persons. As bearer shares accord the ownership to the person who possesses the bearer share certificate, they allow the beneficial owner to remain anonymous. To ensure that those shares are not misused for money laundering or terrorist financing purposes, companies - other than those with listed securities on a regulated market or whose shares are issued as intermediated securities - should convert all existing bearer shares into registered shares. In addition, only bearer share warrants in intermediated form should be allowed.

(93) The anonymity of crypto-assets exposes them to risks of misuse for criminal purposes. Anonymous crypto-asset ***accounts as well as other anonymising instruments,*** ~~***such as privacy wallets or mixers and tumblers,***~~ do not allow the traceability of crypto-asset transfers, whilst also making it difficult to identify linked transactions that may raise

suspicion or to apply to adequate level of customer due diligence. In order to ensure effective application of AML/CFT requirements to crypto-assets, it is necessary to prohibit the provision and the custody of anonymous crypto-asset ***accounts*** ~~***as well as the provision of anonymising instruments***~~ ***allowing for the anonymisation of the customer account holder or the increased obfuscation of transactions*** ~~***such as privacy wallets, mixers and tumblers***~~ by crypto-asset service providers. (237) ***Anonymising instruments or services, such as privacy wallets, mixers and tumblers, should treated by obliged entities as factors of higher risk.***

~~***By […]***~~ ***Given their potential misuse to obfuscate transactions for illicit purposes, the Commission should assess whether the provision of anonymising instruments and services, such as mixers and tumblers, by crypto-asset service providers for or on behalf of another person should also be subject to a prohibition.*** ~~***the need and proportionality of extending the prohibition of anonymous accounts to the provision by crypto-asset service providers of anonymising instruments and services allowing the anonymisation of the customer account holder or the obfuscation of transactions.***~~ ~~***The provisions should not apply to providers of hardware and software or providers of self-hosted wallets to the extent they do not perform crypto-asset services for or on behalf of another person, unless they retain control or sufficient influence over the crypto-assets even if this is exercised through a smart contract.***~~ (910)

The provisions should not apply to providers of hardware and software or providers of self-hosted wallets to the extent they do not possess access to or control over the crypto-assets of another person.

COMP AH
Article 59 - Limits to large cash payments

Recital 94, 95

AMs covered: 17 (Rapporteurs), 110 (Rapporteurs), 111 (Rapporteurs), 246 (EPP), 247 (Renew), 925 (ECR), 926 (Renew), 927 (EPP), 928 (S&D), 929 (S&D), 930 (Greens), 933 (Left), 936 (Renew), 937 (Left), 938 (S&D), 939 (Left), 941 (Greens, S&D)
AMs falling: 238 (EPP), 239 (EPP), 240 (Left), 241 (EPP), 242 (ID), 243 (ID), 244 (Renew), 245 (Renew), 248 (Renew), 249 (ID), 250 (S&D), 251 (Left), 252 (ECR), 916 (Renew), 917 (Renew), 918 (EPP), 919 (Left), 920 (EPP), 921 (ID), 922 (Renew), 923 (Renew), 924 (ID), 931 (Renew), 932 (Renew), 934 (ID), 935 (EPP), 940 (S&D)

Article 59

Limits to large cash payments

1. Persons trading in goods or providing services may accept or make a payment in cash only up to an amount of EUR ~~10 000~~ ***~~3000~~*** ***~~[5000]~~*** ***7 000*** or equivalent amount in national or foreign currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked. (110, 925, 926, 927, 928, 929, 930)

1a. In implementing paragraph 1, Member States shall not discriminate between residents and non-residents with regard to the limits applicable for cash payments. (111, 925)

2. Member States may adopt lower limits following consultation of the European Central Bank in accordance with Article 2(1) of Council Decision 98/415/EC[19] ***provided that financial inclusion is guaranteed in accordance with Article 15 and Article 16(2) of Directive 2014/92/EU. Any lower limit adopted by Member States shall be necessary to pursue legitimate objectives and proportionate to such objectives.*** (933). Those lower limits shall be notified to the Commission within 3 months of the measure being introduced at national level.

3. When limits already exist at national level which are below the limit set out in paragraph 1, they shall continue to apply. Member States shall notify those limits within 3 months of the entry into force of this Regulation.

