Banks' internal governance obligations vis-à-vis money laundering risks emerging from the new technology-enabled means to transfer funds or value ("crypto assets")

Andrea Minto

Department of Economics, Ca' Foscari University of Venice, Venice, Italy and UiS School of Business and Law, University of Stavanger, Stavanger, Norway

Abstract

Purpose – The new technology-enabled means to transfer funds or value via crypto assets have prompted regulators and supervisors to question the effectiveness of the anti-money laundering (AML) regulatory framework. This paper aims to examine the recent developments of the EU AML legislation – leading up to the 2021 AML package – focusing in particular on the banks' internal governance obligations.

Design/methodology/approach – The analysis is based on the legal dogmatic methodology and is therefore conducted thanks to a critical exam of the current and upcoming EU policy and legislation, taking into account the relevant literature and case-law.

Findings – The recent regulatory developments, culminating in the AML regulation, are strengthening the causal links between ML risk assessment–ML risk exposure–ML risk management, via internal governance procedures. One of the major AML regulatory strategies to react to the new challenges brought up by crypto assets amounts to a stricter and more demanding AML risk management regime imposed on banks.

Originality/value – The originality of this article lies in the analysis of the causal connection between money laundering risk identification and internal governance obligations. In particular, this article examines how the risk assessment will be shaping the organizational procedures, processes and internal functions necessary to manage the money laundering risks.

Keywords EU Anti-Money Laundering Legislation, Money laundering risk, Internal governance, Crypto assets, AML policy

Paper type Research paper

This research was financed by 2022 PRIN PNRR research funding granted by the Italian Ministry of University and Research, project code: 2022 Y4MCWZ, CUP: H53D23011450006, title "Legal uncertainties surrounding financial innovation and their consequences on the effectiveness of Anti-Money Laundering policies: coordinating EU reforms with the Italian regulatory and supervisory frameworks".

Journal of Money Laundering Control
Vol. 27 No. 7, 2024
pp. 43-59
Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-04-2024-0068

1. Introduction

In recent years, *policymakers*, legislators and supervisory authorities have been questioning the effectiveness of existing capital markets legislation *vis-à-vis* the new technology-enabled means to transfer funds or value (i.e. crypto assets) [1].

Fifteen years after the advent of bitcoin, crypto assets still remain quite a conundrum when it comes to their precise legal characterization (Annunziata, 2020; ECB *Crypto-Assets Task Force,* 2019). As well known, in fact, for more than a decade scholarship and jurisprudence alike struggled in defining crypto assets, due to the novelty (and complexity) of the technology adopted. Crypto asset *per se* – i.e. observed as a neutral "digital box" – is but a container of different rights (or value). Consequently, the legal characterization of such digital box will depend on the *actual* rights/value it incorporates and the function it ultimately performs. As a result, crypto assets are to be examined on a case-by-case basis, focusing on the "inside" of such digital asset. The taxonomy thus remains firmly anchored to *what* the rights/value are, irrespective - in principle – of *how* the technology enables such rights to be transferred.

Such assessment brings about material legal consequences, in that the qualification of the crypto asset may, or may not, trigger a specific financial market licensing regime. In case a crypto asset incorporates for instance the rights of a share (presenting equity claims on the issuer, e.g. voting rights, dividends, [. . .]) and therefore qualifies as a financial instrument – or rather "transferable security" within the meaning of Directive 2014 / 65/EU – "MiFID 2" [2] – consequently the business service/activity associated with it might amount to an investment service/activity, thus coming within the scope of application of the MiFID legislation [3]. Differently, should the token qualify as 'electronic money', it will therefore fall within the scope of Directive 2009 / 110/EC (the e-money directive or "EMD2"); in such cases, authorization as an electronic money institution is required to carry out activities involving electronic money pursuant to Title II of the EMD2, unless a limited network exemption applies in accordance with Article 9 of that Directive [4]. Furthermore, since such tokens qualify as "electronic money" for the purposes of the EMD2, they in turn come within the definition of "funds" as set out in point (25) of Article 4 of Directive (EU) 2015 / 2366 (the so called "PSD2"), potentially triggering the licensing regime provided for payment services.

However, other crypto assets present features that made them escape the existing regulatory frameworks, with the risk that each member state could adopt – as it was the case, indeed! – different regulatory and supervisory approaches, opening up venues for regulatory arbitrage and moral hazard (Minto *et al.*, 2021).

Indeed, up till 2023, there was no harmonized bespoke regime for crypto assets at the EU level – setting aside the specific rules introduced by the anti-money laundering regulatory framework, which will be discussed in the next paragraph – thus further exacerbating the risks of regulatory fragmentation to the detriment of the end financial users.

In this context, Regulation (EU) 1114 / 2023 – the *Markets in Crypto Assets Regulation,* hereinafter also referred to as "MiCAR" – aims to minimize such regulatory and supervisory fragmentation by setting out a regime that "*fills-in the gaps*", [5] regulating the crypto assets that are not already covered by existing EU regulatory frameworks (except for e-money tokens, which are a type of crypto assets that seem to justify a two-tier regime EMD2-MiCAR, due to their nature and by reason of the underlying technology) [6]. In this perspective, the MICAR provides for two major substantive sets of rules: one concerning with the issuance, offering and admission to trading of crypto assets, and the other introducing a regime for the provision of services related to crypto assets.

2. Technological evolution as the driving force behind EU anti-money laundering legislation: the challenges of the "crypto economy"

Over the last decade, the EU anti-money laundering (AML) regulatory framework has undergone phases of updates and adjustments, which – far from being concluded – are leading up to an institutional and substantive reform [7].

Undoubtedly, financial innovation has been, and remains, one of the most important driving factors behind the AML regulatory developments lately (ECB Crypto-Assets Task Force, 2019).

Indeed, the new technology-enabled means to transfer funds or value via crypto assets have prompted regulators and supervisors to also question the feasibility of the AML "regulatory net" as to capture those crypto assets.

