GUIDANCE

ICE Futures Europe and ICE Endex Guidance on Member Requirements under MiFID II

June 2019

Version 1.2.1

Contents

Members are advised that this document is not intended to be a definitive guide as their obligations under MiFID II. Members should seek their own legal advice with respect to ensuring they fully comply with all applicable MiFID II requirements. Please see the Important Notice in Section 11.

1 Introduction

1.1 Purpose

ICE Futures Europe ("IFEU") and ICE Endex Markets B.V. ("ICE Endex" and together with IFEU referred to as the "Exchanges") both operate as EU Regulated Markets in accordance with the Markets in Financial Instruments Directive (2004/39/EC) ("MiFID"). IFEU is a Recognised Investment Exchange ("RIE") under the Financial Services and Markets Act 2000 ("FSMA"). ICE Endex holds a license as an EU Regulated Market under the *Wet Financieel Toezicht (*Dutch Act on Financial Supervision). As such, the Exchanges each have a regulatory obligation to provide for fair and orderly trading.

Under MiFID II legislation (Directive 2014/65/EU and Regulation 600/2014 ("MiFIR")) ("MiFID II"), and relevant secondary legislation including regulatory technical standards ("RTS"), the Exchanges are required to have in place effective systems, procedures and arrangements for compliance with a number of requirements. The Exchanges are required to set out the rules and conditions applicable to firms which:

- provide Direct Electronic Access ("DEA") to their clients;
- are engaged in algorithmic trading; and
- act as clearing members.

In addition, under the Market Abuse Regulation (Regulation 596/2014) ("MAR"), all persons executing or arranging transactions on the Exchanges, which includes Members of the Exchanges ("Members") and the Exchanges themselves, must have in place arrangements, systems and procedures to prevent, monitor for and detect Market Abuse.

This document (the "Guidance") seeks to provide guidance on the various requirements to which Members are subject under the above legislation, incorporating industry best practice recommendations in the area of systems and controls. The Guidance focuses on areas relevant to the Exchanges' own regulatory obligations and operating standards, and which the Exchanges consider relevant for the majority of their memberships.

In addition to the legal requirements, the Exchanges are also mindful of the following in publishing this Guidance:

- their diverse membership – there is significant variation in the nature, scale and scope of Members' business activities;
- the fact that Members are generally best placed to identify the needs of their business and that responsibility to comply with the applicable Exchange regulations, being the IFEU Exchange Regulations for IFEU and the ICE Endex Market Rules and appendices – Futures (the "ICE Endex Rules") for ICE Endex (together, the "Exchange Regulations") and other applicable laws ultimately rests with the Member; and
- the need for the Exchanges to respond flexibly to the circumstances of each Member.

As Members of the Exchanges agree to be bound by the Exchange Regulations, which are to be interpreted and given effect (by Members) in a manner designed to promote and maintain the Exchanges' status as a RIE and/or Regulated Market, they are obliged under IFEU Exchange Rule A.11 and article I-7 of the ICE Endex Rules to have in place adequate arrangements, systems and controls to ensure they comply with their obligations under the Exchange Regulations. This document is intended to function as guidance for Members in this area and does not override or waive any obligations in the Exchange Regulations. It is without prejudice to any of the Exchanges' rights under the relevant Exchange Regulations, including commencing disciplinary proceedings should a breach be identified.

This Guidance is provided for information purposes only. This Guidance does not form part of the contractual documentation between the Exchanges and its Members. It is neither a full description of the services of the Exchanges, the Exchange Regulations or applicable laws nor a recommendation to make use of any service

(see "Important Notice" at Section 11 below). If Members are uncertain as to the interpretation of any part of this Guidance they should refer to the Exchange Regulations and/or contact the Exchange.

Members should also familiarise themselves with other Rules and Regulations to which they may be subject, including MiFID II, MAR and other applicable domestic or international laws. For this purpose Members can find a non-exhaustive list of 'Useful Reading' documents in Section 10.

1.2 Applicability

This Guidance applies to all Members of the Exchanges and will take effect from 3 January 2018, on the implementation of MiFID II. It has been published in advance of its effective date to help Members with their preparations for MiFID II implementation. This Guidance is based on the MiFID II legislation, including technical standards, as published in the Official Journal.

Members should be aware that certain of the requirements referred to in this Guidance are already in effect. Where this is the case, Members should ensure that they are in compliance with the relevant requirements. As set out in the Exchange Regulations, Members are required to comply at all times with all applicable laws.

The Exchange Regulations will be amended in due course to incorporate the MiFID II requirements. All changes will be published to the Market by Circular.

For ease of reference, we have outlined below a compliance timeline for various items of relevant legislation and guidelines and recommendations which are referred to in this Guidance. Full references and links are set out in Section 10.

Requirements already in effect on the date of publication of this Guidance:	**Additional requirements applying from 3 January 2018:**
MAR	MiFID II
"ESMA Guidelines - Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities", published 24 February 2012 (the "ESMA Guidelines")	Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading ("RTS 6")[1]
Committee of European Banking Supervisors ("CEBS"), Guidelines on the management of operational risks in market-related activities, published October 2010	Commission Delegated Regulation (EU) 2017/574 of 7 June 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards for the level of accuracy of business clocks ("RTS 25")[2]
The Exchange Regulations	Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (the "Organisational Requirements Delegated Regulation")[3]
	Amendments to Exchange Regulations incorporating MiFID II requirements, as notified by Circular

[1] RTS 6: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0589&from=EN

[2] RTS 25: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0574&from=EN

[3] Organisational requirements: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0565&from=EN

In addition, Members should be mindful of and take into account the recommendations set out in the following documents, which apply at the date of publication of this Guidance:

- FIA, Market Access Risk Management Recommendations, published April 2010.
- FIA – Principal Traders Group, Recommendations for Risk Controls for Trading Firms, published November 2010.
- IOSCO, Principles for Direct Electronic Access to Markets, published August 2010.

Note that several other laws are likely to be relevant to activities on the Exchanges but these are outside the scope of this Guidance (see Section 11).

1.3 Member Review Programme

For Members of IFEU:

IFEU operates an annual risk based Member review programme to review and assess the arrangements, systems and controls a Member has in place to ensure compliance with the IFEU Exchange Regulations. When performing its assessment, IFEU will consider how a Member complies with the IFEU Exchange Regulations with reference to:

- the areas outlined in this document;
- the ESMA Guidelines;
- MAR; and
- the criteria under Section B of the IFEU Exchange Regulations.

For Members of ICE Endex:

ICE Endex performs due diligence on prospective members and a Periodic Member Review on a selection of Members to analyse if a (prospective) Member complies with the requirements listed in bullets 1-3 above and meets all the membership criteria as reflected in article I-4 of the ICE Endex Rules.

In addition, from 3 January 2018, both Exchanges will assess against the specific MiFID II criteria as set out in Section 2.1; which shall include the additional MiFID II Membership Criteria.

1.4 Member responsibility

Members are reminded that under the Exchange Regulations they retain full responsibility for both their activity, as well as the trading activity conducted by their clients on the Exchange. For clarity, outsourcing agreement and/or client agreement provisions do not alter this responsibility.

