PAUL HASTINGS

Stay Current

June 2024

Follow @Paul_Hastings

MiCA – ESMA's Mandates for Crypto Market Abuse, Suitability and Crypto Transfer Services

By Arun Srivastava, Nina Moffatt, Konstantin Burkov, Bhavesh Panchal, & David Wormley

Introduction

Crypto-asset firms are increasingly focused on the impact of MiCA[1] on their businesses both from the perspective of high-level strategy and in relation to changes to their day-to-day compliance arrangements. MiCA represents a seismic shift in compliance standards. While 29 December 2024, when MiCA's rules on the provision of crypto-asset services comes into force, is many months off, firms will need time to build the required compliance systems and processes as well as prepare to operate to the new standards that MiCA will introduce.

U.K.-registered crypto-asset businesses should also take note of MiCA requirements, given that the U.K. is expected to introduce similar regulatory requirements. Many U.K. firms also have affiliates operating in the EU who will be subject to MiCA. The new EU rules will also be relevant to U.K. firms who wish to service clients in the EU and MiCA will change market access rules.

In this note, we review MiCA requirements relating to market abuse, suitability, and transfer services.

MiCA and Level-Two Requirements

MiCA was published in the Official Journal of the EU on 9 June 2023 and entered into effect on 29 June 2023. As with most EU-level legislation, the MiCA Regulation will be accompanied by Regulatory Technical Standards and Guidelines. These have been worked on by the European Banking Authority and by the European and Securities Market Authority ("ESMA").

The third—and final—Consultation Paper ("CP") was published by ESMA on 25th March 2024. The CP addressed four mandates covering the following:

1. The prevention and detection of market abuse in relation to crypto-assets;
2. Suitability requirements for advice and portfolio management services in crypto-assets;
3. Transfer services for crypto-assets; and
4. The maintenance of systems and security access protocols.

[1] The Markets in Crypto Assets Regulation (Regulation (EU) 2023/1114)

The consultation process has very recently ended.

MiCA draws heavily on concepts found in other EU-level financial services legislation. It is not surprising, therefore, that the draft ESMA RTS and Guidelines promulgated under the above mandates are modelled on other EU legislation. For example, the Guidelines proposed by ESMA for suitability standards (see 2 above) closely follow suitability requirements under the EU Markets in Financial Instruments Directive ("MiFID"), while the requirements relating to crypto-asset transfer services (3 above) follow the requirements set out in the Second Payment Services Directive ("PSD2").

There is clear benefit in carrying across to the crypto world certain terms and concepts that the financial services industry is already familiar with from other EU legislation, whether in the banking, investment services, or payments fields. However, a key question is whether existing concepts have been appropriately modified for application in the crypto sector.

Market Abuse

ESMA's latest CP discusses market abuse issues in the context of the crypto market and contains a draft Commission Delegated Regulation ("CDR") on market abuse for crypto transactions. By its own admission, ESMA has modelled the CDR on the EU's Market Abuse Regulation that applies to the securities sector.

As already noted, using existing securities regulations as a template for the new crypto rules is understandable and not objectionable. However, one potential criticism is that ESMA has not sufficiently sought to address the fundamental differences between the securities sector and the crypto sector. Some key differences include the following:

- The crypto market is a truly decentralised global market that operates 24 hours per day, year-round.
- In contrast, the securities market is still centralised and geographically siloed, lending itself more obviously to the implementation of regulatory frameworks such as those for addressing market abuse. The nature of the crypto market means that many activities will simply be out of reach of regulators and beyond the capacity of U.K. and EU firms to monitor, detect, and deter.
- Securities issuers are typically established in the jurisdiction in which their securities are listed, and the majority of trading in the issuer's securities will take place in their "home" jurisdiction.
- This centralised model is more amenable to a system where the home Competent Authority is responsible for the listing of securities and for the supervision of trading venues on which the relevant trading occurs and where any abusive conduct is most likely to take place.
- There are also differences in the concept of what constitutes "inside information" for the crypto sector. For securities issuers, commercially sensitive information relating to an operating company is easily understood as "relevant" to an investment decision. With crypto-assets, however, the "relevance" of commercially sensitive information is not as readily apparent.

MiCA Requirements

Title VI of MiCA establishes rules to deter market abuse with respect to trading of crypto-assets. As part of these rules, MiCA prohibits insider dealing, unlawful disclosure of inside information, and market manipulation, and it includes specific obligations for the prevention and detection of abusive behaviours.