Policy makers and financial supervisory authorities expressed AML concerns with the production of a wide array of *soft law* acts. At the international level, the first steps in this regard were taken by the *Financial Action Task Force* (FATF), which, as early as June 2014, published a *Report* entitled "*Virtual Currencies: Key Definitions and Potential AML/CFT Risks*" in response to the emergence of virtual currencies and associated payment mechanisms aimed at providing new digital methods of transferring value.

Specifically, the development of platforms and portals enabling for digital onboarding and remote relationships with the client, along with the prospect of anonymous transactions through the use of (more or less) decentralized systems, were considered factors that increased dramatically the AML risks.

In June of the following year, the FATF published a set of *Guidelines* concerning the money laundering and terrorist financing risks specifically associated with products and services based on virtual currencies (*Guidance for a Risk-Based Approach to Virtual Currencies*).

Along with these first "red-flags", the European Supervisory Authorities (ESAs) issued some key soft-law documents and *warnings* – published between 2013 and 2014 and 2016–2019 – emphasizing the need to protect the potential users of these *digital assets*.

Indeed, in July 2014, in its *Opinion on virtual currencies*, the European Banking Authority proposed a functional approach to classify cryptocurrencies in a first attempt to raise awareness of the risks associated with crypto assets (EBA/Op/2014 / 08). This *Opinion* was then followed by other documents and *Discussion Papers*, calling upon the European Commission to include cryptocurrencies within the perimeter of the anti-money laundering framework (EBA/Op/2016 / 14; EBA/Op/2021 / 04), and alerting prospective crypto holders to the risks they could be exposed to when purchasing crypto assets (ESMA, EBA, EIOPA *Joint Warning on Virtual Currencies*, 12 February 2018).

In particular, in the "*Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015 / 849 (4AMLD)*" of 11 August 2016 (EBA/Op/2016 / 07), the EBA overtly bridges the previous *Opinion of* 2014 and the uncertain legal qualification of crypto assets with the risk of money laundering, thus urging the need to adapt the AML framework to the new technology-enabled means of exchange of funds/value.

Interestingly, all such soft acts issued in recent years in this matter (either as "*Opinion*", "*Warning*" or "*Report*") present a two-fold legal basis [8].

On the one hand, they derive from the tasks of promoting a "*common supervisory culture*" pursuant to Article 29 of the respective ESAs establishing regulations (see, e.g. Regulation 1093 / 2010 with regard to the EBA), which entrust the authorities with the task of facilitating the identification of common supervisory practices, as well as ensuring the

consistency of the procedures of the approaches shared by the national competent authorities throughout the Union.

On the other hand, the acts are also based on Article 9 of the ESAs establishing regulations, which is titled "*Tasks relating to consumer protection and financial activities*" (see, again, Regulation 1093 / 2010 for the EBA). The provision states, first, that *"The Authority shall monitor new and existing financial activities and may adopt guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence of regulatory practice*" (par. 2); then, the European Banking Authority "*establishes, as an integral part of the Authority, a Committee on financial innovation, which brings together all relevant competent national supervisory authorities with a view to achieving a coordinated approach to the regulatory and supervisory treatment of new or innovative financial activities and providing advice for the Authority to present to the European Parliament, the Council and the Commission*" (par. 3).

This shows how relevant the contribution of the supervisory authorities is for the law-making process, due to their technical expertise, on the one hand, and – most importantly – to their proximity and direct contact with market practices. It is increasingly evident that the complexity of financial markets imposes the need to have a close scrutiny of the marketplace in order to promptly adapt the checks-and-balances of the relevant regulatory frameworks [9].

In this perspective, the ESMA "*Advice on Initial Coin Offerings and Crypto-Assets*" of January 2019 (ESMA50/157 / 1391) most certainly amounts to a "wake-up call" that urged the European Commission to draw up in September 2020 the proposal for the aforementioned regulation on the "*Market in Crypto Assets*".

With specific regard to the AML ambit, in fact, it was evident the need – as voiced by the ESAs – to account for the new AML risks associated with the innovative technology-enabled means to transfer/exchange funds/value (Kelly, 2015; Halaburda and Sarvary, 2016; Chimienti *et al.*, 2019).

Such a need was in fact satisfied by means of the Directive 2018/843/EU (the so called fifth anti-money laundering directive, in acronym "AMLD5"), which updated Directive 2015/849/EU ("AMLD4") as to introduce the definition of "*crypto currency*" and expand of the list of obliged entities to include (certain!) cryptocurrency service providers.

According to article 3(1)(18) of the IV AML Directive, as amended by the AMLD5, virtual currency means a:

> "[. . .] digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically" [10].

With regard to the list of obliged entities, the revised article 2(1) AMLD4 subjects the "*service providers whose activity consists in the provision of exchange services between virtual and hard currencies*" (lett. *g))* and "*digital portfolio services*" (lett. h) [11] to the AML requirements (i.e. customer due diligence, record-keeping obligations and reporting of suspicious transactions).

This extension of the subjective scope is justified by the wisdom that the alleged anonymity of crypto assets may allow for their potential misuse for criminal purposes [12].

This gives the competent authorities the opportunity to monitor the use of virtual currencies for anti-money laundering purposes and through obliged entities. Such monitoring "*would provide a balanced and proportional approach, safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship"* [13].

In this context, however the broadening of the scope of application of AMLD4 to include those entities exercising an activity related to the provision of crypto-related services (*exchanges* and *wallet providers*) does not entirely solve the root problem of anonymity, since users may carry out transactions even without using such providers, on a *peer-to-peer* basis (e.g. using unhosted wallets).

The recently enacted Regulation (EU) 2023/1113 (the so called "travel rule" regulation) – which shall apply from 30 December 2024 – will amend the subjective scope of the AML regulatory framework [14].

Art. 38 of the travel rule regulation, in fact, recasts AMLD4 to embrace the definitions of crypto assets and crypto assets service providers enshrined in the MICAR. Consequently, "*crypto-asset*" refers to "*a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology*" (see Article 3(1), point (5) MiCAR) [15] and "*crypto-asset service provider*" means a crypto-asset service provider as defined in Article 3(1), point (15) of MiCAR, where performing one or more of the following crypto-asset services: *(a) providing custody and administration of crypto-assets on behalf of clients; (b)operation of a trading platform for crypto-assets; (c) exchange of crypto-assets for funds; (d) exchange of crypto-assets for other crypto-assets; (e) execution of orders for crypto-assets on behalf of clients; (f) placing of crypto-assets; (g) reception and transmission of orders for crypto-assets on behalf of clients; (h) providing advice on crypto-assets; (i) providing portfolio management on crypto-assets; (j) providing transfer services for crypto-assets on behalf of clients*"(see Article 3(1), point (16)).