2 Exchange Membership requirements

2.1 Due diligence for Members

Firms seeking to be a Member of the Exchange(s) must apply directly to the relevant Exchange and undergo a formal due diligence process, including but not limited to: KYC/AML checks and a compliance review and an on-site visit from the Exchange. Prospective Members of an Exchange are required to meet the membership criteria as set out in the applicable Exchange Regulations at the time of applying and on an on-going basis. In accordance with MiFID II, from 3 January 2018 each Exchange will require that prospective Members meet pre-defined standards in relation to:

- pre-trade controls on price, volume, value and usage of the system and post-trade controls on their trading activities;
- qualification of staff in key positions within Members' organisations;
- technical and functional conformance testing (see Section 5.4);
- policy of use of the kill functionality (see Section 5.2); and

- whether the Member may provide DEA[4] to its own clients and if so, the conditions applicable to those clients.

2.2 Authorisation requirements for Members

2.2.1 Authorisation

Under the Exchange Regulations, Members are required to have in place all necessary authorisations to conduct their business and hold all licences, permits, consents, contracts and other approvals (if any) that are required to carry out business on the relevant Exchange, or be able to rely on an available exemption. This also includes ensuring the Members' clients have the relevant authorisation and permission to conduct business on the Exchange or are able to rely on an available exemption.

2.2.2 Firms that may provide Direct Electronic Access

Under MiFID II and with reference to the UK Government's draft amendments to the Recognition Requirements Regulations to transpose MiFID II into UK Law[5] and the Dutch Authority for the Financial Markets (AFM)'s Guidance on the MiFID II requirements[6], ICE Futures Europe and ICE Endex may permit Members to provide DEA ("DEA Providers") only if the Member is:

(i) an investment firm authorised in accordance with MiFID II ("MiFID Investment Firm");

(ii) a credit institution authorised under Directive 2013/36/EU ("Credit Institution");

(iii) exempt from MiFID under Articles 2.1(a), (e), (i), or (j) of MiFID II and for IFEU is authorised in the UK to provide investment services and activities. Authorisation is not required in the Netherlands in this instance;

(iv) a third country firm providing DEA subject to an equivalent regime under Articles 46(1) and 47(3) of MiFIR[7];

(v) a third country firm providing DEA in accordance with the relevant UK or Dutch national regime for the purposes of Article 54.1 (transitional provisions) of MiFIR[8] - i.e. in the UK, providing services subject to the Overseas Persons Exclusion or in the Netherlands, in accordance with the Dutch Financial Supervision Act, is a firm from Switzerland, Australia or the USA; or

(vi) a third country firm which does not come within paragraph (iv) or (v) and is otherwise permitted to provide DEA under UK or Dutch Law.

If any Member is currently providing DEA to clients and does not meet any of the above criteria, they should seek their own legal advice on the matter. For further information, please contact the relevant Exchange.

DEA Providers should also consider the authorisation status of their clients. Prior to the implementation of MiFID II, an exemption is available from the scope of MiFID for firms that deal on own account and do not provide any other investment services and activities. This means that they may not have been investment firms for the purposes of MiFID. However, under MiFID II, these exemptions will not be available where a:

- firm dealing on own account in instruments other than commodity derivatives, emission allowances, or derivatives on emission allowances, accesses a trading venue through DEA or is a market maker, unless the firm is a non-financial entity executing transactions for hedging purposes;
- firm deals on own account, including market makers, in commodity derivatives or emission allowances or derivative products, unless the activity is ancillary to their main business;

[4] See Glossary of Terms.

[5] HM Treasury - Transposition of the Markets in Financial Instruments Directive II: Response to the Consultation- https://www.gov.uk/government/consultations/transposition-of-the-markets-in-financial-instruments-directive-ii

[6] The Dutch Authority for the Financial Markets (AFM) MiFID II Important changes: https://www.afm.nl/en/professionals/nieuws/2017/jan/mifid-vergunningaanvraagformulieren

[7] Markets in Financial Instruments Regulation: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600&from=EN

[8] Markets in Financial Instruments Regulation: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600&from=EN

- firm applies a high frequency algorithmic trading technique ("HFT")[9].

Such firms may be able to rely on the third-country provisions in MiFIR[10] or the UK Overseas Person Exclusion regime or any similar national exemptions or regulatory perimeter exclusions under the laws of other EEA countries. Guidance on MiFID II requirements has been issued by the AFM in the Netherlands[11] and in the UK, MiFID II Transposition Draft legislation has been published by the UK Government, which covers DEA[12]. Legal advice should then be sought by Members and their clients. For further information, please contact the relevant Exchange.

2.3 Additional Membership Criteria for DEA Providers

DEA Providers must meet certain criteria and have in place effective systems and controls before they can provide their clients with access to the trading venue, which ensure:

- that the suitability of the client(s) using this service have been reviewed and assessed;
- clients using the service are prevented from exceeding appropriate credit and risk limits;
- trading by DEA clients is properly monitored; and
- risk controls prevent trading by DEA clients which:
    - may create risks to the Member itself;
    - may create, or contribute to, a disorderly market;
    - may breach the Market Abuse Regulation (MAR) or the Exchange Regulations.

These criteria include:

- DEA Providers must always retain responsibility for the trading their DEA clients carry out in their name and for the effectiveness of the controls;
- DEA Providers must establish policies and procedures to ensure that the trading of DEA clients complies with the relevant Exchange's Rules and Regulations and allows the DEA Providers to meet the requirements applicable to DEA.
- DEA Providers must apply pre- and post-trade controls on the order flow of each of their DEA clients (see Sections 5.2 and 5.2), as well as have in place real-time monitoring and market surveillance controls.
- DEA Providers may use their own pre- and post-trade controls, controls offered by a third party, or the controls offered by the Exchanges, and they must have sole entitlement to set or modify the parameters of such limits that apply to the controls. The controls to be applied by DEA Providers must be separate and distinct from those of DEA clients. In particular, and regardless of the application by the DEA client of its own pre- and post-trade controls, real-time monitoring and market surveillance controls, the orders of DEA clients must always pass through the pre-trade controls that are set and controlled by the DEA Provider.
- Pre-trade controls on order submission must be based on the credit and risk limits which the DEA Provider applies to the trading activity of its clients, based on the initial due diligence and periodic review of the client (see Section 4.1).
- The DEA Provider must monitor the effectiveness of its pre- and post-trade controls on an on-going basis.

[9] See Glossary of Terms.

[10] MiFIR, Articles 46 and 47.

[11] The Dutch Authority for the Financial Markets (AFM) MiFID II Important changes: https://www.afm.nl/en/professionals/nieuws/2017/jan/mifid-vergunningaanvraagformulieren

[12] HM Treasury - Transposition of the Markets in Financial Instruments Directive II: Response to the Consultation- https://www.gov.uk/government/consultations/transposition-of-the-markets-in-financial-instruments-directive-ii

- The controls applied to DEA clients using sponsored access must be as stringent as those imposed on DEA clients using DMA.