Persons Professionally Arranging or Executing Transactions

Article 92(1) of MiCA requires that persons professionally arranging or executing transactions ("PPAETs") in crypto-assets should have in place effective arrangements, systems, and procedures to prevent and detect market abuse.

A key issue, therefore, is what types of business should be included in the definition of a PPAET. Drawing on the MAR regime for securities, ESMA has determined that this concept should be construed broadly.

ESMA has confirmed that while Crypto-Asset Service Providers ("CASPs") operating a trading platform are not specifically mentioned in Article 92(1) of MiCA, they should nevertheless be considered PPAETs and therefore subject to the new market abuse regime.

In addition to this, ESMA's draft CDR makes clear that the following are in scope of the concept of PPAETs:

- reception or transmission of orders for crypto-assets on behalf of clients;
- execution of orders for crypto-assets on behalf of clients;
- portfolio management of crypto-assets;
- exchange of crypto assets for funds or for other crypto assets; and
- persons dealing on own account in crypto-assets on a professional basis or as part of their business activity.

ESMA states that an open question remains as to whether other contributors of the crypto ecosystem will also be considered PPAETs and specifically calls out:

- miners/validators; and
- CASPs providing custody and administration of crypto-assets on behalf of clients.

Our view is that it would not be appropriate to extend market abuse regulation to such participants. Miners and validators fall outside the scope of the MiCA-regulated sector, and it would not be appropriate to include them, particularly where the large majority of persons engaged in these activities are likely to be located outside the EU. Custodians are not in a position to police market abuse activities given their limited role and should also be outside scope.

Ongoing Requirements

MiCA also prescribes ongoing requirements for crypto firms in scope of the market abuse regime. These are developed in the ESMA draft CDR.

Firms in scope will be required to ensure:

- effective and ongoing monitoring of all orders received and transmitted, and of all transactions in crypto-assets executed, for the purposes of preventing, detecting, and identifying orders and transactions that could constitute market abuse;
- effective and ongoing monitoring for the purposes of detecting and identifying other aspects of the functioning of distributed ledger technology, such as the consensus mechanism, where there might exist circumstances indicating that market abuse has been committed, is being committed, or is likely to be committed; and
- the transmission of Suspicious Transaction and Order Reports ("STORs") to competent authorities in accordance with the requirements set out in MiCA using the prescribed template.

The draft CDR requires that firms, on a proportionality basis, employ software systems that assist the prevention and detection of market abuse. The systems and procedures are required to include software capable of deferred automated reading, replaying, and analysing of order book data and to have sufficient capacity to operate in an algorithmic trading environment.

The above procedures will need to be accompanied by arrangements and procedures that ensure an appropriate level of human analysis in the monitoring and processing arrangements that a firm puts in place.

The draft CDR permits the delegation of these processes on the usual outsourcing principles whereby the firm retains responsibility and must continue to have resources available in house to monitor these functions.

The proposals from ESMA in relation to ongoing obligations appear reasonable, though they clearly present a barrier to entry to smaller, less well-resourced firms. Firms will need to ensure appropriate levels of investment in technology and human resources to implement transaction monitoring.

In addition, MiCA requires PPAETs to report to the competent authority of the Member State where they are registered or have their head office (or in the case of a branch, the Member State where the branch is situated) any reasonable suspicion regarding an order or transaction, as well as other aspects of the functioning of the distributed ledger technology such as the consensus mechanism, where there might be circumstances indicating the existence of market abuse. ESMA notes that MiCA is clear when indicating that orders, transactions, and other aspects of distributed ledger technology may suggest the existence of market abuse such as the well-known Maximum Extractable Value ("MEV"), whereby a miner/validator can take advantage of its ability to arbitrarily reorder transactions to front-run a specific transaction(s) and therefore make a profit.

Suitability Assessments

The CP also discusses draft guidelines issued in support of MiCA's suitability assessment arrangements.

Article 81(1) of MiCA requires CASPs that provide portfolio management or advice on crypto-asset investment to conduct an assessment of whether the crypto-asset service, or crypto-assets more generally, are suitable for clients.