This update demonstrates – once again – how the AML regulatory net keeps expanding as to align with crypto assets' market practices: at present, in fact, AMLD4 only applies to two categories of crypto-asset service providers, namely, custodial wallet providers and providers engaged in exchange services between virtual currencies and fiat currencies. In order to close existing loopholes in the AML framework, the AMLD4 has been coordinated with all categories of crypto-asset service providers as defined in the MICAR, which covers indeed a broader range of crypto-asset service providers [16].

3. Recent developments to reform the European anti-money laundering framework

As shown, the recent updates of the AML regulatory framework have been driven, amongst other things, by the quest to counter the new AML risks associated with crypto assets.

In addition to what has been done in this respect by the AMLD5, however, the matter just underwent a more profound institutional and substantive restructuring process.

On 20 July 2021, in fact, the European Commission presented its proposal to reform the anti-money laundering and counter-terrorism system, which consisted of four integrated legislative initiatives and namely:

- the 6th Anti-Money Laundering Directive [17];
- the regulation establishing a European *Anti-Money Laundering Authority* or "AMLA [18]";
- the regulation containing directly applicable AML/CFT rules; and
- a revision of the Regulation (EU) No 2015/847 on funds transfers for the purpose of tracking crypto assets transfers (also known as "Travel Rule" Regulation).

The first measure to be taken was the Travel Rule Regulation by means of Regulation (EU) 2023/1113. On 19 June 2024, the AML Regulation [Regulation (EU) 2024/1624, the "AMLR"], the Regulation establishing the Anti-Money Laundering Authority [Regulation (EU) 2024/

1620, the "AMLAR"] and the sixth AML Directive [Directive (EU) 2024/1640, the "AMLD6"] – the remaining three of the four building-blocks of the so called "AML package" – have been published on the Official Journal of the EU, setting in motion a true paradigmatic shift in the institutional and substantive architecture of the field.

These measures aim to refine "*the current EU regulatory framework,* adapting it to new and emerging challenges related to technological innovation, such as virtual currencies*, the increased integration of financial flows in the single market and the global nature of terrorist organisations. These proposals will help create a much more coherent framework to facilitate compliance of operators subject to AML/CFT rules, in particular those operating across borders*" (emphasis added) (European Commission Press Release, 2021).

First of all, as much obvious as it may be, it is worth emphasizing the paradigm shift that the legislator made by moving from a directive-based legislation to a regulation-based framework: since 1991 (when the first AML directive was enacted), and after other four acts of such nature, the decision to abandon the instrument of the directive is a much welcome, and a much needed, step forward in the direction of ensuring a consistent implementation of the AML requirements across countries (namely, customer due diligence, data retention and reporting of suspicious transactions). This holds particularly true since:

> [. . .] markets in crypto-assets are global and thus inherently cross-border. Therefore, the Union should continue to support international efforts to promote convergence in the treatment of crypto-assets and crypto-asset services through international organisations or bodies such as the Financial Stability Board, the Basel Committee on Banking Supervision and the Financial Action Task Force [19].

Secondly, great efforts have been spent to coordinate the new anti-money laundering regime with the other pieces of financial law, especially in the area of digital finance. In such perspective, the regulation on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing [Regulation (EU) 2024/1624, also "AMLR"] – following the steps already taken by the "travel rule" regulation, which amended the AMLD4 in order to incorporate the definitions elaborated by the MiCAR – departs from "sectorial" definitions in favor of the harmonized notions of crypto assets a crypto assets service providers referred to in the MiCAR.

In its Opinion of 16 February 2020 on a Proposal for a Regulation Establishing an Authority to Combat Money Laundering and Terrorist Financing (CON/2022/4), the European Central Bank welcomed the AML package [20]. In another document, the Central Bank expressed its appreciation for the legislative initiatives undertaken, also with reference to the definition of crypto-assets (see *Opinion of the European Central Bank of 16 February 2022 on a proposal for a directive and a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing* (CON/2022/5)).

The reform of the European anti-money laundering institutional and substantive framework thus seems to be motivated, among other things, precisely by the new AML risks associated with crypto assets. In such context, the AMLR intervenes also on the rules concerning the internal organization of credit institutions, which will be examined in the next section.

4. The relevance of internal governance in the context of the AMLR

Within the different trajectories the reform of the EU AML legislation branches out, a relevant one most certainly relates to the effectiveness of the internal governance measures, compliance and risk management.

Internal governance refers to the set of processes, procedures and organizational measures, as well as:

> [. . .] all standards and principles concerned with setting an institution's objectives, strategies and risk management framework; how its business is organised; how responsibilities and authority are defined and clearly allocated; how reporting lines are set up and what information they convey; and how the internal control framework is organised and implemented, including accounting procedures and remuneration policies. Internal governance also encompasses sound information technology systems, outsourcing arrangements and business continuity management [21].

In fact, the AMLR is projected at ramping up and cementing the identification, management and mitigation of money laundering and financing of terrorism risk as an essential component of credit institutions' sound internal governance arrangements and risk management frameworks. In this specific perspective, therefore, the AMLR advances and develops the governance arrangements that credit institutions are required to have in place to ensure sound and effective risk management as provided for in this regard by the relevant requirements of the AMLD4, Directive 2013/36/EU as well as the indications in the EBA guidelines on internal governance [22].

The increased emphasis on internal governance emerges already from how the AMLR is designed.

Unlike the AMLD4, in fact, where this matter is scattered between Article 8 and then Articles 45 and 46, the AMLR shows a clear and neat structure, in that it consolidates all the relevant set of rules in Chapter II, under the heading "*internal policies, procedures and controls of obliged entities*".