4. The limit referred to in paragraph 1 shall not apply to:

   (a) payments between natural persons who are not acting in a professional function, ***except for transactions related to land and real estate, precious metals and stones and other luxury goods above the corresponding thresholds as listed in Annex X***; (939)

   (b) payments or deposits made at the premises of credit institutions. In such cases, the credit institution shall report the payment or deposit above the limit to the FIU ***except for recurrent instalments in accordance with an agreement with the credit institution***.

[19] Council Decision of 29 June 1998 on the consultation of the European Central Bank by national authorities regarding draft legislative provisions (OJ L 189, 3.7.1998, p. 42).

5. Member States shall ensure that appropriate measures, including sanctions, are taken against natural or legal persons ~~acting in their professional capacity~~ which are suspected of a breach of the limit set out in paragraph 1, or of a lower limit adopted by the Member States.

6. The overall level of the sanctions shall be calculated, in accordance with the relevant provisions of national law, in such way as to produce results proportionate to the seriousness of the infringement, thereby effectively discouraging further offences of the same kind.

Article 59a

~~Transfers~~ Payments in crypto-assets without the involvement of a crypto-asset service provider

1. ***Persons trading in goods or providing services may accept or make a transfer in crypto-assets from a self-hosted address only up to ~~exceeding~~ an amount equivalent to EUR 1000 ~~only where the transfer is carried out by means of a crypto-asset service provider authorised under the MiCA Regulation~~, whether the transaction is carried out in a single operation or in several operations which appear to be linked, unless the customer or beneficial owner of such self-hosted address can be identified.***

2. ***The limit referred to in paragraph 1 shall not apply to***

(a) transfers of crypto-assets between natural persons who are not acting in a professional function~~;~~.

(b) transfers of crypto-assets involving a crypto-asset service provider.

3. ***Member States shall ensure that appropriate measures, including sanctions, are taken against natural or legal persons acting in their professional capacity which are suspected of a breach of the limit set out in paragraph 1.***

4. ***The overall level of the sanctions shall be calculated, in accordance with the relevant provisions of national law, in such way as to produce results proportionate to the seriousness of the infringement, thereby effectively discouraging further offences of the same kind.*** (941)

5. ***By [three years after entry into force of this Regulation], the Commission shall assess whether ~~the scope of means of~~ the provisions relating to payment in crypto-assets ~~which may be accepted above the limit~~ referred to in paragraph 1 ~~by persons trading in goods or providing services,~~ should be amended, in light of the regulatory technical standards developed by AMLA in accordance with Article 30b and taking into account technological developments and the framework for a European Digital Identity~~, taking into account relevant regulatory technical standards developed by AMLA in accordance with Article 30b~~. Where appropriate, the Commission shall present a legislative proposal.***

Recital 94

(94) The use of large cash payments is highly vulnerable to money laundering and terrorist financing; this has not been sufficiently mitigated by the requirement for traders in goods to be subject to anti-money laundering rules when making or receiving cash payments of

EUR ~~10 000~~ ***7 000*** or more. At the same time, differences in approaches among Member States have undermined the level playing field within the internal market to the detriment of businesses located in Member States with stricter controls. It is therefore necessary to introduce a Union-wide limit to large cash payments of EUR ~~***10 000 3000 5000***~~ ***7 000***. Member States should be able to adopt lower thresholds and further stricter provisions. ***The Union-wide limit should not be applicable to payments between natural persons who are not acting in a professional function, except for transactions related to land and real estate, precious metals and stones and other luxury goods, and to payments or deposits made at the premises of credit institutions. In the latter case, however, the credit institution should report the payment or deposit above the limit to the FIU. Such reporting should not replace reporting ~~in particular~~ in case of suspicious activities and transactions. Unusually large transactions in cash even below the threshold, including the withdrawal, should be subject to enhanced customer due diligence measures in cases of higher risk and, if necessary, to reporting of suspicions.*** (17, 246, 247, 936, 937, 938)

Recital 94a

(94a) ***Technological developments enable merchants to accept payments in crypto-assets for the provision of goods and services either in store or online. Where such payments are not carried by means of a regulated service providers, the level of traceability to a verified identity may not be sufficient for the purpose of preventing their misuse for money laundering, terrorist financing and predicate offences. The use of these means of payment, in a context of increasing digitalisation, may create a loophole and undermine the effectiveness of the cash limit. While maintaining the possibility to make payments in crypto-assets for goods and services, it is therefore necessary to require merchants to ~~rely on a crypto-asset service provider authorised~~ under MiCA, when accepting accept large payments in crypto-assets only when the customer can be identified. Such limitation should apply to persons trading in goods or providing services and should not be interpreted as a ~~ban~~ restriction on private transactions by means of self-hosted wallets nor as a restriction to the use of self-hosted wallets in the context of commercial transactions, as long as the customer or beneficial owner of the self-hosted address can be identified ~~a crypto-asset service provider is involved~~.***