In particular, the suitability assessment should take into consideration the client's:

- knowledge and experience in investing in crypto-assets;

- investment objectives, including risk tolerance;
- financial situation, including their ability to bear losses; and
- basic understanding of the risks involved in purchasing crypto-assets.

The results of the suitability assessment should enable CASPs to recommend to clients or prospective clients whether or not the crypto-assets are suitable for them in accordance with their risk tolerance and ability to bear losses.

To support the implementation of the suitability assessment, Article 81(15) of MiCA mandates ESMA to issue guidelines specifying the criteria for the suitability assessment. The draft guidelines are included in Annex III of the CP ("Guidelines") and can be summarised as follows:

Guideline	Description
1. Information to clients about the purpose of the suitability assessment and its scope	CASPs need to inform clients clearly and simply about the suitability assessment and its purpose, which is to enable the CASP to act in the client's best interest. In providing this information, CASPs need to make clear that they are responsible for determining what is suitable and should not encourage clients to tailor answers to the outcome they wish for (i.e., reverse-engineer the suitability assessment). This means that any assessment tools or questionnaires should be gauged appropriately to prevent gaming of the system. Where a CASP provides robo-advice, they will need to provide a "very clear explanation of the exact degree and extent of human involvement". They will also need to provide clients with a description of the sources of information used to generate the services. For instance, the CASP should explain whether responses to any questionnaire might be the sole basis for the robo-advice or whether the CASP takes into account other information, such as other information provided by the client at different stages of the service. This Guideline also considers how information should be disclosed. An example given is emphasising relevant information through the use of pop-up boxes.
2. Arrangements necessary to understand clients	Suitability assessments have typically taken the form of questionnaires, whether completed in a fully digitised manner or through a combination of digitisation and discussion. CASPs should ensure that their questions are specific enough, are likely to be understood correctly, and are designed to get the information required for the suitability assessment. CASPs will need to ensure that their questions are suitably tailored to the services that they offer and the demographic that they target. This means that questions should not just seek to extract information directly relevant to the relevant criteria, but they should also seek to extract information that is indirectly related to the relevant criteria. For instance, an analysis of a client's financial situation may require obtaining information on the client's: marital status, family situation, age, employment situation, need to liquidity in certain investments, or need to fund a future financial commitment.

Guideline	Description
3. Extent of information to be collected from clients (proportionality)	CASPs should obtain from clients such information as is necessary for the CASP to understand the essential facts about the client and to have a reasonable basis for determining that the specific transaction be recommended. The information collected can be proportionate to the service offered, which will need to be determined by the CASP both vis-à-vis its service offering and the service it provides to clients. In determining what is necessary, CASPs should consider: • the type of crypto-assets or transactions that may be recommended/entered into (including the complexity and level of risk); • the nature and extent of the service that the CASP may provide; • the needs and circumstances of the client (e.g., CASPs should collect more information from vulnerable clients); and • the features of the client (e.g., their level of sophistication, knowledge of investing—including in relation to crypto-assets—and their financial situation, amongst other matters). When determining the client's **knowledge and experience**, CASPs should gather information on: • the types of service, transaction, and financial products with which the client is familiar; • whether the client understands distributed ledger technology and the risks associated with it; • the nature, volume, and frequency of the client's transactions and the period over which they have been carried out (which would include understanding the client's knowledge of specific types of crypto-assets); and • the level of education, and profession or relevant former profession of the client or potential client. When assessing the client's **investment objectives**, CASPs should seek to understand the length of time for which the client wishes to hold the investment, their preferences regarding risk-taking, and their risk profile. The information collected about a client's **financial situation** should include: • the client's regular and total income, and their sources and frequency of income; • the client's assets, including savings, investment, and real property; and • the client's regular financial commitments.