The rules on internal governance thus form the first set of obligations, as enshrined in Chapter II, that banks have to comply with. Chapter II is then divided in two Sections: Section I on "*Internal policies, procedures and controls, risk assessment and staff*" and Section II concerning "*Provisions applying to groups*", thus confirming how important they are in the overall architecture of AML requirements.

The AMLR advances the current provisions of the AMLD4 in particular by adding new obligations on the management body that aim to:

- intensify its oversight on the institution's activities;
- foster the implementation of a sound risk culture; and
- strengthen the risk management frameworks of institutions by including the aspect of AML risk factors.

The AMLR does not explicitly set out *ad hoc* organizational obligations concerning the new technology-enabled solutions. Rather, it accounts for crypto assets indirectly, by means of the internal governance obligations that obliged entities – and credit institutions in particular – are subject to.

In such way, in fact, the focus is centered around *how* such innovative technology-enabled means to transfer funds/value may affect money laundering risk. Then, the need to properly and effectively manage such ML risk will translate into organizational obligations.

In other words, the concrete money laundering risk – as arising from the business/operational model of the bank and its specific engagement with crypto assets – will be shaping and determining the internal governance, as a result of the responsibility for the management body to adopt an organizational set-up that is appropriate to manage the money laundering risk the bank is exposed to.

This regulatory approach therefore intensifies the close link between the organizational obligations and the ML risk management, to take into account how the market is developing thanks to new emerging technologies [23].

Article 9 AMLR demonstrates the pivotal role of risk management, in that it requires credit institutions to adopt policies, procedures and controls in order to ensure compliance with the

AML framework in a much more articulated and precise fashion than the corresponding Article 46 AMLD4. In particular, the internal governance should be designed as to 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, as well as to curb the risks of non-implementation and evasion of proliferation financing related targeted financial sanctions [24].

Those policies, procedures and controls have to be proportionate to the nature of the business, including its risks and complexity, and the size of the obliged entity. In particular, Article 9, par. 2, identifies in a detailed fashion the minimum elements of the internal governance structure. Namely, it have to include:

- the carrying out and updating of the business-wide risk assessment;
- the obliged entity's risk management framework;
- customer due diligence;
- reporting of suspicious transactions;
- outsourcing and reliance on customer due diligence performed by other obliged entities;
- record retention and policies in relation to the processing of personal data;
- the monitoring and management of compliance with such internal policies and procedures, the identification and management of deficiencies and the implementation of remedial actions;
- the verification, proportionate to the risks associated with the tasks and functions to be performed, when recruiting and assigning staff to certain tasks and functions and when appointing agents and distributors, that those persons are of good repute;
- the internal communication of the obliged entity's internal policies, procedures and controls, including to its agents, distributors and service providers involved in the implementation of its AML/CFT policies; and
- a policy on the training of employees and, where relevant, agents and distributors with regard to measures in place in the obliged entity to comply with the AML requirements, the "travel rule" Regulation and any administrative act issued by any supervisor.

Furthermore, it is necessary for the obliged entity to have in place internal controls and an independent audit function to test the abovementioned internal policies and procedures. In the absence of an independent audit function, obliged entities may have this test carried out by an external expert.

In designing and implementing the appropriate internal governance measures, the banks' management body has to carry out a business-wide risk assessment, taking into account the risk variables and risk factors indicated by the AMLR [25] as well as the results of risk assessments conducted both by the Commission and by Member States. The self-risk-assessment elaborated and prepared by each bank will then be made available to the supervisory authorities, according to what is already provided for in this regard by the current AML legislation (see in fact Article 8 AMLD4).

The AMLR therefore further consolidates the link between "risk assessment'" and the implementation of the "internal controls", emphasizing the functional relationship of the first (the self-assessment) phase to the second (organizational) phase. The identification of the inherent money laundering and terrorist financing risks amounts thus to a pre-condition to discharge properly the internal governance obligations, in that the policies, procedures, and internal controls will be shaped by the actual nature and level of ML risks the bank is exposed

to. In carrying out their self-assessment, credit institutions are required to take into account the characteristics of their customers, the products, services or transactions offered, the countries or geographic areas concerned, and the distribution channels used: "An appropriate risk-based approach requires obliged entities to identify the inherent risks of money laundering and terrorist financing as well as the risks of non-implementation or evasion of targeted financial sanctions 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, including, for crypto-asset service providers, transactions with self-hosted addresses, 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." (see *recital* 30 AMLR).

The ML self risk-assessment, first, and the ML risk management, after, will be mirroring the changes that are affecting finance, factoring in, amongst other things, the new technology-enabled ways to transfer funds/value as well as the innovative digital venues (platforms, portals, *exchanges*, metaverse and so on).

Indeed, the need to take into consideration all such new products and services in the context of the risk assessment is well expressed by *Recital* 7 AMLR:

> 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 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 (emphasis added).

Consistently with such accentuated role of the internal governance, the AMLR emphasizes the relevance of AML *compliance* as management of the risk arising from the violation of legal, regulatory and self-regulatory provisions concerning the prevention of the use of the financial system for the purposes of money laundering or the financing of terrorism.

In fact, according to Article 11 AMLR the AML compliance crosses the bank from the top management strategic decisions, down to operation of the internal control functions: indeed, such provision is concerned with the board member endowed with the role of "*compliance manager*" on the one hand, and the internal control function of compliance and the "*compliance officer*", on the other.

Pursuant to Article 11(1) AMLR:

> [. . .] Obliged entities shall appoint one member of the management body in its management function who shall be responsible for ensuring compliance with this Regulation, Regulation (EU) 2023/1113 and any administrative act issued by any supervisor ('compliance manager').

This provision replaces Article 46(4) of the current AMLD4, which sets out the obligation to "*identify the member of the management board who is responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this Directive*". This provision raised some interpretative doubts as to whether such board member should be an executive one or not. In this respect, the final text does not seem much clearer than the corresponding AMLD4's provision. Interestingly, the text of the AMLR Proposal was straightforward in that Article 9(1) set out that "obliged entities shall appoint one executive member of their board of directors or, if there is no board, of its equivalent governing body who shall be responsible for the implementation of measures to ensure compliance with this Regulation ('compliance manager'). Where the entity has no governing body, the function should be performed by a member of its senior management".

