GIMENEZ - SALINAS
ABOGADOS

CRITICAL ANALYSIS OF THE TECHNICAL STANDARD (RTS) REGARDING THE NOTIFICATION BY CERTAIN FINANCIAL ENTITIES OF THEIR INTENTION TO PROVIDE CRYPTOASSET SERVICES

ESMA CONSULTATION PAPER ON THE FIRST PACKAGE OF TECHNICAL STANDARDS (TECHNICAL STANDARDS) ON MiCA (July 2023)

BARCELONA
Balmes, 209, planta 2
08006 - Barcelona
+34 93 218 40 00

MADRID
Alberto Bosch 5, bajo D.
28014 - Madrid
+34 91 037 84 81

www.gimenez-salinas.es
info@gimenez-salinas.es

INDEX

1. OBJECTIVE

The Regulation on cryptoasset markets (MiCA) was published in the Official Journal of the European Union on June 9, 2023. The European Securities and Markets Authority (ESMA) has been empowered to develop technical standards and guidelines specifying certain provisions. ESMA will publish three consultation papers in July 2023, October 2023, and the first quarter of 2024.

This consultation paper is the first of three consultation papers. The purpose of the document is to gather views, comments, and opinions from stakeholders and market participants on the proper implementation of MiCA.

ESMA will consider the comments received in this consultation before September 20 and expects to publish a final report and submit draft technical standards to the European Commission for approval no later than June 30, 2024.

2. KEY HIGHLIGHTS

MiCA requires ESMA to develop a series of Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS), and Guidelines, many of which will be developed in close collaboration with the European Banking Authority (EBA).

This first consultation package covers five (5) RTS projects and two (2) ITS projects on: (i) notification by certain financial entities of their intention to provide services related to cryptoassets; (ii) authorization of cryptoasset service providers; (iii) handling complaints by cryptoasset service providers; (iv) identification, prevention, management, and disclosure of conflicts of interest; and (v) proposed acquisition of a qualified stake in a cryptoasset service provider.

In this note, we analyze the first RTS project on the notification by certain financial entities of their intention to provide cryptoasset services. Our analysis is conducted under the assumption that the entity is a credit institution.

Article 60 of MiCA sets out the notification requirements for certain financial entities intending to offer services related to cryptoassets. According to Article 60 of MiCA, such entities must submit the notification to the National Competent Authority (NCA) of their home member state.

Article 60 outlines the information that must be included in the notification. This includes the following key elements:

- An operations program detailing the types of services related to crypto-assets it intends to offer, including how and where these services will be marketed.
- A description of internal control mechanisms regarding anti-money laundering and counter-terrorism financing obligations.
- A description of the procedure for segregating clients' crypto-assets and funds.
- If intending to provide custody and administration of crypto-assets on behalf of clients, a description of the custody and administration policy.
- Documentation of information technology and communication (ITC) systems and security arrangements.

- f. If intending to provide crypto-asset order execution services on behalf of clients, a description of the execution policy.
- g. If intending to provide crypto-asset exchange services for funds or other crypto-assets, a description of the trading policy.