Guideline	Description
4. Reliability of client information	The Guidelines seek to ensure that CASPs gather reliable information from clients. This involves CASPs educating clients on the importance of providing reliable information, ensuring that any questions asked are likely to be understood by the clients, and taking steps to ensure the consistency of client information. The Guidelines provide examples of how this Guideline can be met—for instance, when determining a client's risk profile, CASPs could present practical examples to the client of positive and negative scenarios. Similarly, CASPs should avoid asking broad questions with binary responses. Where CASPs use assessment tools, they should also ensure that there are reviews of the tools to ensure their ongoing suitability.
5. Updating client information	To ensure that CASPs have an ongoing understanding of the client's situation, they should seek to ensure that they identify which information that they collect should be updated, at what frequency, and as a result of what trigger events (i.e., changes in the client's risk profile). CASPs will therefore need to employ systems and controls to review and determine the method for updating this information. In any event, MiCA requires all suitability assessments are updated at least every two years.
6. Client information for legal entities or groups	MiCA requires a policy and/or procedure to be prepared which sets out, in relation to legal entities (e.g., companies/partnerships), who should be subject to the suitability assessment and how this should be done in practice (i.e., which individual within the company's knowledge and experience should be assessed). The financial situation and risk profile assessment should be that of the company rather than the individual.
7. Arrangements necessary to understand crypto-assets	CASPs will need to implement objective procedures, methodologies, and tools that allow them to appropriately consider the different characteristics and relevant risk factors of each crypto-asset they recommend or invest in on behalf of clients.
8. Arrangements necessary to ensure the suitability of crypto-assets or crypto-asset services	This Guideline brings together the foregoing to create the overall suitability assessment. It requires CASPs to establish policies and procedures that match the characteristics and risks of crypto-assets (see Guideline 7) with the characteristics, needs, and risk profile of their client under the suitability assessment. The policies and procedures should enable the CASP to ensure that: • there is an appropriate degree of risk diversification; • the client has an understanding of the risk-return profile; • the client's financial situation is sufficient to finance the transaction; and • illiquid crypto-asset investments take into account the client's investment time horizon. The application of the knowledge and experience elements of the suitability assessment should be conducted at a crypto-asset level. Depending on the complexity of the crypto-assets, it should take into

Guideline	Description
	account the client's knowledge in the specific crypto-assets, not just the type of crypto-assets (e.g., stablecoins). The application of the financial situation and investment objectives should be conducted at the level of the client's portfolio as a whole. Where the CASP uses automated tools to conduct the suitability assessment, it should ensure that it regularly monitors and tests the algorithms that underpin the suitability assessment. ESMA has set out various expectations on CASPs using tools. These expectations mirror operational resilience requirements seen in the traditional finance sectors, including system design documentation, testing strategies, change management, error handling, and governance.
9. Costs and complexity of equivalent products	CASPs are required to provide clients with information regarding equivalent crypto-assets in terms of their ability to meet the client's needs and circumstances, such as crypto-assets with similar risk-return profiles. This will require a consideration of all costs and charges involved, which includes costs such as third-party costs like gas fees (if relevant). Where a more costly or complex crypto-asset is chosen over an equivalent crypto-asset, CASPs should document and justify those decisions for review by compliance and internal audit functions.
10. Costs and benefits of switching investments	Where CASPs switch crypto-assets in a portfolio, they should have policies and procedures in place that govern the analysis of the costs and benefits. CASPs are expected to demonstrate that the expected benefits of switching are greater than the costs. The costs and benefits analysis should take into account monetary and non-monetary factors, including: • the expected net return of the alternative transaction vs the existing transaction; • any changes in the client's circumstances and needs; • any changes in the crypto-asset's features and/or market circumstances; and • benefits to the client's portfolio stemming from the switch, such as diversification, risk profile alignment, liquidity improvements, or reductions in credit risk. Blanket switches applied to common portfolio strategies do not necessarily require a costs-and-benefits analysis against each of the individuals invested in that strategy. However, CASPs would need to have appropriate controls in place to determine whether there are particular characteristics of certain client that might require more discrete analysis. Costs-and-benefits analyses for switches within bespoke mandates should be performed at the individual client level.

Guideline	Description
11. Qualifications of staff	CASPs should ensure that staff involved in the material aspects of the suitability process have an adequate level of knowledge, skills, and expertise with regards to crypto-assets and crypto-asset services. This will require assessments of staff and corresponding training to ensure staff meet the minimum requirements. Staff that are ancillary to the suitability assessment should also possess the necessary skills, knowledge, and expertise for their role. For instance, this may capture those setting up questionnaires or algorithms governing suitability assessments.

Commentary

In preparing the Guidelines, ESMA—as with other elements of MiCA—has sought to lean on concepts and guidelines that apply to the traditional securities and investments sector, and, in particular, under MIFID II. This is an understandable position given ESMA's observation that persons providing portfolio management and investment advice in relation to securities and investments under MIFID II may also extend their activities to cover crypto-assets under MICA.