Thus, the Proposal was formulated in a way that clarified that such role is assigned to one of the members of the administrative body "*with executive functions*". Furthermore, as for the nature of its mandate, it specified that this board member is entrusted with the responsibility for "*implementing the measures aimed at ensuring compliance with this Regulation*" [26].

Despite such a "revirement" by the EU legislators, there casts no doubt that the compliance manager is responsible for the implementation of the obliged entity's policies, procedures and controls thus acting as a member with executive functions.

The compliance manager in fact acts as a medium between the management body and the AML control functions, thus filling in the informational gap between those parties and enabling the board members not only to increase their awareness by creating a new informational channel but also to have a reference person, amongst them, who can be called upon and questioned for matters concerning AML compliance.

This key coordinating role is also confirmed by the compliance manager's duty to submit once a year, or more frequently where appropriate, to the management body a report on the implementation of the bank's internal policies, controls and procedures. According to Art. 11 (6), in fact, "The compliance manager shall regularly report on the implementation of the obliged entity's internal policies, procedures and controls to the management body. In particular, the compliance manager shall submit once a year, or, where appropriate, more frequently, to the management body a report on the implementation of the obliged entity's internal policies, procedures and controls drawn up by the compliance officer, and shall keep that body informed of the outcome of any reviews. The compliance manager shall take the necessary actions to remedy in a timely manner any deficiencies identified".

The report allows the management body to be aware of the situation and, where appropriate, to take the necessary measures to remedy any identified deficiencies in a timely manner.

Article 11(2) and (3) AMLR then regulate the internal control functions.

Para. 2 deals specifically with the so-called "compliance officer", i.e. the person in charge of the compliance function, who will be responsible for the day-to-day operation of the obliged entity's AML/CFT policies.

Interestingly, the person appointed as "compliance officer" will also become responsible for the reporting of suspicious transactions, as provided for in Article 69(6) AMLR.

According to Art. 11(3), obliged entities must provide their internal control functions with adequate resources, including in terms of personnel and technology, commensurate with the size, nature and risks to which they are exposed, and to ensure that the persons responsible for those functions are empowered to propose the measures necessary to ensure the effectiveness of internal policies, controls and procedures [27].

Another area where the upcoming EU AML legislation is expanding relates to the training of personnel. While today the topic is confined to what shortly Art. 46(1)(2) AMLD4 sets out, the AMLR devotes a quite self-explanatory provision – art. 12 – named "*awareness of requirements*".

The intent seems to formalize the indications coming from the EBA into "hard law" provisions, [28] and aimed at emphasizing the importance of corporate culture and training programs.

Thus, Article 12 AMLR provides that obligated entities shall take measures:

> [...] to ensure that their employees or persons in comparable positions whose function so requires, including their agents and distributors are aware of the requirements arising from this Regulation, Regulation (EU) 2023/1113 and any administrative act issued by any supervisor, and of the business-wide risk assessment, internal policies, procedures and controls in place in the obliged entity, including in relation to the processing of personal data for the purposes of this Regulation.

Such measures include the participation of employees in specific, ongoing training programmes to help them recognize operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases. Also the training programmes have to be appropriate to their functions or activities and to the risks of money laundering and terrorist financing to which the obliged entity is exposed.

5. Concluding remarks

In a world characterized by high a pace of digitalization and the emergence of new technology-enabled ways to transfer funds or value, namely by means of crypto assets, the EU AML legislation is adapting by strengthening, amongst other things, the essential link between ML risk assessment and internal governance obligations.

Money laundering risk has always been at the epicenter of EU AML legislation, but lately it has been playing a functional role in shaping the internal organizational obligations imposed on obliged entities.

Even though Directive 1991/308/EEC (AMLD1) and Directive 2001/97/EC (AMLD2) did not explicitly mention it, [29] such regulatory frameworks were already based on ML risk.

In fact, if the objective of this specific regulatory regime has always been to prevent the occurrence of a certain event (the phenomenon of money laundering), it seems at least reasonable - if not obvious - that the set of AML rules, controls and obligations presupposes (and has always been based on) the existence of a risk that these same rules, controls and obligations are projected at managing and possibly minimizing (Pellegrini, 2005; Siclari, 2016).

Although this risk was indirectly highlighted by AMLD3, with the formalization of the so-called *risk-based approach* as the key principle the entire anti-money laundering framework revolves around, [30] the AMLD4 represents the real turning point in that it introduced on the one hand an entire section to the assessment of money laundering risk, [31] and, on the other hand, a map of the risk factors that the obliged entities must take into account in the ambit of the risk self-assessment exercise [32].

Such a trend is confirmed and consolidated in the EU AML package reforming the AML institutional and substantive architecture of this matter.

In particular the AMLR is strengthening the causal links between ML risk assessment–ML risk exposure–ML risk management, via internal governance procedures. Such steps are in fact regulated in greater details than the current AMLD4 and, most importantly, is such a way as to account for the latest market developments. Therefore, one of the major AML regulatory strategies to react to the new challenges brought up by crypto assets amounts to a stricter and more demanding AML risk management regime imposed on banks.

Notes

1. See, e.g., International Monetary Fund (2023); see also, among others, Basel Committee on Banking Supervision, *Prudential treatment of crypto-asset exposures*, *Consultative Document*, June 2022; Financial Stability Board, *International Regulation of Crypto-asset Activities: A proposed framework*, 11 October 2022; Financial Stability Board (2019).

2. Annunziata (2023), Annunziata *et al.* (2021), Brener (2019), Cham *et al.* (2022), Chiu (2017, 2021), I. H.-Y. Chiu, G. Deipenbrock (eds), *Routledge Handbook of Financial Technology and Law*, 1st edn, Routledge, Madir (2021), Minto (2021), Panetta (2022), Zetzsche *et al.* (2018).