The Exchanges recommend that such systems used by the DEA Provider have the ability to:

- monitor any orders submitted by DEA clients using the trading code of the DEA Provider;
- automatically block or cancel orders from:
    - individuals which operate trading systems that submit orders related to algorithmic trading and which lack authorisation to send orders through DEA;
    - a DEA client in financial instruments that a DEA client does not have permission to trade;
    - a DEA client when they breach the DEA Provider's risk management thresholds.;
- stop order flow transmitted by their DEA clients;
- suspend or withdraw DEA services to any clients where the DEA Provider is not satisfied that continued access would be consistent with their rules and procedures for fair and orderly trading and market integrity; and
- carry out, whenever necessary, a review of the internal risk control systems of a DEA client.

DEA Providers must have in place procedures to evaluate, manage and mitigate market disruption and firm-wide risk, and must be able to identify the persons to be notified in the event of an error resulting in violations of the risk profile, or potential breaches of the Exchange Regulations.

DEA Providers must at all times have the ability to identify its different DEA clients and the trading desks and traders of those DEA clients, who submit orders through the DEA Provider's systems by assigning unique identification codes to them.

Where a DEA Provider allows a client to sub-delegate the DEA access it receives to its own clients, the DEA Provider must be able to identify the different order flows from the sub-delegated entities. For these purposes, it will not be necessary for the DEA Provider to know the identity of these sub-delegated entities.

DEA Providers must record the relevant data relating to the orders submitted by their DEA clients, including modifications and cancellations, the alerts generated by their monitoring systems and the modifications made to their filtering process.

DEA Providers on ICE Futures Europe under Section 2.2.2 (iii) and (v) above may be required on a regular or ad hoc basis to provide to the FCA:

- a description of the systems used under Section 2.3 above
- evidence that those systems have been applied; and
- the information stored relating to:
    - the due diligence performed on DEA clients in accordance with Section 4.2; and
    - the arrangements, systems and controls the DEA Provider has in place with respect to its DEA clients.

2.3.1 Sponsored Access[13]

The provision of sponsored access will be subject to the authorisation of the relevant Exchange. Members must apply the same pre-trade and post-trade risk limits and controls that they are required to have in place as Members to clients accessing the trading platform through sponsored access. Please note that Members providing clients with access to the Exchange through WebICE must make their own assessment as to whether they are providing sponsored access.

2.4 Market makers

[13] See Glossary of Terms.

MiFID II contains a number of new requirements for market makers. The Exchanges have a separate programme for updating Members regarding these requirements. Please consult relevant Circulars on market maker programmes for current requirements. More information will follow in due course.

3 General organisational requirements

3.1 Governance

Members are required to ensure that, as part of their overall governance and decision-making framework, they establish and monitor their trading activity, systems and trading algorithms through a clear and formalised governance arrangement, having regard to the nature, scale and complexity of their business.

The Exchanges recommend that this governance arrangement:

- establishes, implements and maintains decision-making procedures and an organisational structure which clearly, and in a documented manner, specifies clear accountability and reporting lines, and allocates functions and responsibilities, including procedures, where applicable, to approve the development, deployment and subsequent updates of any trading algorithms and to solve problems identified when monitoring trading algorithms;
- establishes, implements and maintains adequate internal control mechanisms designed to secure compliance with decisions and procedures, Exchange Regulations and applicable laws at all levels of the Member firm;
- ensures that personnel with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them are employed;
- sets out effective procedures for the communication of information at all levels within the Member, such that all relevant persons are aware of the procedures which must be followed for the proper discharge of their responsibilities, and that instructions can be sought and implemented in an efficient and timely manner;
- ensures that adequate and orderly records of the Member's business and internal organisation are maintained;
- ensures that the performance of multiple functions by their staff does not and is not likely to prevent those persons from discharging any particular function soundly, honestly and professionally; and
- sets out a separation of tasks and responsibilities of trading and brokerage desks on the one hand and supporting functions, including risk control and compliance functions, on the other, to ensure that unauthorised trading activity cannot be concealed.

3.2 Senior management

Management staff must be sufficiently knowledgeable and experienced or otherwise qualified to properly supervise the business and the risks to which the firm may be exposed, in order to ensure continued compliance with the firm's obligations.

3.3 Supervisory structure and escalation process

Members are required to organise and control themselves appropriately according to the nature, size and scope of their business activities, which may include having:

- an effective supervisory structure, which should aim to control and monitor business conducted by the Member and its representatives on the relevant Exchange platform;
- arrangements whereby senior management and, where applicable, the supervisory function, assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to

comply with the relevant Exchange Regulations and applicable laws and take appropriate measures to address any deficiencies (see Section 3.1);
- reporting to senior management by the supervisory function on all compliance, risk and audit matters, which must include reporting on whether the appropriate remedial measures have been taken in the event of any deficiencies; and
- a formal escalation process, ensuring that issues are raised to the appropriate person / team and resolved in a timely manner, and where necessary reported to the relevant authorities, which may include the Exchange(s).

Members engaged in algorithmic trading[14] must ensure strong governance exists when developing, testing, deploying and managing algorithms and systems. Management sign-off must be required for initial deployment or substantial updates. When making changes to existing algorithms and/or systems, and when introducing new algorithms and/or systems, representatives from trading, risk, compliance and software management must be involved, and all policies and procedures for these processes must be clearly documented.

Members must also establish procedures to ensure that any such changes to the functionality of their systems are communicated to traders in charge of the trading algorithm and to the compliance function and the risk management function.

3.4 Segregation of duties

To prevent the sharing of sensitive or confidential information that may harm the interests of clients, and to prevent inappropriate influence being exercised over other individuals, the Exchanges recommend that teams are organised in a way to achieve, where appropriate and/or required, a separation of duties. In particular, the Exchanges recommend that arrangements are put in place to separate front, middle and back office functions, including between risk control and compliance functions. Particular consideration should be given to individuals with overlapping functions within the firm.

The specific duties and responsibilities of staff and teams should be defined, documented, regularly monitored and reviewed periodically to identify any possible conflicts of interest.

3.5 Staff and resourcing

Members must have the appropriate number of staff with the necessary skills, knowledge and experience for the tasks assigned to them, including having knowledge of the relevant Exchange Regulations.

In particular, in order to ensure that a Member's systems and trading are effectively monitored and controlled appropriately and in a timely manner, and challenged where applicable, staff must have sufficient technical knowledge of:

- relevant trading systems and algorithms;
- the monitoring and testing of such systems, strategies and algorithms;
- where applicable, the trading strategies that the Member deploys through its algorithmic trading strategies and trading algorithms; and
- the legal obligations of the Member.

The Exchanges encourage Members to define the skills necessary for staff, and provide initial and on-going tailored training to ensure relevant staff have the appropriate knowledge. All staff involved in order submission, which may include back office and trading staff, must receive training on order submission systems and market abuse.