Recital 95

(95) The Commission should assess the costs, benefits and impacts of lowering the limit to large cash payments at Union level with a view to levelling further the playing field for businesses and reducing opportunities for criminals to use cash for money laundering. This assessment should consider in particular the most appropriate level for a harmonised limit to cash payments at Union level considering the current existing limits to cash payments in place in a large number of Member States, the enforceability of such a limit at Union level and the effects of such a limit on the legal tender status of the euro.

CHAPTER VIII
FINAL PROVISIONS

COMP AI

Article 60 - Delegated acts
Article 61 - Committee
Article 62 – Review
Article 63 - Reports
Article 64 - Relation to Directive 2015/849
Article 65 - Entry into force and application
Recitals 96, 97, 98, 99, 100, 101, 102, 103, 103a

AMs covered: 18 (Rapporteurs), 112 (Rapporteurs), 113 (Rapporteurs), 114 (Rapporteurs), 115 (Rapporteurs), 116 (Rapporteurs), 117 (Rapporteurs), 942 (Left), 943 (Left), 944 (Left), 945 (NI), 950 (Left)
AMs falling: 252 (ECR), 946 (ID), 947 (Renew), 948 (Renew), 949 (Left), 951 (ID)

Article 60

Delegated acts

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 23, 24 ~~and 25~~ ***~~25, 25a~~ and 42*** shall be conferred on the Commission for an indeterminate period of time from *[date of entry into force of this Regulation]*. (112, 942)

3. The power to adopt delegated acts referred to in Articles 23, 24 ~~and 25~~, ***~~25, 25a~~ and 42*** may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. (113, 943)

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 23, 24 ~~and 25~~, ***~~25, 25a~~ and 42*** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of one month of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by one month at the initiative of the European Parliament or of the Council. (114, 944)

Article 61

Committee

1. The Commission shall be assisted by the Committee on the Prevention of Money Laundering and Terrorist Financing established by Article 28 of Regulation *[please insert reference – proposal for a recast of Regulation (EU) 2015/847 - COM/2021/422 final]*. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 62

Review

By *[~~5~~ **3** years from the date of application of this Regulation]*, and every ~~three~~ ***two*** years thereafter, the Commission shall present a report to the European Parliament and to the Council on the application of this Regulation. (115)

Article 63

Reports

By *[~~3~~ **2** years from the date of application of this Regulation]*, the Commission shall present reports to the European Parliament and to the Council assessing the need and proportionality of: (116, 945)

(a) ~~lowering~~ ***amending*** the percentage for the identification of beneficial ownership of legal entities;

ab) introducing a prohibition of nominee arrangements as well as measures to detect undisclosed nominees, including in combination with transparency and licensing measures for different type of nominee arrangements;

ac) extending the prohibition on anonymous accounts to the provision by crypto-asset service providers of privacy wallets, mixers and tumblers;

ad) including as obliged entities in the scope of this Regulation professional sport clubs, sport federations and sport confederations and sport agents in sectors other than football;

ae) including as obliged entities in the scope of this Regulation additional categories of providers of digital services;

(b) ~~further lowering~~ ***amending*** the limit for large cash payments, ***following consultation with the European Central Bank***. (950)

Such reports shall be accompanied, if appropriate, by a legislative proposal.

Article 64

Relation to Directive 2015/849

References to Directive (EU) 2015/849 shall be construed as references to this Regulation and to Directive *[please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final]* and read in accordance with the correlation table set out in Annex IV.

Article 64a
Amendments to Regulation (EU) No xx/2023 [please insert reference to the new Funds Transfer Regulation]

Regulation (EU) No xx/2023 [please insert reference to the new Funds Transfer Regulation] is amended as follows:

(1) Article 23, second paragraph, is replaced by the following:
'The European Banking Authority (EBA) shall issue guidelines by … [18 months after the date of entry into force of this Regulation] specifying the measures referred to in this Article. On ... [18 months after the date of entry into force of this Regulation] the power to issue such guidelines shall be transferred to the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). Guidelines issued by EBA pursuant to this paragraph shall continue to apply until amended or repealed by AMLA.'