The practical importance of the legal qualification of crypto activites also highlighted with regard to the effectiveness of the sanctions applied in the context of the Russia-Ukraine conflict. As is well known, in fact, among the various sanction measures imposed against Russia, there are those relating to financial services, which aim to prevent access to the capital markets of the European Union and to

block the foreign currency reserves held by Russia in the old continent through the exclusion of the main Russian banks from the SWIFT system, the most important financial messaging system in the world (on the objectives see European Commission, *Joint Statement on further restrictive economic measures*, 26 February 2022, STATEMENT/22/1423). See the first actions implemented under Council Regulation (EU) 2022/334 of 28 February 2022 '*amending Council Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*' (Art. 3e, para. 4, "*Transactions related to the management of reserves as well as of assets of the Central Bank of Russia, including transactions with any legal person, entity or body acting on behalf of, or at the direction of, the Central Bank of Russia, are prohibited*") and Council Regulation (EU) 2022/345 of 1 March 2022 "*amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*" (cf. Article 5h, '*It shall be prohibited as of 12 March 2022 to provide specialised financial messaging services, which are used to exchange financial data, to the legal persons, entities or bodies listed in Annex XIV or to any legal person, entity or body established in Russia whose proprietary rights are directly or indirectly owned for more than 50% by an entity listed in Annex XIV*'. The same sanctions concerning the Central Bank and restrictions on the use of SWIFT were later extended to Belarus with the sanctions package of 9 March 2022.

Article 5a of the sanctions package provides that '*It shall be prohibited to directly or indirectly purchase, sell, provide investment services for or assistance in the issuance of, or otherwise deal with transferable securities and money-market instruments issued after 9 March 2022 by: (a) Russia and its government; or (b) the Central Bank of Russia; or (c) a legal person, entity or body acting on behalf or at the direction of the entity referred to in point (b)*'. The same provision then dictated a specific definition – i.e. for the purposes of the measures contained therein – of transferable securities (i.e. "*transferable securities means the following classes of securities which are negotiable on the capital market, with the exception of instruments of payment: (i) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares, (ii) bonds or other forms of securitised debt, including depositary receipts in respect of such securities, (iii) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities*").

Significantly, the Council Regulation (EU) 2022/394 of 9 March 2022 "*amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*" intervened on this point, first highlighting, in recital 6, that "*it is appropriate to further specify the* notion of *'transferable securities' in relation to such assets* [crypto assets] *given their specific nature*", and then proceeding to amend the notion of transferable securities as follows "*in Article 1, the introductory words of point (f) are replaced by the following: "'transferable securities' means the following classes of securities*, including in the form of crypto-assets*, which are negotiable on the capital market, with the exception of instruments of payment'* [. . .]" (emphasis added).

3. See Esma, *Legal qualification of crypto-assets - survey to NCAs*, Annex I, 2019. The European Central Bank in the context of its "*European Central Bank Opinion of 19 February 2021 on a proposal for a Regulation of the European Parliament and of the Council on crypto-asset markets and amending Directive (EU) 2019/1937*" highlights the need to precisely delineate the distinction between crypto assets that can be qualified as financial instruments and those that instead fall within the scope of the MiCAR.

4. See, already before the introduction of the Market in Crypto Asset Regulation (MiCAR), European Banking Authority, *Report with advice for the European Commission on crypto-assets*, 2019, sez. 2.1.1. European Central Bank, *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, 2019.

5. See recital n. 5 of the MiCAR, where, amongst other things, it is pointed out that "*the lack of an overall Union framework for markets in crypto-assets could also lead to regulatory fragmentation, which would distort competition in the internal market, make it more difficult for crypto-asset service providers to scale up their activities on a cross-border basis and would give rise to regulatory arbitrage*".

6. In this respect, it could be deemed that the regulatory engagement with EMTs is departing from the principle of "technology neutrality". See in this perspective recital n. 19 "*Because e-money tokens are also crypto-assets and can also raise new challenges in terms of protection of retail holders and market integrity specific to crypto-assets, they should also be subject to rules laid down in this Regulation to address these challenges to protection of retail holders and market integrity*".

7. On the need to restructure the AML regulatory and institutional frameworks, see e.g. Minto and Rasmussen (2022).

8. As well known, there is a lively debate on the nature of the *soft-law* acts produced by the European financial market supervisory agencies (EBA, ESMA, EIOPA), which has also resulted in some relevant case-law of the European Court of Justice. In the wake of what has already been stated more generally about the *non-binding* nature of *soft law* acts (C-322/88 *Salvatore Grimaldi* v *Fonds des maladies professionnelles*, par. 13), the Court more recently took a position on the nature of such acts in case C-911/19 FBF. The case concerned the possibility for a French credit institution to bring an action under Article 263 TFEU for the annulment of the guidelines issued by the EBA under Article 16 of the EBA Regulation (Regulation 1093/2010). The Court, in setting as a prerequisite for any decision on the annulment of *soft law* instruments the need to determine whether an act produces binding legal effects, held that the guidelines in question are subject to the same rules as recommendations issued by the EBA, which are not binding on the addressees and therefore do not, in principle, have any binding force (see paras. 38 and 42) The Court also referred to Article 16(3) of the aforementioned EBA Regulation, which enshrines the "*comply or explain"* principle, which does not entail an obligation to comply, but merely the need to provide detailed explanations in the event of non-compliance (see para. 45). On the basis of these arguments, the Court concluded that the Guidelines cannot be regarded as producing binding legal effects vis-à-vis the addressees. On this topic, see also Case C-28/15 *Koninklijke KPN NV and Others* v *Autoriteit Consument en Markt* (Second Chamber) paras. 34 and 35; *Belgium* v *Commission*, C-16/16 P, para. 26. In the literature, see e.g. Annunziata (2021); Moloney, (2021), *passim*; Nielsen, *Main Features of the European Banking Union*, in *European Business Law Review, p.* 805 ff., esp. p. 809; Senden (2004).

9. On the concept of 'multiple centres of knowledge construction', see Minto (2018), where extensive bibliographical references on this subject are provided.

10. This definition has been most certainly influenced by the one elaborated by the FATF a few years earlier: "*virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency-i.e., it electronically transfers value that has legal tender status*" (see FATF Report, 2014).