All staff responsible for the risk and compliance functions of algorithmic trading must have:

- sufficient knowledge of algorithmic trading and strategies;
- sufficient skills to follow up on information provided by automatic alerts; and

[14] See Glossary of Terms

- sufficient authority to challenge staff responsible for algorithmic trading where such trading gives rise to disorderly trading conditions or suspicions of market abuse.

The Exchanges expect Members to have sufficient staff available during trading hours to ensure that transactions are booked and recorded in a timely manner as well as dealing with any trading and/or compliance queries.

The Exchanges encourage information provided via Exchange Circulars to be drawn to the attention of staff, including, for example, details about opening hours and changes to the Exchange Regulations.

3.6 Documentation

All policies and procedures across the main functions of the firm including, but not limited to, risk, compliance, operations and IT should be documented, reviewed and updated regularly to ensure that domestic and international rules and regulations, and the Exchange Regulations are taken into account.

3.7 Outsourcing agreements

Members are reminded that they retain full responsibility for fulfilling their obligations when outsourcing any systems, functions or processes. Members should comply with the requirements as set out in this Guidance document; the requirements relating to outsourcing for investment firms in MiFID II[15] or other such similar legislation, as applicable.

Members outsourcing the compliance function should provide information and access to the external compliance consultant as it would with its own compliance staff. Members must also ensure data privacy is guaranteed; and should regularly assess the compliance function by internal and/or external auditors, ensuring that such assessments, including any undertaken by the firm's competent authority, are not constrained.

With regard to any procured or outsourced software or hardware, Members should ensure they have sufficient knowledge of how the systems operate and have in place documented procedures on how to utilise the systems, including those used in algorithmic trading.

Members must have in place robust procedures, including an escalation process, that ensure the timely resolution of system issues related to and / or resulting from having outsourced daily Exchange related procedures to third party service providers.

3.8 Business Continuity Plans ("BCPs")

The Exchanges recommend that Members have a BCP in place which is appropriate for the nature, size and scope of their business. A BCP must include details of how to continue operations under adverse conditions, and in the event of a failure of a Member's systems.

Members engaged in algorithmic trading must have a suitable BCP in place for its algorithmic trading systems. The BCP must deal effectively with disruptive incidents and, where appropriate, ensure a timely resumption of algorithmic trading. The BCP must cover at least the following:

- governance for the development and deployment of the BCP;
- a range of possible adverse scenarios relating to the operation of the algorithmic system;
- trading system relocation and operating procedures;
- staff training;
- arrangements for each trading venue;
- kill functionality policies (see Section 5.2);
- alternative arrangements for managing outstanding orders and positions; and
- the shutting down of algorithms and systems without creating disorderly trading conditions.

[15] MiFID II, Articles 16(2) and 16(5); Organisational Requirements Delegated Regulation, Articles 30-32.

BCPs must be documented and reviewed and tested on an annual basis and amended as appropriate.

4 Client due diligence

4.1 General requirements

Whenever a Member is providing services on behalf of a client on the Exchange(s), they will need to ensure that they have complied with all applicable client due diligence requirements, including those under the UK Money Laundering Regulations 2007, *Wet ter voorkoming van Witwassen en Financieren van Terrorisme*, and the Exchange Regulations.

In addition, DEA Providers and Clearing Members are subject to the following specific requirements set out in Sections 4.2 and 4.3.

4.2 DEA Providers

Additional and specific due diligence requirements apply to DEA Providers under MiFID II. DEA Providers, whether they provide Direct Market Access ("DMA") or Sponsored Access, are responsible for ensuring that their DEA clients comply with Exchange Regulations. To fulfil this obligation, DEA Providers must perform due diligence on prospective clients to ensure they meet the requirements set by the Exchange(s) or under any other applicable law, including MiFID II.

The due diligence must ensure that the DEA Provider discharges its obligations under the Exchange Rules, and must cover relevant matters including:

- the governance and ownership structure;
- the types of strategies to be undertaken by the prospective DEA client;
- the operational set-up, the systems and the pre- and post-trade controls and the real-time monitoring of the prospective DEA client. Where the DEA Provider allows clients to use third-party trading software for accessing trading venues, it must ensure that the software includes pre-trade controls that are equivalent to the pre-trade controls set out in this Guidance;
- the responsibilities within the prospective DEA client for dealing with actions and errors;
- the historical trading pattern and behaviour of the prospective DEA client;
- the level of expected trading and order volume of the prospective DEA client;
- the ability of the prospective DEA client to meet its financial obligations to the DEA Provider;
- the disciplinary history of the prospective DEA client, where available; and
- verifying that the client is/was not the target of any Sanction.

Where a DEA Provider allows a client to sub-delegate the access it receives to its own clients, the DEA Provider must ensure that, before granting that client access, it has a due diligence framework in place that is at least equivalent to the one described above.

DEA Providers are required to perform due diligence before giving clients access to the Exchanges and must perform a risk-based reassessment of the adequacy of their clients' systems and controls on an annual basis.

DEA Providers must have in place a binding written agreement between themselves and their clients which:

- details the rights and obligations of both parties arising from the provision of their services; and
- states that the DEA Provider is responsible for ensuring the client complies with the requirements of MiFID II and Exchange Rules.

4.3 Clearing Members[16]

Clearing Members must have effective and robust systems and controls in place to ensure that their clearing services are only available to persons who are suitable and have successfully met, and continue to meet the

[16] A Member that has been authorised as a clearing member by ICE Clear Europe, or as a General Clearing Participant or Direct Clearing Participant by ICE Clear Netherlands.

relevant criteria. For more information on these criteria please refer to either ICE Clear Europe's Membership Requirements[17] or ICE Clear Netherlands' Participation Requirements.[18] In situations where the Clearing Member also provides their clients with DEA services, the Clearing Member must ensure that they comply with both sets of responsibilities, i.e. as a Clearing Member and as a Member of the Exchange(s) which is a DEA Provider. DEA providers which also offer indirect clearing services for the purposes of MiFID and Regulation (EU_No 648/2012 (EMIR)), must ensure that they also comply with the requirements applying to such arrangements under MiFIR Article 30, EMIR Article 4 and the relevant level 2 measures. More information on Indirect Clearing will be provided by the Clearing Houses in due course.

In order to mitigate and manage their own counterparty, liquidity, operational and any other risks, Clearing Members must set and communicate appropriate trading and position limits in commodity derivatives to their clients (see Section 5.2).

5 Risk management

5.1 General

The Exchanges expect Members to have in place effective systems and risk controls suitable to their business and size. As a minimum, a Member's risk framework must include appropriate and proportionate pre- and post-trade controls on its own trading, systems and algorithms; to its clients' trading, and where applicable comply with the requirements relating to risk management for investment firms in MiFID II[19] or in other similar legislation. Members engaged in algorithmic trading, providing DEA services or providing clearing services are required to have additional risk controls to mitigate the level of risk associated with their business model, as stated in Section 3.3.

5.2 Risk limits, Monitoring and Alerts

Members are expected to have in place effective and resilient systems with proportionate risk controls in order to ensure that their trading system does not contravene market abuse laws, create or contribute to disorderly trading conditions or breach the Exchange Regulations.