The benefits of this approach means that firms can apply a single set of principles across different types of asset classes, streamlining their operations and compliance efforts. It also means that historic lessons learned by managers/advisors in the traditional finance spheres can be taken forward for corresponding crypto-asset services.

However, ESMA has noted that there are some differences between the MIFID II and MICA regimes, albeit the differences are minor. For instance:

- The MIFID II guidelines now require assessments of sustainability preferences. This contrasts to the MICA Guidelines, which only reference consideration of suitability preferences as a form of good practice.
- The MICA Guidelines (in particular, Guideline 1) requires CASPs to explain to clients that, without necessary information, they are unable to provide services to clients.

In spite of the benefits of a broadly harmonised approach between MIFID II and MICA, there are some perceived disadvantages.

For instance, the basis of the suitability assessment has been to reduce consumer detriment by ensuring that CASPs providing in-scope services only recommend and manage crypto-assets that are within a client's knowledge, experience, understanding, and risk tolerance. However, crypto-assets are generally more volatile and speculative compared to traditional investments, posing different risks and requiring additional knowledge. This means that the types of questions asked during the assessment would typically be different from the questions that would be asked to determine, for instance, knowledge and risk tolerance in relation to traditional investments. Therefore, any perceived advantage of streamlining processes for firms offering both asset classes would seemingly be reduced by the bifurcation of questions, depending on the CASP's services and crypto-assets on offer.

However, on balance, our view is that ensuring consistency across the MIFID II and MICA frameworks is an appropriate starting point for crypto-asset suitability assessments. As with any novel regime, the

more that can be gleaned from the implementation of previous/related regimes, the more immediately effective the novel regime can be.

Transfer Services for Crypto-assets

MiCA requires ESMA to issue guidelines for CASPs providing transfer services for crypto-assets.

MiCA regulates the provision of transfer services for crypto-assets on behalf of clients. Persons authorised to provide such services must enter into an agreement with their clients specifying their duties and responsibilities.

Crypto-asset transfer services bear some resemblance to payment services, which are currently regulated in the EU under PSD 2.

ESMA recognises this and has therefore drawn heavily on PSD 2 provisions to develop their draft guidelines.

We summarise and comment below on ESMA's proposals.

Topic	Commentary
Prior General Information	Crypto-asset service providers (CASPs) must provide their clients with "essential information" on the conditions of the provision of the service. This must be provided in good time before the client enters into the agreement with the service provider. This is to ensure transparency for crypto-asset holders. The information to be provided includes, among other things, the method of instructing and withdrawing instructions for transfers; the conditions under which transfer instructions may be rejected; cut-off times; information on the DLT used to support the transfer; the maximum execution time; and details of fees and charges. In addition, for each DLT network, the service provider must specify the time or number of block confirmations needed for the transfer to become irreversible. This information is expected to be provided at the time that a contract for services is entered into. This is, of course, similar to existing pre-contractual disclosure requirements under PSD 2, as well as EU Distance Marketing rules.
Information on Individual Transfers for Crypto-assets	Further details must be provided to clients when an instruction for the transfer of crypto-assets is received. Prior to the execution of the instruction, the CASP must provide a "brief warning" that indicates when a transfer will become irreversible. The charges payable by the client must be disclosed. This should allow the client to cancel or amend the instruction before it is executed. Following execution, the CASP is expected to provide a confirmation with the basic details of the transfer. If the transfer is rejected, returned, or suspended, the client is to be provided with the reason, options to remedy

	the situation, and the amount of any fees and charges incurred (along with reimbursement details, where relevant).
Execution Times and Cut Off Times	CASPs are required to establish cut off times for transfer instructions, maximum execution times, and the numbers of block confirmations needed for transfers to become irreversible (or sufficiently irreversible in cases of probabilistic settlement) for each DLT network.
Rejection of an instruction	Taking into account the requirements of the restated Transfer of Funds Regulation, CASPs must also have policies and procedures for the execution, rejection, return, or suspension of crypto-asset transfers.
Liability	CASPs are required to establish policies and procedures determining the conditions for the provider to be liable to clients in case of unauthorised or incorrectly initiated or executed transfers.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings London lawyers:

Arun Srivastava
44.020.3023.5230
arunsrivastava@paulhastings.com

Nina Moffatt
44.020.3023.5248
ninamoffatt@paulhastings.com