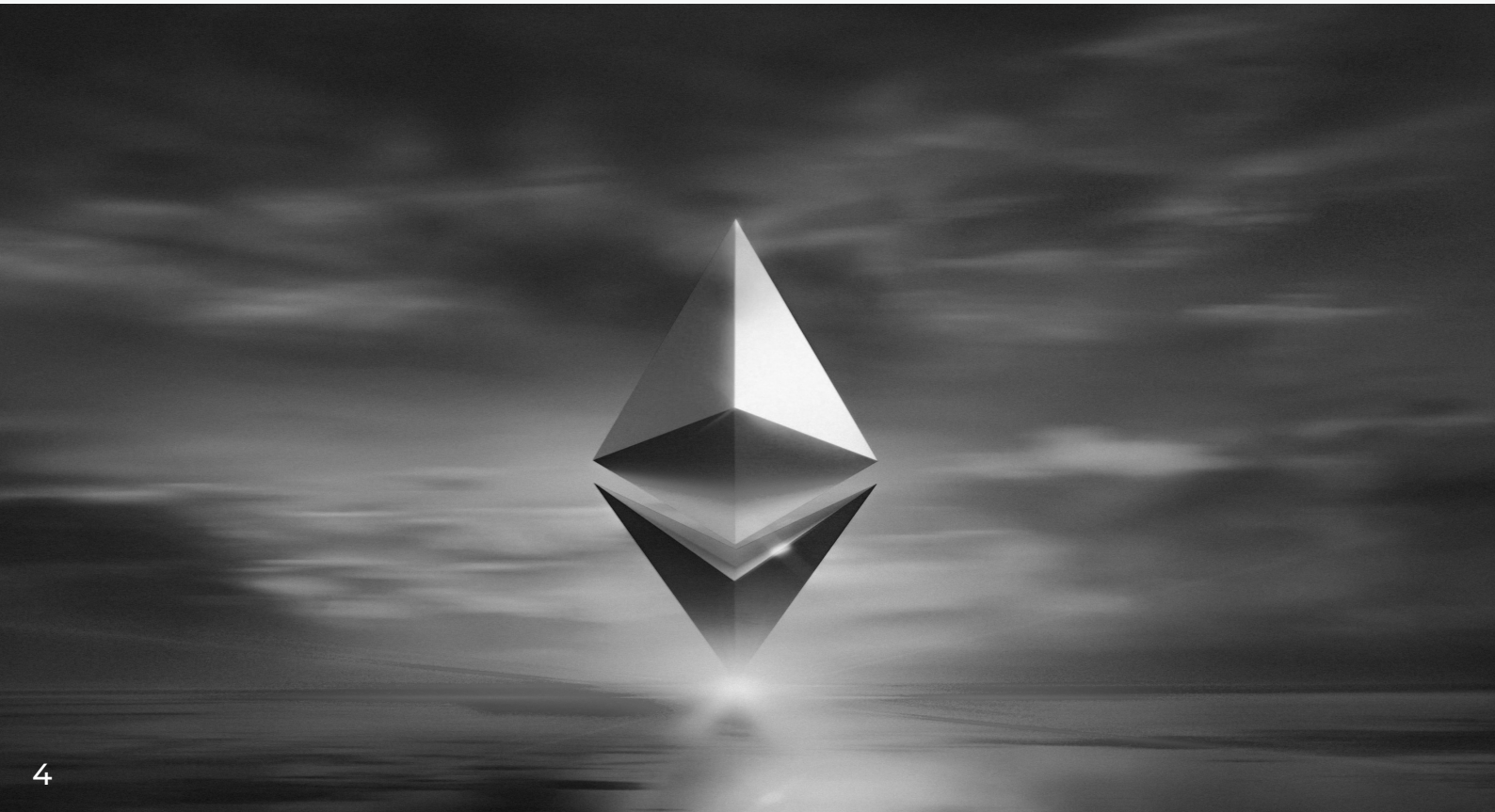
MiCA establishes that entities that already hold a license to offer financial services and have undergone the authorization process with their National Competent Authority (NCA) in their home member state (such as investment firms, credit institutions, etc.) do not need to go through the entire authorization process again. However, MiCA requests that they complement it with specific information for the provision of crypto-asset-related services to enable effective supervision.

ESMA believes that the requirements for credit institutions to perform these activities do not increase costs. However, ESMA requests confirmation from credit institutions through this consultation document, and this premise should be carefully analyzed.

As we will discuss in the following section, regarding each requirement, it is difficult to think that a credit institution can provide crypto-asset services without making significant changes to its corporate governance structure, including control structures. Several factors complicate the ability of a credit institution to provide crypto-asset services without significant changes to its control structure. Some of these factors include the nature of crypto-assets, ongoing uncertainties about whether certain crypto-assets fall within MiCA's scope, hybrid natures in many crypto-assets, whether decentralized finance (DeFi) offerings by some operators are genuinely decentralized and therefore within or outside MiCA's scope, etc.

In our opinion, it is not easy to assume, for example, that a New Products Committee of a credit institution with its traditional structure can handle the assessment of a new crypto-asset product or service. Another example could be that controls and risk committees would not require substantial modification to handle custody services for crypto-assets. We can think of many examples where it seems unlikely that current control structures would be sufficient and would not require substantial modifications that come with significant costs.

Therefore, the first conclusion is that ESMA does not seem to have accurately assessed the potential costs for a credit institution if it wanted to comply with ESMA's requirements to provide crypto-asset services. What we will analyze in the next section is whether some of the requirements imposed by ESMA could be eliminated or modified to have a lesser impact on costs without compromising risk control.



3. CRITICAL ANALYSIS OF REQUIREMENTS

3.1 Operations Program

The entity must provide the competent authority with the operations program for the next three years, including all of the following information:

(a) If the entity is part of a group, an explanation of how the entity's activities will align with the group's strategy and how they will interact with the activities of other group entities, including a description of the current and planned organization and structure of the group.

This requirement seems unnecessary since the credit institution will have already notified the NCA or the ECB of this explanation in the past. It does not appear necessary solely for the purpose of starting to provide crypto-asset services, unless such services are provided jointly with another subsidiary of the group. Therefore, it should not be necessary to submit this information again.

(b) An explanation of how the activities of subsidiary entities, including regulated entities in the group, are expected to affect the entity's activities. This explanation should include a list and information about subsidiary entities, including regulated entities, services provided by these entities (including regulated services, activities, and types of clients), and the domain names of each website operated by such entities.