In order to achieve this, Members must have a number of pre- and post-trade controls in place.

5.2.1 Pre-trade Controls

Members must have in place the following pre-trade controls on order entry:

- price collars which automatically block or cancel orders that do not meet set price parameters, differentiating between different financial instruments, both on an order-by-order basis and over a specified period of time;
- maximum order volume, which prevents orders with an uncommonly large order size from entering the order book; and
- maximum messages limit which prevents sending an excessive number of messages to order books pertaining to the submission, modification or cancellation of an order.

Members must all have in place repeated automated execution throttles which control the number of times an algorithmic trading strategy has been applied. After a pre-determined number of repeated executions, the trading system must be automatically disabled until re-enabled by a designated staff member.

Members must set controls appropriately in accordance with their risk tolerances, strategy, scale and type of business. The systems that Members have in place should allow them to readjust the parameters as necessary and they must be able to block or cancel orders that may put them at risk of breaching their own thresholds. Members must automatically block or cancel orders from a trader if they become aware that the trader does not have permission to trade a particular financial instrument. Controls must be applied where appropriate, at

[17] ICE Clear Europe Clearing Membership Rules - Part 2: www.theice.com/clear-europe/regulation#rulebook

[18] ICE Clear Netherlands Participation Requirements - Clauses 4 and 5 www.theice.com/publicdocs/ICE_Clear_Netherlands_Rulebook.pdf

[19] MiFID II, Article 16(5); Organisational Requirements Delegated Regulation, Article 23.

client level; by product; by trader; by trading desk or at the Member level. Pre-trade controls may only be over-ridden with the full knowledge of risk management staff; and all such decisions must be properly documented. Such over-ride procedures and arrangements must be applied in relation to a specific trade on a temporary basis and in exceptional circumstances. They must be subject to verification by the risk management function and authorisation by a designated individual of the Member.

5.2.2 Post-trade controls

Post-trade controls must include as a minimum the continuous assessment and monitoring of market and credit risk of the Member and controls regarding the maximum long and short and overall strategy positions. If a post-trade control is triggered, the Member must take appropriate action.

Members must reconcile their own trading logs with the data provided by the Exchange, by their clearing members; central counterparties; DEA Providers; third party data vendors and/or other relevant business partners. Member must be able to calculate their outstanding exposure, and that of its traders and clients in real-time.

For Members operating an algorithmic trading system, post-trade monitoring must be undertaken by the traders responsible for the algorithm and the risk control functions within the firm.

5.2.3 Position Limits set by Clearing Members

Clearing Members must set and communicate appropriate trading and position limits in commodity derivatives to their clients in order to mitigate and manage their own counterparty, liquidity, operational and any other risks.

Clearing Members must monitor their clients' positions against these limits as close to real-time basis as possible and have appropriate pre-trade and post-trade procedures for managing the risk of breaches, by way of appropriate margining practice and other means.

Clearing Members must document such procedures in writing and maintain records of their compliance.

5.2.4 Monitoring systems

Members are encouraged to use automated surveillance where proportionate, or have in place a system that alerts them to breaches, either automatically or through system monitoring appropriate to the size, nature and scope of their business. Members should pay particular attention to how alerts outside of normal office hours are dealt with.

Members should have in place procedures for ensuring issues are escalated and appropriate action taken in a timely manner. Appropriate action may involve the automatic or manual closing out or reducing of positions if limits are breached.

Functionality is available to Members through the relevant Exchange's risk management tools, such as ACE and the various APIs, and for Clearing Members in the ICE Clearing Administration tool where they can set and/or change risk limits.

Members must have the capability to monitor real-time orders during their trading hours. This includes any trading activity undertaken by their clients. Members that engage in HFT must also monitor heartbeats between their systems and the Exchange to make sure connectivity has not been lost. This monitoring should be undertaken by an independent function within the firm.

5.2.5 Kill functionality

Members must be able to cancel immediately, as an emergency measure, any or all of its unexecuted orders submitted to any or all trading venues to which the Member is connected (the "kill functionality"). For these purposes, unexecuted orders include those originating from individual traders, trading desks or, where applicable, clients. Members must be able to identify which trading algorithm and which trader, trading desk, or, where applicable, which client is responsible for each order that has been sent to a trading venue. Compliance staff at a Member must have, at all times, direct access, or contact with the person or persons within the Member who has access to the kill functionality.

5.3 Members engaged in algorithmic trading

Members engaged in algorithmic trading and/or operating automated trading systems ("ATSs") that are active on the Exchange platform are expected to comply with the relevant MiFID II requirements, the Exchange Regulations, the FIA's *Recommendations for Risk Controls for Trading Firms,* and other applicable rules and regulations.

5.4 Testing of trading systems, strategies and algorithms

5.4.1 Conformance Testing

All Members must undertake conformance testing with the Exchanges to ensure that:

- the basic functioning of the Member's trading system, algorithm and strategy complies with the Exchange's conditions;
- the system or algorithm interacts with the Exchange's matching logic as expected;
- basic functionalities, such as submission, modification or cancellation of an order and all business data flows are functioning; and
- the connectivity, including the cancel on disconnect command, market data feed loss and throttles, and the recovery all function.

Members will be required to undertake conformance when accessing the Exchange as a Member and prior to the deployment or a substantial update of:

- the access to the Exchange's system;
- the Member's trading system, trading algorithm or trading strategy.

DEA providers should note that any DEA clients which operate an algorithmic trading system or trading algorithm will be required to test its conformance in any of the following cases:

- when connecting to the Exchange through a sponsored access arrangement for the first time;
- when the relevant Exchange makes material changes to its systems; and
- prior to initial deployment or material update of the algorithmic trading system, trading algorithm or algorithmic trading strategy.

The Exchange will provide a conformance testing environment which all Members and prospective Members can access.

5.4.2 Testing of algorithms

Prior to the deployment or substantial update of an algorithmic trading system, trading algorithm or algorithmic trading strategy, Members are responsible for ensuring that sufficient testing is undertaken in a non-live, segregated test environment to ensure that any signs of disorderly trading or Exchange Regulation violations are identified and rectified.

As part of such testing, Members must also ensure that their trading system, trading strategy or algorithm works adequately under stressed conditions. Members must ensure that the testing methodologies used address the design, performance, recordkeeping and approval of the algorithmic trading system, trading algorithm or algorithmic trading strategy, in addition to setting out the allocation of responsibilities and sufficient resources, and the procedures to seek instructions within the Member. The methodologies must ensure that the trading system, trading algorithm or trading strategy:

- does not behave in an unintended manner;
- complies with the Member's obligations under MiFID II, as applicable;
- complies with the relevant Exchange Regulations;
- does not contribute to disorderly trading conditions;
- continues to work effectively in stressed market conditions; and

- where necessary under those conditions, allows for the switching off of the algorithmic trading system or trading algorithm.

Before deployment of a trading algorithm, Members must set pre-defined limits on:

- the number of financial instruments being traded;
- the price, value and number of orders;
- the strategy positions; and
- the number of trading venues to which orders are sent.