11. According to Article 3(1)(19) AMLD4 "*digital wallet service provider*" means "*an entity that provides services for the safeguarding of private cryptographic keys on behalf of its clients, for the purpose of holding, storing and transferring virtual currencies*".

12. See *recital* 9 AMLD5 describing the essential role of the national financial intelligence units (FIUs) which, in order to counter the aforementioned anonymity-related consequences, "*should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed*".

13. See *recital* 8 AMLD5.

14. As well known, however, the primary objective of Regulation (EU) 2023/1113 is to expand the scope of the legislation on the information accompanying transfers of funds, which, according to Regulation (EU) 2015/847, only applied to transfers of banknotes and coins, scriptural money, and electronic money (indeed, "funds"). Regulation (EU) 2023/1113 repealed Regulation (EU) 2015/847 in order to extend its scope also to cover transfers of virtual assets.

15. Significantly, recital n. 8 specifies that the definition of crypto assets should be future-proof: "*Crypto-assets* [. . .] *should therefore be defined as widely as possible to capture all types of crypto-assets which currently fall outside the scope of Union legislation on financial services*".

16. See recital 59 of the Travel Rule Regulation: "*In particular, with a view to ensuring that crypto-asset service providers are subject to the same requirements and level of supervision as credit and financial institutions, it is appropriate to update the list of obliged entities by including crypto-asset service providers within the category of financial institutions for the purpose of Directive (EU) 2015/849. In addition, taking into account that traditional financial institutions also fall within the definition of crypto-asset service providers when offering such services, the identification of crypto-asset service providers as financial institutions allows for a single consistent set of rules that applies to entities providing both traditional financial services and crypto-asset services. Directive (EU) 2015/849 should also be amended in order to ensure that crypto-asset service providers are able to appropriately mitigate the money laundering and terrorist financing risks to which they are exposed*".

17. COM(2021) 423 *final*.

18. COM(2021) 421 *final*.

19. See Recital n. 8 MiCAR.

20. In its opinion, the Central Bank suggests certain amendments to the draft Regulation with regard to, *inter alia*, the criteria for identifying the obliged entities that will be subject to the direct supervision of the AMLA (the so called selected obliged entities, "SOE"), the cooperation between the AMLA and the Central Bank itself, and the composition of the *governance* structure of the Authority to be established.

21. See EBA, *Guidelines on internal governance under Directive 2013/36/EU,* 2 July 2021). On the definition of internal governance, see, e.g., van Setten (2019); Hopt (2012); BCBS (2015); Miller (2017); Chiu (2015); Vos *et al.* (2019).

22. See EBA, *Guidelines on internal governance under Directive 2013/36/EU, 2 July 2021*, Executive summary: "*in recent years, internal governance issues have received increased attention from various international bodies. Their main aim has been to correct institutions' weak or superficial internal governance practices, as identified during the financial crisis. Recently, there has been a greater focus on conduct related shortcomings, including compliance with the framework to prevent money laundering and terrorist financing and activities in offshore financial centres*".

23. This is well described in recitals 28, 29, 30 and 31 AMLR.

24. The notion of "*targeted financial sanctions*" refers to "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 TEU and Council Regulations adopted on the basis of Article 215 TFEU" (see art. 2 (1)(49) AMLR).

25. Risk factors are but a mere indication and they represent a non-exhaustive list of circumstances to be taken into account. Without prejudice to this, it is worth noticing that the AMLR expands such list of risk factors, as compared to the list that the AMLD4 provides. The final version of the AMLR is the result of the integrations proposed by the European Parliament during the trilogue

in order to widen the sources and indications to be considered (see EUROPEAN PARLIAMENT, *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, Compromise Amendments AML Regulation, 22 March 2023).

26. In this direction, the European Parliament proposed to amend Article 9(1) of the AMLR Proposal as follows "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*' (bold is used in the original text).

27. The importance of the issue of compliance is further confirmed by some amendments that were proposed by the European Parliament on 29 March 2023: see European Parliament, *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, Compromise Amendments AML Regulation, 22 March 2023, bold is used in the original text).

28. See, e.g., EBA, *Guidance on Policies and Procedures on Compliance Management and the Role and Responsibilities of the AML Officer under Article 8 and Chapter VI of Directive (EU) 2015/849*, 14 June 2022, partic. number 56 ff. where it is emphasized that the AML Officer should coordinate the preparation and implementation of an AML training programme for all staff. Then, for the purposes of Article 46(1). 1, of Directive (EU) 2015/849, the AML Officer "*should assess, in addition to basic education, the specific training needs within the credit or financial institution and ensure that appropriate theoretical and practical training is provided to persons exposed to different levels of ML/TF risks, such as: (a) persons working in the anti-money laundering function under the responsibility of the AML officer; (b) persons in contact with customers or in charge of executing their transactions (employees, agents and distributors); (c) persons responsible for the development of internal procedures or tools applicable to activities that could be sensitive to ML/TF risk*" (cf. Guideline No. 58).

29. While in the AMLD1 the term 'risk' is even absent, the AMLD2 refers to the "*risk of money laundering*" only once, with regard to the hypothesis of remote operations. Notably, Article 3(11) on the duty of identification (later replaced by customer due diligence by AMLD3) required obliged persons to take specific and adequate measures to compensate for the greater risk of money laundering arising from establishing business relations or carrying out a transaction with a customer who is not physically present for identification purposes.

30. Starting from recital 22, which sets out the underlying reasons for the risk-based approach to Articles 8, 9 and 13 on customer due diligence, the AMLD3 is characterized by many references to the money laundering risk as the benchmark for the correct implementation of the AML requirements.

31. Section Two of Chapter I (containing the 'general provisions' that inform the whole matter) deals precisely with the identification, analysis and monitoring of money laundering risk.

32. Despite the fact that money laundering risk and its assessment - with all the consequences in terms of internal governance - are at the heart of European legislation, it seems curious that it has never been defined.

A definition of money laundering risk is, however, to be found in some national regimes. For instance, the Bank of Italy defines money laundering risk as the "*risk arising from the violation of legal, regulatory and self-regulatory provisions aimed at preventing the use of the financial system for the purposes of money laundering, terrorist financing or the financing of programmes for the development of weapons of mass destruction*" (see *Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari,* 2019, Part One, Section I).