This requirement seems unnecessary since the credit institution will have already notified the NCA or the ECB of this explanation in the past. It does not appear necessary solely for the purpose of starting to provide crypto-asset services, unless such services are provided jointly with another subsidiary of the group. Therefore, it should not be necessary to submit this information again.

(c) A list of crypto-asset-related services that the entity intends to provide, as well as the types of crypto-assets to which the crypto-asset-related services will refer.

The problem is that until a clear definition of which crypto-assets are considered financial instruments (to which MiCA does not apply) is established, it will be difficult to delineate this issue. This is because depending on the definition adopted in the EU, some crypto-assets that we might consider within the scope of MiCA today could fall outside it or vice versa (although the latter possibility seems more difficult). Furthermore, it would seem more reasonable to consider a gradual implementation of services. In other words, it does not seem appropriate for an entity, given all the uncertainties related to these products and services, to notify the provision of all services for implementation from the outset.

(d) Other planned activities, regulated and unregulated, including whether the entity intends to offer crypto-assets to the public or seek the admission to trading of crypto-assets and, if so, what type of crypto-assets.

(e) The geographical distribution of the crypto-asset-related services that the entity plans to provide, including information about the domicile of target clients.

While this requirement is entirely reasonable and can surely be adapted to the passporting regime that the entity already has for other banking and financial services, the problem could arise in relation to certain services such as managing a trading platform. Without delving into the topic of "reverse solicitation" here, it is true that in managing a trading platform, the geographical aspect largely fades, and the controls that the entity must have to ensure that the offer of these services is considered to take place within the jurisdictions of its target clients become more challenging.

(f) Categories of potential clients for whom the notifying entities' services are intended.

(g) A description of the means of access to the entity's crypto-asset-related services by clients, including all of the following information:

- (i) The domain names of each website or other ICT-based application through which the entity will provide crypto-asset-related services and information about the languages in which the website will be available, the types of crypto-asset-related services that will be accessible through it, and, if applicable, from which EU Member States the website will be accessible.

- (ii) The name of any ICT-based technology application available for clients to access crypto-asset-related services, the languages in which it is available, and which crypto-asset-related services can be accessed through it.

The need to include information in subsections (i) and (ii) seems excessive. This requirement not only forces the entity to incur costs that may later be seen as unnecessary but also can mean a clear competitive disadvantage initially and with each modification it wants to make since it would be subject to communication. This requirement (g) should be more general and only state that the entity on its website will clearly explain to clients the different websites or apps available for clients in relation to these services, and the explanations on them will be clear and in a language understandable by the target client.

This requirement is not designed for the times of web 3, web 4, etc. Its requirement could be a limitation for the credit institution.

(h) Planned marketing and promotion activities and agreements for crypto-asset-related services, including:

- (i) All marketing media that will be used for each of the services, the identification media that the entity intends to use, and information about the relevant category of clients and types of crypto-assets.

- (ii) The languages that will be used for marketing and promotion activities.

This requirement is unnecessary since the credit institution would have already notified the ANC or the ECB of this explanation in the past for its activity. It does not seem necessary to do so solely for the purpose of starting to provide crypto asset services, unless such services significantly change what the institution has been doing. Therefore, it should not be necessary to submit this information again.

(i) A detailed description of the human, financial, and technical resources allocated to the planned crypto asset services, as well as their geographical location.

This requirement is reasonable but complex. The complexity does not only lie in the almost certain need to hire suitable profiles with adequate knowledge but also in the difficulty of assessing, for example, the appropriate allocation of financial and technical resources. MiCA aims to establish European standards on some technical aspects, but it seems reasonable to think that crypto asset services require global standards. However, the current state of the art in this field is far from reaching an agreement on these global standards.

(j) The outsourcing policy of the institution and a detailed description of the planned outsourcing agreements of the institution, including intra-group agreements, how the institution intends to comply with the requirements set out in Article 73 of Regulation (EU) 2023/1114. The institution must also include information about the functions or the person responsible for outsourcing, the resources (human and technical) allocated to the control of the functions, services, or activities outsourced from related agreements, and the risk assessment related to outsourcing.

This requirement is reasonable. The difficulty lies, as always, in determining whether outsourcing is essential or not, and therefore, the need for authorization for such outsourcing. And this problem is exacerbated because in such novel products as crypto assets, it will be more difficult to determine the essentiality of some outsourcing.

(k) The list of entities that will provide outsourced services, their geographical location, and the relevant outsourced services.

(l) A forecast of the accounting plan at the individual level and, where applicable, at the consolidated and sub-consolidated group level in accordance with Directive 2013/34/EU. The financial forecast should consider any intra-group loans granted or to be granted by the institution.

(m) Any exchange of crypto assets for funds and other activities related to crypto assets that the institution intends to carry out, even through any decentralized finance applications with which the institution intends to interact on its

own.