Members must test that their algorithmic trading systems and relevant procedures and controls can withstand increased order flows or market stresses, on a regular basis, in accordance with applicable laws. Members must design such tests having regard to the nature of their trading activities and trading systems. Members must ensure that the tests are carried out in such a way that they do not affect the production environment. The tests should comprise:

- running high messaging volume tests using the highest number of messages received and sent by the Member during the previous six months, multiplied by two; and
- running high trade volume tests, using the highest volume of trading reached by the Member during the previous six months, multiplied by two.

Members retain full responsibility for testing irrespective of any outsourcing arrangement, and will be required to certify that the algorithms they deploy have been tested and to explain the means used for that testing. For clarity, this self-certification obligation lies with the Exchange Member.

5.5 Electronic and Physical Security

Members must consider the electronic and physical security of their trading and business networks and must maintain appropriate arrangements that minimise the risks of attacks against its information systems. Such arrangements must ensure the confidentiality, integrity, authenticity, and availability of data and the reliability and robustness of the Member's information systems. Members are strongly encouraged to use passwords, network firewalls, VPN connections or other security devices to prevent unauthorised access and minimise the risks of cyber-attacks against their systems and Exchange systems. Third-party electronic security audits, performed at regular intervals, are encouraged.

It is recommended that Members implement an IT strategy with defined objectives and measures which:

- complies with the business and risk strategy of the Member and is adapted to its operational activities and the risks to which it is exposed;
- is based on a reliable IT organisation, including service, production and development; and
- complies with effective IT security management.

Members should check that staff have appropriate access to systems, including permissions to view and modify positions, and conversely do not have access inappropriate to their role. This should incorporate activity undertaken out of the office, or out of office hours. Where out of office/hours trading is permitted, Members are encouraged to have in place an approval process to consent to such activity. The sharing of passwords and the use of a login other than one's own is prohibited and usage must be monitored.

Use of systems to log user and system activity is strongly encouraged. Members must be able to identify all persons who have access to IT systems, and monitor their access. Members must have clear and effective monitoring and escalation procedures to detect and deter unauthorised activity and ensure it takes appropriate action if security breaches are identified. Members are encouraged to undertake annual penetration tests and vulnerability scans to protect against cyber-attacks.

5.6 Business clocks

Members must ensure that they comply with the requirements under MiFID II relating to the synchronisation of business clocks.[20] In particular, Members must synchronise the business clocks they use to record the date and time of any reportable event with the Coordinated Universal Time ("UTC") issued and maintained by the timing centres listed in the latest Bureau International des Poids et Mesures Annual Report on Time Activities. They must also ensure that they adhere to the requisite level of accuracy and comply with the maximum divergence requirements in MiFID II.

6 The Compliance function

6.1 General

The Exchanges recognise that Members have a variety of systems in place to deal with compliance risk. Accordingly, the Exchanges do not aim to be overly prescriptive as to how Members deal with compliance issues but note the requirements relating to the Compliance function within Investment Firms under MiFID II[21]. The Exchanges recommend that all Members have appropriate systems and controls in place to ensure that the Member and its clients are adhering to the Exchange Regulations, this Guidance and other applicable rules and regulations.

The Exchanges expect all Members, including those solely doing proprietary business, to have in place measures against potentially abusive trading behaviour.

6.2 Compliance in algorithmic firms

The Exchanges expect Compliance staff to have an understanding of the way in which the algorithmic trading systems and algorithms of the Member operate. The compliance function should be in continuous contact with persons who have detailed knowledge of the Member's algorithmic trading systems.

Compliance staff should have access to the kill functionality, or direct contact with persons who have access to it, and to those responsible for each trading system or algorithm.

Members must ensure that compliance controls are embedded during the initial deployment and any subsequent updates of algorithmic trading systems or strategies, trading algorithms, or ATSs operating on the Exchange(s), for example, by having compliance sign-off on any new algorithmic trading systems or strategies, trading algorithms, or ATSs.

6.3 Compliance manual

Members' compliance manuals should, where appropriate, make specific reference to Exchanges' Regulations and obligations and how the Members comply. Further, the Exchanges recommend that Members take steps to ensure that staff adhere to the Member's compliance manual. This may include requiring staff to: agree to be bound by the Member's compliance manual, undergo training, acknowledge that they have read and understood the relevant Exchange Regulations etc. The Exchanges may request to review a Member's compliance manual in accordance with its powers under the Exchange Rules. As a result, Members should be prepared to disclose compliance manuals upon demand, if requested.

6.4 Compliance monitoring

Members must monitor all trading activity that takes place through their trading systems, including orders and trading activity of their clients, to detect signs of potential market abuse as specified in MAR, its supplementing Regulations and technical standards. MAR prohibitions include insider dealing, unlawful disclosure of inside information and market manipulation and sets out a non-exhaustive list of indicators and practices which may highlight such potential market abuse.[22]

---

[20] MiFID II, Article 50.

[21] MiFID II, Articles 16(2) and 17(1); RTS 6, Article 2; and Organisational Requirements Delegated Regulation, Article 22.

[22] Commission Delegated Regulation (EU) 2016/522 - Indicators of Market Manipulation

Depending on the nature, scale and complexity of the Member's business, the monitoring tools utilised by the Member should be able to produce alerts, reports and include visualisation tools to detect potentially suspicious activity. Systems must be adaptable to changes and reviewed on an annual basis, including the parameters and filters, to ensure they remain appropriate to the business.

The Exchanges emphasise the importance of clear investigation procedures, using all information available to Members, such as other relevant trading undertaken by those clients if applicable. Further, clear escalation procedures are important, ensuring that suspicious trading is reported to the relevant Exchange and/or other appropriate regulatory bodies.

Members conducting algorithmic trading should recognise the complexity of their business and have an automated surveillance system which monitors orders and transactions and generates alerts and reports. The system should be able to read, replay and analyse order and transaction data on an ex-post basis and be able to generate alerts at the beginning of the following trading day or, where manual processes are involved, at the end of the following trading day. The system must also have adequate documentation and procedures in place for the effective follow-up to alerts generated by it.

In addition to monitoring for suspicious activity, Members should also undertake compliance monitoring, which may involve a level of human analysis, for adherence to the Exchange Regulations, such as (but not limited to):

- monitoring of error trades;
- adherence to Exchange Regulations on Block trades, Exchange for Physical and Exchange for Swap transactions, including ensuring all relevant documentation is available to the Exchange upon request and minimum thresholds are met;
- adherence to Exchange Regulations on Basis trades, Cross trading, and Asset Allocations;
- monitoring of default accounts: Members should make best endeavours to register trades promptly on the day the trade was executed; and
- accessing and managing their own or their clients ability and decision to make / receive delivery of physically deliverable contracts, including appropriate client due diligence and monitoring during the days immediately prior to expiry of relevant Contracts.

The monitoring employed should be proportionate to the scale, size and nature of the Member's business.