References

Annunziata, F. (2020), "Speak, if you can: What are you? An alternative approach to the qualification of tokens and initial coin offerings", *European Company and Financial Law Review*, Vol. 17 No. 2, p. 129.

Annunziata, F. (2021), "The remains of the day: EU financial agencies, soft law and the relics of meroni", European Banking Institute Working Paper Series – no. 106, available at: https://ssrn.com/abstract=3966980

Annunziata, F. (2023), "An overview of the markets in Crypto-Assets regulation (MiCAR)", European Banking Institute Working Paper Series no. 158, available at: https://ssrn.com/abstract=4660379 or http://dx.doi.org/10.2139/ssrn.4660379

Annunziata, F., Douglas, A.W., Ross, B.P. and Zetzsche, D.A. (2021), "The markets in crypto-assets regulation (MiCA) and the EU digital finance strategy", *Capital Markets Law Journal*, Vol. 16 No. 2, p. 203.

Brener, A. (2019), "Payment service directive II and its implications", in T. Lynn, J. Mooney, P. Rosati, M. Cummins (Eds), *Disrupting Finance, Palgrave Studies in Digital Business and Enabling Technologies*, Palgrave Pivot, New York, NY.

BCBS (2015), "Guidelines. Corporate governance principles for banks", July p. 3.

Cham, T.H., Casanova, J. Savoie M. (Eds), (2022), *Payment Services – Law and Practice*, Edward Elgar Publishing, London.

Chimienti, M.T., Kochanska, U. and Pinna, A. (2019), "Understanding the crypto-asset phenomenon, its risks and measurement issues", *ECB Economic Bulletin*, Vol. 5.

Chiu, H.-Y. (2015), *Regulating (from) the Inside–The Legal Framework for Internal Control in Banks and Financial Institutions*, Oxford University Press, Oxford.

Chiu, I.H.-Y. (2017), "A new era in fintech payment innovations? A perspective from the institutions and regulation of payment systems", *Law, Innovation and Technology*, Vol. 9 No. 2, p. 190.

Chiu, I.H.-Y. (2021), *Regulating the Crypto Economy: Business Transformations and Financialisation*, Hart Publishing, Oxford.

ECB Crypto-Assets Task Force (2019), "Crypto-Assets: implications for financial stability, monetary policy, and payments market infrastructures", Occasional Paper Series no. 223.

European Commission Press Release (2021), "Defeating financial crime: Commission reviews rules against money laundering and terrorist financing", 20 July, available at: https://ec.europa.eu/commission/presscorner/detail/it/ip_21_3690

FATF Report (2014), "Virtual currencies key definitions and potential AML/CFT risks", June, available at: www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html

Financial Stability Board (2019), Decentralised financial technologies: report on financial stability, regulatory and governance implications, June.

Halaburda, H. and Sarvary, M. (2016), *Beyond Bitcoin: The Economics of Digital Currencies*, Palgrave Macmillan, New York, NY.

Hopt, K. (2012), "Corporate governance of banks after the financial crisis", in Wymeersch, E Hopt, K. and Ferrarini G (Eds), *Financial Regulation and Supervision—A Post Crisis Analysis*, Oxford University Press, Oxford, pp. 11-17

International Monetary Fund (2023), "Elements of effective policies for crypto assets", IMF Policy Papers, February.

Kelly, B. (2015), *The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World*, John Wiley and Sons, NJ.

Madir, J. (2021), *FinTech Law and Regulation, Elgar Financial Law and Practice*, 2nd edn Edward Elgar Publishing, Chelthenam.

Miller, G.P. (2017), *The Law of Governance, Risk Management, and Compliance*, 2nd ed Wolters Kluwer, Baltimore, pp. 709-784.

Minto, A. (2018), "Enlisting internal and external financial gatekeepers: problems of multiple centres of knowledge construction", *European Journal of Risk Regulation*, Vol. 9 No. 2, p. 283.

Minto, A. (2021), "The legal characterization of Crypto-Exchange platforms", *Global Jurist*, Vol. 22 No. 1, p. 1.

Minto, A. and Rasmussen, N.S. (2022), "Approaching the danske bank scandal in a 'tragedy of the commons' perspective: implications for anti-money laundering institutional design and regulatory reforms in Europe", *European Company and Financial Law Review*, Vol. 19 No. 2, pp. 305-338.

Minto, A., Prinz, S. and Wulff, M. (2021), "A risk characterization of regulatory arbitrage in financial markets", *European Business Organization Law Review*, Vol. 22 No. 4, p. 719.

Moloney, N. (2021), *The Age of ESMA Governing EU Financial Markets*, Hart Publishig, London.

Panetta, F. (2022), "For a few cryptos more: the wild west of crypto finance", Speech, European Central Bank.

Pellegrini, M. (2005), "Anti-Money laundering legislation in the light of the proposal of the third EC directive", *European Business Law Review*, Vol. 16 No. 5, p. 1181.

Senden, L. (2004), *Soft Law in European Community Law*, Hart Publishig, London, p. 112.

Siclari, D. (2016), "The new Anti-Money laundering law", *First Perspectives on the 4th European Union Directive*, Springer, London.

van Setten, L. (2019), "Risk, risk management, and internal controls", in Busch, D. Ferrarini, G. and Van Solinge G. (Eds), *Governance of Financial Institutions*, Oxford University Press, Oxford, p. 221.

Vos, T.K., Morbee, S., Cools. and M., Wyckaert. (2019), "A cross-sectoral analysis of corporate governance provisions", in Colaert, V. Busch, D. and Incalza T. (Eds), *European Financial Regulation. Levelling the Cross-Sectoral Playing Field*, Hart publishing, London, p. 182.

Zetzsche, D.A., Buckley, R.P., Arner, D.W. and Barberis, J.N. (2018), "From FinTech to TechFin: the regulatory challenges of Data-Driven finance", *New York University Journal of Law and Business*, Vol. 14, p. 393.

Corresponding author
Andrea Minto can be contacted at: andrea.minto@unive.it