This requirement is reasonable in terms of the need to determine the services to be provided.

When the institution intends to offer the service of receiving and transmitting orders for crypto assets on behalf of clients, it must provide the competent authority with a copy of the policies and procedures and a description of the agreements ensuring compliance with the requirements set out in Article 80 of Regulation (EU) 2023/1114.

This requirement seems reasonable. However, the difficulty lies in determining in the policies and procedures how the reception and transmission of orders operate depending on the nature of each crypto asset and its issuer.

When the institution intends to offer the service of placing crypto assets, it must provide the competent authority with a copy of the policies, procedures, and a description of the agreements in place to comply with Article 79 of Regulation (EU) 2023/1114, as well as Article 9 of [RTS on conflicts of interest of crypto asset service providers (CASPs)].

3.2 Money Laundering and Terrorism Financing Detection and Prevention

The credit institution must provide the competent authority with information about its internal control mechanisms, systems, and procedures for assessing and managing the risks related to money laundering and terrorism financing, including all of the following information:

(a) The assessment of inherent and residual money laundering and terrorism financing risks associated with its business, including risks related to the institution's customer base, the services provided, the distribution channels used, and the geographical areas of operation.

(b) The measures that have been or will be implemented to prevent identified risks and comply with applicable laws on anti-money laundering and terrorism financing obligations, including the risk assessment process, policies and procedures to meet customer due diligence requirements, and policies and procedures to detect and report suspicious transactions or activities.

(c) Detailed information on how these mechanisms, systems, and procedures are suitable and proportionate to the scale, nature, inherent risk of money laundering and terrorism financing, the range of crypto asset-related services provided, the complexity of the business model, and how they ensure compliance with Directive (EU) 2015/849 and Regulation (EU) 2023/1113.

(d) The identity of the person responsible for ensuring compliance with anti-money laundering and terrorism financing obligations, and evidence of the person's skills and experience.

(e) The agreements, human resources, and financial resources dedicated to ensuring that personnel receive adequate training on anti-money laundering and terrorism financing matters (annual indications).

(f) A copy of the anti-money laundering and terrorism financing prevention procedures and systems.

(g) The frequency of the assessment of the adequacy and effectiveness of these mechanisms, systems, and procedures, as well as the person or function responsible for such evaluation.

These requirements of sections (a), (b), (c), (d), (e), (f), and (g) are unnecessary since the credit institution would have already notified the ANC of this explanation in the past for its activity. It does not seem necessary to do so solely for the purpose of starting to provide crypto asset services, unless such services significantly change what the institution has been doing. Therefore, it should not be necessary to submit this information again.

3.3 Business Continuity

The institution must submit to the competent authority a detailed description of the institution's business continuity plan, including the steps that will be taken to ensure the continuity and regularity of the provision of the institution's crypto asset services.

The description should include details demonstrating that the established business continuity plan is appropriate and that provisions have been made to maintain and periodically test it, with regard to critical or important functions supported by third-party service providers, also taking into account the potential eventuality that the quality of the provision of such functions deteriorates to an unacceptable level or fails. Such plans must also consider the potential impact of insolvency or other failures of third-party service providers, the death of a key person, and, where relevant, political risks in the jurisdiction of the service provider.

This requirement is unnecessary since the credit institution would have already notified the ANC of this explanation in the past for its activity. It does not seem necessary to do so solely for the purpose of starting to provide crypto asset services, unless such services significantly change what the institution has been doing. Therefore, it should not be necessary to submit this information again.

3.4 ICT Systems and Related Security Provisions

The institution must submit to the competent authority all of the following information:

(a) Technical documentation of the ICT systems, the DLT infrastructure on which it is based, when relevant, and security provisions. The applicant must include a description of the agreements, policies, procedures, systems, protocols, tools, and human resources for ICT implemented to ensure compliance with Regulation (EU) 2022/2554.

This requirement is reasonable.

(b) If available, the results of audits or tests of the institution's ICT systems conducted by external and independent parties in the last 3 years, including a review of the source code of smart contracts used and/or developed by the institution.

This requirement seems unnecessary since the credit institution would have already notified the ANC of this explanation in the past for its activity. It does not seem necessary to do so solely for the purpose of starting to provide crypto asset services.

(c) A non-technical description of the information provided in sections (a) and (b).

This requirement is reasonable regarding section (a).

3.5 Segregation of Crypto Assets and Customer Funds

When the institution intends to hold crypto assets belonging to customers or the means of access to such crypto assets or customer funds (other than electronic money tokens), the institution must provide the competent authority with a detailed description of its procedures for segregating crypto assets and customer funds, including all of the following information:

(a) How the institution ensures that:

- (i) Customer funds are not used for its own account.
- (ii) Crypto assets belonging to customers are not used for its own account without explicit customer consent.
- (iii) The wallet addresses of customer crypto assets are different from the institution's own wallet address.