(2) Article 25 is amended as follows:

(a) Paragraph 1 is replaced by the following:
'1. The processing of personal data under this Regulation is subject to Regulation (EU) 2016/679. Personal data that is processed pursuant to this Regulation by the Commission, EBA or AMLA is subject to Regulation (EU) 2018/1725.'

(b) Paragraph 4, second subparagraph, is replaced by the following:
'The European Data Protection Board shall, after consulting EBA, issue guidelines on the practical implementation of data protection requirements for transfers of personal data to third countries in the context of transfers of crypto-assets. EBA shall issue guidelines on suitable procedures for determining whether to execute, reject, return or suspend a transfer of crypto-assets in situations where compliance with data protection requirements for the transfer of personal data to third countries cannot be ensured. On ... [18 months after the date of entry into force of this Regulation], the right to be consulted and the power to issue guidelines shall be transferred from EBA to AMLA. Guidelines issued by EBA pursuant to this paragraph shall continue to apply until amended or repealed by AMLA.'

(3) Article 28 is replaced by the following:

'1. Without prejudice to the right to provide for and impose criminal sanctions, Member States shall lay down rules on administrative sanctions and measures applicable to breaches of this Regulation and shall take the measures necessary to ensure that those rules are implemented. The sanctions and measures provided for shall be effective, proportionate and dissuasive and shall be consistent with those laid down in accordance with Chapter VI, Section 4, of Directive (EU) ... [please insert reference to AML Directive].

[deleted]

2. ***Member States shall ensure that, in the event of a breach of this Regulation and where obligations apply to payment service providers and crypto-asset service providers, administrative sanctions and measures can be applied separately and individually to the provider, to its senior management, and to any other natural persons who under national law are responsible for the breach.***

Note
This article aims to horizontally align the provisions in Funds Transfer Regulation with AMLA Regulation, AMLR and AMLD. The modifications compared to existing provisions in FTR are highlighted in yellow. It results from the agreement on the AML horizontal level and follows the legal advice to insert all amending provision in a single legal instrument of direct application.

Article 65

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
It shall apply from *[~~3~~ **2** years from its date of entry into force]*. (117)

This Regulation shall be binding in its entirety and directly applicable in all Member States.

(97) In order to ensure consistent application of AML/CFT requirements, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to supplement this Regulation by adopting delegated acts identifying high-risk third countries, third countries with compliance weaknesses ~~and countries~~ ***~~and specific entities~~*** ~~(18)~~ ~~that pose a threat to the Union's financial system~~ and defining harmonised and proportionate enhanced due diligence measures as well as, where relevant, mitigating measures as well as the regulatory technical standards setting out the minimum requirements of group-wide policies, controls and procedures and the conditions under which structures which share common ownership, management or compliance controls are required to apply group-wide policies, controls and procedures, the actions to be taken by groups when the laws of third countries do not permit the application of group-wide policies, controls and procedures and supervisory measures, the sectors and transactions subject to lower thresholds for the performance of customer due diligence and the information necessary for the performance of customer due diligence***, as well as specific rules and criteria to identify the beneficial owner(s) of legal entities other than corporate entities***. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[20]. In particular, to ensure equal participation in the

[20] OJ L 123, 12.5.2016, p. 1.

preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(98) In order to ensure uniform conditions for the application of this Regulation, implementing powers should be conferred on the Commission in order to identify legal arrangements similar to express trusts governed by the national laws of Member States as well as to adopt implementing technical standards specifying the format to be used for the reporting of suspicious transactions. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[21].

(99) This Regulation respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life (Article 7 of the Charter), the right to the protection of personal data (Article 8 of the Charter) and the freedom to conduct a business (Article 16 of the Charter).

(100) In accordance with Article 21 of the Charter, which prohibits discrimination based on any grounds, obliged entities should perform risk assessments in the context of customer due diligence without discrimination.

(101) When drawing up a report evaluating the implementation of this Regulation, the Commission should give due consideration to the respect of the fundamental rights and principles recognised by the Charter.

(102) Since the objective of this Regulation, namely to prevent the use of the Union's financial system for the purposes of money laundering and terrorist financing, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(103) The European Data Protection Supervisor has been consulted in accordance with Article 42 of Regulation (EU) 2018/1725 [and delivered an opinion on ...[22]],

---

[21] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

[22] OJ C , , p. .