6.5 Recordkeeping requirements

Members must ensure that they comply with Exchange and all applicable regulatory recordkeeping requirements, including, where applicable, the requirements relating to recordkeeping for investment firms in MiFID II[23]. This includes:

- recording all communication channels and storing all communications relating to client business, ensuring that all telephone lines used for the receipt or giving of orders are tape recorded and the recordings kept for a minimum of five years, unless otherwise specified by the relevant regulator;
- having in place and storing client agreements;
- having a complete audit trail of orders placed and transactions completed on the relevant Exchange for a period of not less than five years;
- all information required to be retained relating to Basis trades, Asset Allocations, Block Trades, EFP, EFS and Soft Commodity EFRP transactions for a period of not less than five years; and
- in the case of HFT firms, storage of accurate and time-sequenced records on orders (including cancellations), executions and quotations on the Exchange(s) for at least the necessary minimum period depending on the nature of the business.

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0522&from=EN

[23] MiFID II, Articles 16(6) and (7); Organisational Requirements Delegated Regulation, Articles 72 to 76.

Members should note that certain regulators or applicable laws may require a longer record retention period, which must be complied with.

The Exchanges also recommend that Members ensure that trade and account information is accurate by reconciling their own electronic trading logs with records provided by the Exchanges and others.

Members must keep records to demonstrate, in the event of a review or on request, adherence with the Exchange Regulations.

In addition, a firm operating an algorithmic system must keep records of any material changes made to the software used for algorithmic trading, to accurately determine:

- when a change was made;
- who made the change;
- who approved the change; and
- the nature of the change.

6.6 Order Receipt and Execution

Member must ensure that order slips or electronic order records contain the information specified under the Exchange Regulations. Further to the compliance monitoring requirements set out in Section 6.4, the Exchanges encourage regular sampling of order slips or electronic order records and other relevant records to ensure that all information is included and other relevant Exchange Regulations are being adhered to. In addition to testing, the Exchanges strongly recommend that Members have in place procedures and policies governing client order receipt and execution. Members should ensure that they comply with all relevant regulatory requirements relating to order receipt and execution, including, where applicable, the requirements relating to client order handling for investment firms in MiFID II[24] or other relevant legislation.

6.7 Client Agreements

Members must have client agreements in place. The Exchanges deem it prudent for such agreements to oblige clients to comply with the Exchange Regulations and to co-operate with the Exchanges, for instance, when in receipt of an Exchange enquiry. Members are reminded, however, that this does not absolve the Member of its obligations under the relevant Exchange Regulations (see Section 1.4).

The Exchanges also recommend that such agreements permit the Member to, if necessary, take appropriate action on behalf of their client. This would include, for example, closing out or otherwise liquidating affected contracts.

For Members that are DEA Providers, please see section 4.2 for requirements.

Where a Member is a Clearing Member of ICE Clear Europe, the ICE Clear Europe Customer-CM F&O Transaction Standard Terms ("ICEU F&O Standard Terms")[25] also apply and override such agreements to the extent of any inconsistency. Where a Member is a General Clearing Participant of ICE Clear Netherlands, a Clearing Agreement must also have been concluded.

Members and clients should ensure these are duly incorporated into client agreements, as set forth in the ICE Clear Europe Clearing Rules ("ICEU Clearing Rules") and ICE Clear Netherlands Clearing Rules ("ICN Clearing Rules"). Circular C14/055 (including any successor Circulars) provides details on the documentation Clearing Members and Customers of ICE Clear Europe should execute pursuant to ICE Clear Europe Rule 202(b).[26]

6.8 Jurisdictions[27]

Members should be familiar with specific jurisdictional obligations regarding entering orders on the Exchanges via the ICE Platform, and have in place appropriate policies and procedures to ensure compliance with any

[24] MiFID II, Articles 24(1) and 28(1); Organisational Requirements Delegated Regulation, Articles 67 to 70.

[25] Exhibit 2, ICEU Clearing Rules: https://www.theice.com/publicdocs/clear_europe/rulebooks/rules/Clearing_Rules.pdf.

[26] ICE Clear Europe Customer Documentation Requirements https://www.theice.com/publicdocs/clear_europe/circulars/C14055.pdf

[27] IFEU Jurisdictions Document: https://www.theice.com/publicdocs/futures_jurisdiction.pdf.

conditions that apply in that jurisdiction. Providing access to entities within jurisdictions prohibited by the Exchanges is not permitted.

7 Back office operations

The Exchanges remind Members of the importance of the specific procedures below and the need for Members to have in place clear, documented policies and procedures on each operational process. In addition these policies and processes should be regularly reviewed, at least on an annual basis, to ensure that they continue to be appropriate and do not cause a violation of Exchange Regulations:

- Close out procedures / Position maintenance: The Exchanges remind Members of the importance of completing their close out procedures accurately and adhering to the Exchanges' position maintenance cut-off times.
- Position reporting: The Exchanges also emphasise the importance of accurately reporting all positions by submitting their electronic large trader file(s) by the Exchanges' deadline.
- Default accounts: Members should not delay the correct registration or booking of a trade (for example, by allowing it to remain in a default account overnight) where such registration could be achieved more promptly.
- Physically deliverable contracts: Members are strongly encouraged to monitor and manage both their own and their clients' ability and decision to make and receive delivery of physically deliverable contracts.

8 Additional Membership requirements

Members are reminded of on-going Membership requirements, including notifying and seeking the consent of the relevant Exchange in relation to any changes in the nature of business or legal status of the Member.[28]

Members must keep the relevant Exchange up to date with the details of all contacts and Responsible Individuals (as defined in the relevant Exchange Regulations), and seek consent from the relevant Exchange for any proposed change to the identity or location of any Responsible Individual.[29] Such Exchange may need to contact a Member urgently and often only accepts instructions from Responsible Individuals when dealing with trade or execution issues, or administrators. It is essential that contact details of any relevant person, especially within compliance, are current.

9 Straight through processing

Under Article 29(2) of MiFIR, trading venues, CCPs and clearing members must have in place systems, procedures and arrangements to ensure that cleared derivatives are submitted and accepted for clearing as quickly as technologically practicable. This requirement is further specified in Commission Delegated Regulation (EU) 2017/582 (RTS 26). It is the Exchanges' view that the Exchange Regulations together with Part 4 (Rules 401 and 403) of the Clearing Rules and the Standard Terms (section 3(b)-3(c)), meet the conditions set out in Article 2(1)(a)-(c) of RTS 6.

10 Useful Reading

10.1 MiFID II

The following come into effect on 3 January 2018.

MiFID II Directive: Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU

[28] Rule B.5.1A(a), IFEU Exchange Rules; article I-7.2(a), ICE Endex Rules.

[29] Rule B.5.1A(b), IFEU Exchange Rules; article I-7.2(b), ICE Endex Rules.

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0065&from=EN.

MiFIR: Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0600&from=EN.

RTS 6: Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0589&from=EN

RTS 7: Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0584&from=EN

RTS 25: Commission Delegated Regulation (EU) 2017/574 of 7 June 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards for the level of accuracy of business clocks

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0574&from=EN

RTS 26: Commission Delegated Regulation (EU) 2017/582 of 29 June 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards specifying the obligation to clear derivatives traded on regulated markets and timing of acceptance for clearing

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0582&from=EN

Organisational Requirements Delegated Regulation: Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0565&from=EN

10.2 MAR

The following came into effect on 3 July 2016.