This requirement should only apply if the credit institution is the custodian of the crypto assets or, exceptionally, if, although not being the custodian, it has executed the original purchase order on behalf of the customer but in its own name and for exceptional reasons could not temporarily validate the final acquisition by the customer. If the credit institution is the custodian, as it is the private keys that are being custodied and not the crypto asset itself, what needs to exist is a clear ownership path by the customer. It is important to note that standards will emerge, such as the one that emerged in 2023 called ERC-4337 (account abstraction), which will facilitate the use and maintenance of private accounts for users.

(b) A detailed description of the cryptographic key approval system and the safeguarding of cryptographic keys (e.g., multi-signature wallets).

This requirement seems reasonable if the credit institution is the custodian of the crypto assets.

(c) How the institution segregates customer crypto assets.

This requirement should only apply if the credit institution is the custodian of the crypto-assets or, exceptionally, if, even though it is not the custodian, it has executed the original purchase order on behalf of the client, but for exceptional reasons, the acquisition could not be temporarily validated by the client.

(d) A description of the procedure to ensure that client funds (other than electronic money tokens) are deposited with a central bank or a credit institution by the end of the next working day after they are received. This requirement does not apply to a credit institution.

(e) If the entity does not intend to deposit funds with the relevant central bank, what factors does the entity consider when selecting credit institutions to deposit client funds, including the entity's diversification policy, if available, and the frequency of reviewing the selection of credit institutions to deposit client funds. This requirement does not apply to a credit institution.

(f) How the entity ensures that clients are informed in a clear, concise, and non-technical language about the key aspects of the entity's systems, policies, and procedures to comply with Article 70(1), (2), and (3) of Regulation (EU) 2023/1114. This subparagraph (f) should be limited to those requirements that are applicable to credit institutions.

3.6 Custody and Administration Policy

The entity intending to provide custody and administration services for crypto-assets on behalf of clients must provide the competent authority with the following information:

(a) A description of the agreements related to the type or types of custody offered to clients, a copy of the entity's standard agreement for the custody and administration of crypto-assets on behalf of clients, as well as a copy of the custody policy summary available to clients in accordance with Article 75(3) of Regulation (EU) 2023/1114.

(b) A description of the entity's custody and administration policy, including a description of identified sources of operational and information technology risks for the secure custody and control of clients' crypto-assets or means of access to clients' crypto-assets, along with a description of:

- (i) Procedures and a description of agreements to ensure compliance with Article 75(8) of Regulation (EU) 2023/1114.
- (ii) Procedures, systems, and controls to manage these risks, even when custody and administration of crypto-assets on behalf of clients is outsourced to a third party.
- (iii) Procedures and a description of systems to ensure the exercise of rights associated with crypto-assets by clients.
- (iv) Procedures and a description of systems to ensure the return of crypto-assets or means of access to clients.

The nature of crypto-assets makes custody arguably the most complex yet essential service for widespread crypto-asset adoption. The risks associated with crypto-asset custody are multifaceted and will require a thorough analysis by the entity to properly reflect agreements and obligations. It's important to note that what is truly being custody are the private keys providing access to crypto-assets, not the crypto-assets themselves. It's important to consider that standards, such as ERC-4337 (account abstraction) introduced in 2023, will facilitate the use and maintenance of private accounts for users.

The operational requirement to mitigate operational risks in crypto-asset custody is very high. This will demand from entities a risk-cost-benefit analysis that complicates the adoption of custody services initially.

(c) Information about agreements to ensure that crypto-assets or means of access to crypto-assets of clients are clearly identified as such.

(d) Information about agreements to minimize the risk of loss of crypto-assets or means of access to crypto-assets

(e) When the crypto-asset service provider has delegated the provision of custody and administration services for crypto-assets on behalf of clients to a third party:

- (i) Information about the identity of any third party providing custody and administration services for crypto-assets and their status as an authorized entity under Article 59 of Regulation (EU) 2023/1114.
- (ii) A description of the functions related to the custody and administration of crypto-assets delegated by the crypto-asset service provider, the list of delegates and sub-delegates (as applicable), and any conflicts of interest that may arise from such delegation.
- (iii) A description of the supervision procedures related to such delegations or sub-delegations.

The requirements in subparagraphs (c), (d), and (e) are entirely reasonable, but it remains very difficult for entities at this time to assess the operational and investment requirements.

3.7 Operating Rules of the Trading Platform and Market Abuse Detection

An entity intending to operate a trading platform for crypto-assets must provide the competent authority with a description of the following:

(a) Rules related to the admission of crypto-assets to trading.

(b) The approval process for admitting crypto-assets to trading, including due diligence conducted in accordance with Directive (EU) 2015/849 before admitting the crypto-asset to the trading platform.

(c) The list of any category of crypto-assets that will not be admitted to trading and the reasons for such exclusion.

(d) Policies, procedures, and fees for admission to trading, along with a description, when relevant, of membership, discounts, and related conditions;

(e) Rules governing order execution, including procedures for canceling executed orders and disclosure of such information to market participants;

(f) Procedures adopted to assess the suitability of crypto-assets in accordance with Article 76(2) of Regulation (EU) 2023/1114;

(g) Systems, procedures, and agreements implemented to comply with Article 76(7), points (a) to (h), of Regulation (EU) 2023/1114;

(h) Systems, procedures, and agreements to make bid and ask prices and the depth of trading interest at those prices publicly available for crypto-assets through their trading platforms;

(i) Fee structures and justification of how they comply with the requirements set out in Article 76(13) of Regulation (EU) 2023/1114;

(j) Procedures and systems for keeping data related to all orders available to the competent authority or the mechanism to ensure that the competent authority has access to the order book;

(k) Regarding transaction settlement:

- (i) Whether final settlement of transactions is initiated on the distributed ledger or outside the distributed ledger;

- (ii) The timeframe within which final settlement of crypto-asset transactions is initiated;
- (iii) Systems and procedures for verifying the availability of funds and crypto-assets;
- (iv) Procedures for confirming relevant transaction details;
- (v) Measures in place to limit settlement failures;
- (vi) Definition of the moment when settlement becomes final and the point at which final settlement begins after the execution of the transaction.

(l) A description of the procedures and systems for detecting and preventing market abuse, including information on communications to the competent authority about potential cases of market abuse.

Notifying entities intending to operate a trading platform for crypto-assets must provide the competent authority with a copy of the trading platform's operating rules and any procedures for detecting and preventing market abuse.

The requirements in all the above subsections are reasonable. All requirements, both in substance and form, are logical, but some are complex to implement in the current state of the art of crypto-assets.

3.8 Exchange of Crypto-assets for Funds or Other Crypto-assets

An entity intending to exchange crypto-assets for funds or other crypto-assets must provide the competent authority with the following information:

(a) A description of the established trading policy in accordance with Article 77(1) of Regulation (EU) 2023/1114.

(b) A description of the methodology for determining the price of the crypto-assets that the entity proposes to exchange for funds or other crypto-assets in accordance with Article 77(2) of Regulation (EU) 2023/1114, including how market volume and volatility affect the pricing mechanism.

This requirement seems reasonable. However, at this time, it is challenging to determine how market volatility affects the pricing mechanism. Moreover, in certain types of crypto-assets, this can be very complex.

3.9 Execution Policy

An entity intending to provide order execution services for crypto-assets on behalf of clients must provide the competent authority with a description of its execution policy, including the following:

(a) Arrangements to ensure that the client has consented to the execution policy before order execution;

(b) A list of crypto-asset trading platforms on which the entity will rely for order execution in accordance with Article 78(6) of Regulation (EU) 2023/1114;

(c) Which trading platforms it intends to use for each type of crypto-asset and confirmation that it will not receive any form of compensation, discount, or non-monetary benefit in return for directing received orders to a specific crypto-asset trading platform;

(d) How price execution factors, costs, speed, probability of execution and settlement, size, nature, custody conditions of crypto-assets, or any other relevant factors are considered as part of all necessary steps to achieve the best possible result for the client;

(e) If applicable, information about arrangements to inform clients that the entity will execute orders outside a trading platform and how it will obtain the client's prior and express consent before executing such orders;

(f) Information on how the client is warned that any specific instruction from a client may prevent the entity from taking the steps it has designed and implemented in its execution policy to achieve the best possible result for the

execution of those orders regarding the elements covered by those instructions;

(g) Information on the process of selecting trading venues, execution strategies employed, procedures and processes used to analyze the quality of execution obtained, and how the entity monitors and verifies that the best possible results were achieved for clients.

(h) Information about the rules to prevent the misuse of any information related to client orders by employees of the entity;

(i) Information about the rules and procedures on how the entity will disclose to clients information about its order execution policy and notify them of any material changes in its order execution policy.

(j) Information about the rules for demonstrating compliance with Article 78 of Regulation (EU) 2023/1114 to the competent authority, upon request of the authority.

All requirements in the above subsections are reasonable. Regarding subsection (d), if the entity providing order execution services for crypto-assets is not also the one managing the trading platform, it should contract with those platforms with clear policies in this area. Concerning subsection (f), it will be essential if the entity is not the custodian of the crypto-assets to inform the client that the execution performed will require their validation in a timely manner with private keys.