MAR: Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0596&from=EN.

Commission Delegated Regulation (EU) 2016/957 of 9 March 2016 supplementing Regulation (EU) No 596/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the appropriate arrangements, systems and procedures as well as notification templates to be used for preventing, detecting and reporting abusive practices or suspicious orders or transactions

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0957&from=EN.

Commission Delegated Regulation (EU) 2016/909 of 1 March 2016 supplementing Regulation (EU) No 596/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the content of notifications to be submitted to competent authorities and the compilation, publication and maintenance of the list of notifications

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0909&from=EN.

Commission Implementing Regulation (EU) 2016/347 of 10 March 2016 laying down implementing technical standards with regard to the precise format of insider lists and for updating insider lists in accordance with Regulation (EU) No 596/2014 of the European Parliament and of the Council

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0347&from=EN.

Commission Implementing Regulation (EU) 2016/378 of 11 March 2016 laying down implementing technical standards with regard to the timing, format and template of the submission of notifications to competent authorities according to Regulation (EU) No 596/2014 of the European Parliament and of the Council

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0378&from=EN.

10.3 Automated Trade Systems ("ATSs")

ESMA, 'Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities', published December 2011.

https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2012_122_en.pdf

10.4 Market Access

Futures Industry Association ("FIA"), Market Access Risk Management Recommendations, published April 2010.

https://secure.fia.org/downloads/Market_Access-6.pdf

10.5 Risk Controls – recommendations for trading firms

FIA – Principal Traders Group, Recommendations for Risk Controls for Trading Firms, published November 2010.

https://secure.fia.org/downloads/Trading_Best_Pratices.pdf

10.6 Operational risks

CEBS, Guidelines on the management of operational risks in market-related activities, published October 2010.

http://www.eba.europa.eu/documents/10180/16094/CEBS-2010-216-(Guidelines-on-the-management-of-op-risk-in-market-related-activities)-(2).pdf

10.7 Direct Electronic Access to Markets

International Organization of Securities Commissions ("IOSCO"), Principles for Direct Electronic Access to Markets, published August 2010.

http://www.iosco.org/library/pubdocs/pdf/IOSCOPD284.pdf

11 Important notice

The purpose of this Guidance is to provide general information to Members on the organisational obligations under MiFID II, which include obligations to have effective systems, procedures and controls in place to ensure that trading systems are resilient and have sufficient capacity, and that trading is orderly.

Although this document has been prepared on the basis of the best information available at the moment of preparation, the Exchanges accept no liability for any decision taken on the basis of this Guidance or for any omission in disclosure. This Guidance has been prepared on the basis of, and reflects solely, the law and the draft legislation as it exists at the date hereof, and the versions of the Exchange Regulations applicable upon the entry into force of the relevant requirements.

This Guidance does not provide all the information that may be needed for Members to assess their compliance with MiFID II or other legal requirements. This Guidance does not constitute legal, financial or any other form of advice and must not be relied on as such. This Guidance provides only a high level description or summary of a number of detailed legal requirements, whose effect will vary depending on the specific facts of any particular case. It is the responsibility of any person considering using or accessing the Exchanges, whether as a Member, client or otherwise, to review and conduct its own due diligence on the relevant Exchange Regulations, Electronic User Agreements, Procedures, Contract Rules, Contract Procedures, Trading Procedures, Policies, Transition Rules, Standard Terms annexes, Clearing Rules, other legal documentation and any other information that may be relevant to its decision on whether and how to use the Exchanges' services. Members, clients and any other users of the Exchanges should consult their own advisors as to the legal effect

of the contracts they are party to, relevant documentation mentioned above and the appropriateness of any of the above for their particular circumstances.

The Exchange shall not in any circumstances be liable, whether in contract, tort, breach of statutory duty or otherwise, for any losses or damages that may be suffered as a result of using this Guidance. Such excluded losses or damages include (a) any loss of profit or revenue; (b) damage to reputation or loss of any contract or other business opportunity or goodwill; or (c) any indirect loss or consequential loss. No responsibility or liability is accepted for any differences of interpretation of legislative provisions and related guidance on which this Guidance is based. This paragraph does not extend to an exclusion of liability for, or remedy in respect of, fraudulent misrepresentation, death or personal injury caused by negligence or any other liability which by applicable law may not be excluded or restricted.

This Guidance has been prepared on the basis of English laws and the law of the European Union save as otherwise stated. However, issues under other laws, such as those of the place of business of a Member or client or governing laws of documentation between Members and clients (including, without limitation, Standard Terms annexes, brokerage agreements, execution agreements and clearing agreements), and the law of the location of any assets, may be relevant to any due diligence.

12 Glossary of Terms

Algorithmic Trading

MiFID II, Article 4(1)(39): Algorithmic trading means trading in financial instruments where a computer algorithm automatically determines individual parameters of orders such as whether to initiate the order, the timing, price or quantity of the order or how to manage the order after its submission, with limited or no human intervention, and does not include any system that is only used for the purpose of routing orders to one or more trading venues or for the processing of orders involving no determination of any trading parameters or for the confirmation of orders or the post-trade processing of executed transactions.

Direct Electronic Access or “DEA”

MiFID II, Article 4(1)(41) - Direct electronic access means an arrangement where a member or participant or client of a trading venue permits a person to use its trading code so the person can electronically transmit orders relating to a financial instrument directly to the trading venue and includes arrangements which involve the use by a person of the infrastructure of the member or participant or client, or any connecting system provided by the member or participant or client, to transmit the orders (direct market access) and arrangements where such an infrastructure is not used by a person (sponsored access); and

Commission Delegated Regulation of 25.04.2016 as regards organisational requirements and operating conditions for investment firms, Article 20 -

(1) A person shall be considered not capable of electronically transmitting orders relating to a financial instrument directly to a trading venue in accordance with Article 4(1)(41) of Directive 2014/65/EU where that person cannot exercise discretion regarding the exact fraction of a second of order entry and the lifetime of the order within that timeframe.

(2) A person shall be considered not capable of such direct electronic order transmission where it takes place through arrangements for optimisation of order execution processes that determine the parameters of the order other than the venue or venues where the order should be submitted, unless these arrangements are embedded into the clients' systems and not into those of the member or participant of a regulated market or of an MTF or a client of an OTF.

High Frequency Algorithmic Trading Technique

MiFID II, Article 4(1)(40) - 'high-frequency algorithmic trading technique' means an algorithmic trading technique characterised by: (a) infrastructure intended to minimise network and other types of latencies, including at least one of the following facilities for algorithmic order entry: co-location, proximity hosting or high-speed direct electronic access; (b) system-determination of order initiation, generation, routing or

execution without human intervention for individual trades or orders; and (c) high message intraday rates which constitute orders, quotes or cancellations.

Sponsored access

See definition under Direct Electronic Access