3.10 Provision of Advisory or Portfolio Management Services for Crypto-assets.

An entity intending to provide advisory services for crypto-assets or portfolio management of crypto-assets must provide the competent authority with the following information:

(a) The procedures, policies, and a detailed description of the arrangements implemented by the entity to ensure compliance with Article 81(7) of Regulation (EU) 2023/1114. This information should include details on:

- (i) Mechanisms for effectively monitoring, evaluating, and maintaining the knowledge and competence of natural persons providing advice or portfolio management services for crypto-assets.
- (ii) Arrangements to ensure that natural persons involved in providing advice or portfolio management are aware of, understand, and apply the entity's internal policies and procedures designed to ensure compliance with Regulation (EU) 2023/1114, especially Article 81(1) of Regulation (EU) 2023/1114 and anti-money laundering and counter-terrorist financing obligations under Directive (EU) 2015/849.
- (iii) The amount of human and financial resources planned to be allocated annually by the entity for the professional development and training of natural persons providing advice or portfolio management for crypto-assets.

(b) A description of the arrangements adopted by the entity to ensure that natural persons providing advice on behalf of the entity have the necessary knowledge and experience to conduct the suitability assessment mentioned in Article 81(1) of Regulation (EU) 2023/1114.

This requirement seems reasonable. However, compliance is very challenging at this time. Leaving aside e-money tokens and tokens referenced to other assets, in relation to other crypto-assets, the difficulty lies in each specific crypto-asset. Knowledge of the world of crypto-assets in general and how they function is required, as well as knowledge of the specific crypto-asset. The difficulty here is in determining the requirements of internal policies and procedures to determine who and when sufficient knowledge of a specific crypto-asset has been acquired.

3.11 Transfer Services

An entity intending to provide transfer services for crypto-assets on behalf of clients must provide the competent authority with the following information:

(a) Details about the types of crypto-assets for which the entity intends to provide transfer services.

(b) The policies, procedures, and a detailed description of the arrangements implemented by the entity to ensure compliance with Article 82 of Regulation (EU) 2023/1114, including detailed information on the entity's agreements and human and technological resources deployed to address risks promptly, efficiently, and comprehensively during the provision of transfer services for crypto-assets on behalf of clients, considering possible operational failures and cybersecurity risks.

(c) If relevant, a description of the entity's insurance policy, including insurance coverage for damage to client crypto-assets that may result from cybersecurity risks.

(d) Arrangements to ensure that clients are adequately informed about the policies, procedures, and arrangements mentioned in point (b).

The requirements in subsections (a), (b), and (d) are reasonable. However, regarding subsection (c), this requirement does not seem to take into account the nature of crypto-assets. If the entity providing crypto-asset transfer services is not also the custodian, it is not understood how cybersecurity damage can occur. In other words, cybersecurity damage can only occur if the service provider for the transfer is also the custodian.

4. CONCLUSIONS

The most important conclusions that can be drawn from the reading of this first draft of the ESMA Technical Standard (RTS) on the notification by certain financial entities of their intention to provide crypto-asset services (Consultation Paper, July 2023) are, in our opinion, as follows:

1.- ESMA's consideration that the requirements for credit institutions for carrying out these activities do not increase costs is incorrect.

2.- There are requirements that should not be required again from credit institutions unless the new crypto-asset products or services substantially modify what they have already communicated to the ANC or the ECB. In these cases, it is missed that ESMA has not expressly established this exception by stating in each of these cases a clause like "It will not be necessary to communicate this information again if the credit institution has already communicated this information to the ANC or the ECB previously, and it has not been substantially modified by the new crypto-asset products or services provided by the entity." The most important sections to which this should apply are:

- 2.1. Some aspects of the Operations Program explained in this Note.
- 2.2. Anti-money laundering and counter-terrorist financing prevention.

3.- Some requirements seem excessive. We refer, for example, to the already explained need to include a description of the means of access to the entity's crypto-asset-related services by clients. This requirement would not only make the entity incur costs that may later be seen as unnecessary but also may represent a clear competitive disadvantage compared to others at the outset and with each modification that the entity wants to make since it would be subject to communication. This requirement should be more general.

4.- Some requirements are reasonable from a legislative policy perspective but very difficult to implement at this time due to the state of the art of crypto-assets. The most important sections to which this should apply are:

- 4.1. Custody service. The operational requirement to mitigate operational risks in crypto-asset custody is very

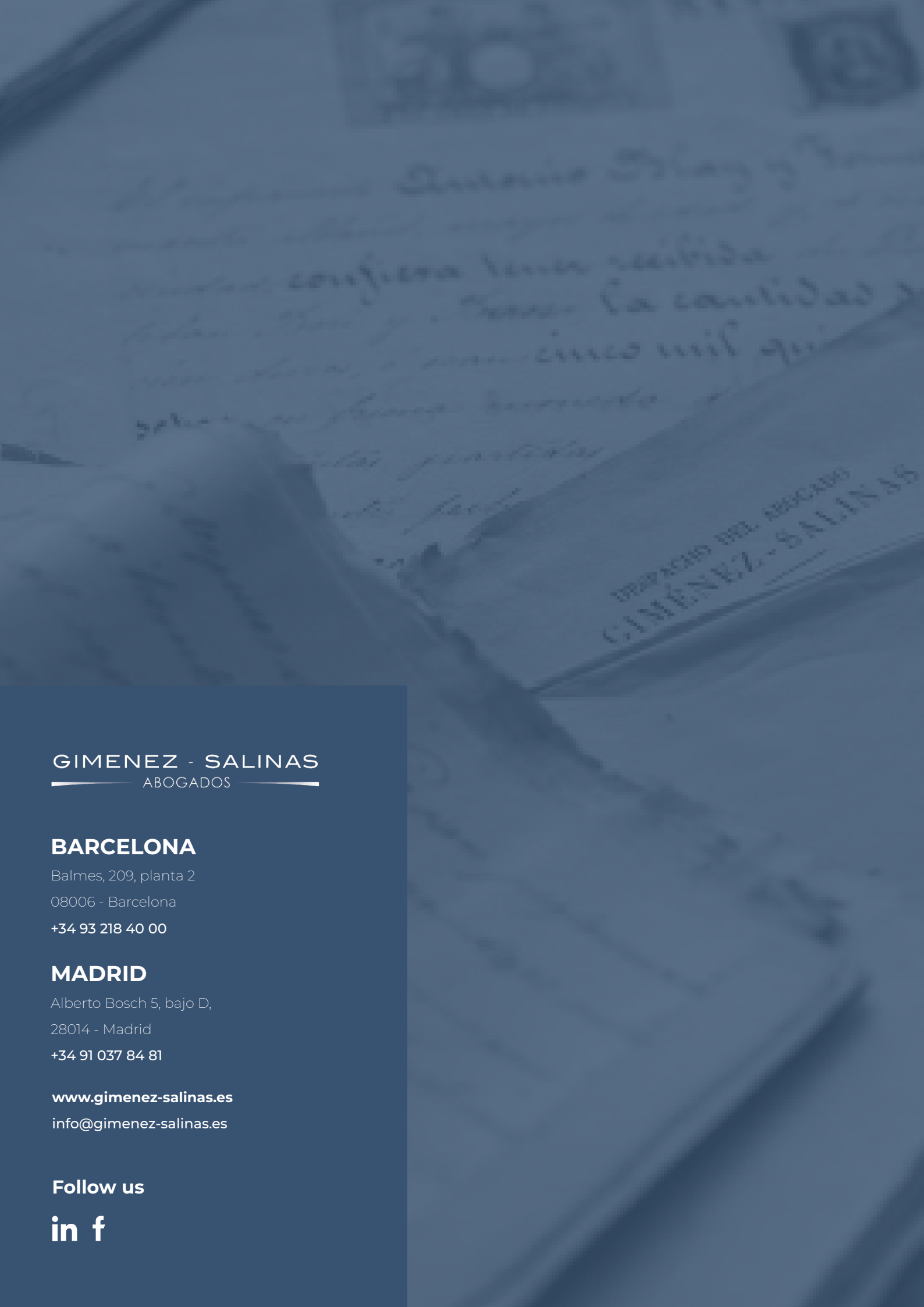
high. This will require entities to conduct a cost-benefit-risk analysis that hinders the adoption of custody services initially. *If the regulator wants to provide more transparency to the world of crypto-asset holding and have holders transfer custody, it should try to regulate requirements and demands from another perspective.

- 4.2. Advisory service. The regulator should seriously consider whether it wants to treat advisory services for crypto-assets that are considered financial instruments (not subject to MiCA) in the same way and, therefore, require the same requirements for crypto-assets that do not have such consideration.

5.- Some requirements do not seem to take into account either the nature of crypto-assets or the operational structure underlying them. This makes implementation very difficult. In these cases, our opinion is that ESMA should refine the requirements a bit more, taking into account this nature and structure. The most important sections to which this should apply are:

- 5.1. Transfer services. If the entity providing crypto-asset transfer services is not also the custodian, it is not understood how cybersecurity damage can occur. In other words, cybersecurity damage can only occur if the service provider for the transfer is also the custodian.

- 5.2. Segregation of crypto-assets. This requirement should only apply if the credit institution is the custodian of the crypto-assets or in other exceptional cases already explained in this Note.



GIMENEZ - SALINAS
ABOGADOS

BARCELONA

Balmes, 209, planta 2
08006 - Barcelona
+34 93 218 40 00

MADRID

Alberto Bosch 5, bajo D,
28014 - Madrid
+34 91 037 84 81

www.gimenez-salinas.es
info@gimenez-salinas.es

Follow us