Suspicious Transaction and Order Reporting under MAR - Implications for EU Asset Managers

DILLON EUSTACE

DUBLIN CAYMAN ISLANDS NEW YORK TOKYO

CONTENTS

Page

Suspicious transaction and order reporting ("STOR") under MAR – implications for EU asset managers

Overview

Persons professionally arranging or executing transactions in the EU, including brokers and asset management firms, are now subject to enhanced requirements in relation to the reporting of suspicious behaviour, trades or orders in financial instruments traded on regulated markets, multi-lateral trading facilities ("MTFs") and organised trading facilities ("OTFs") in the EU.

Article 16 of Market Abuse Regulation EU/596/2014 ("MAR") significantly extends the systems, reporting and recordkeeping obligations relating to suspicious transactions and orders and potential market abuse from the previous market abuse regime. Where such a person has a reasonable suspicion that an order or transaction in any financial instrument, whether placed or executed on or outside a trading venue, could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, the person is required to notify the relevant competent authority without delay.

> **MAR - Article 16** ***[extract]***
>
> *(2)* ***Any person professionally arranging or executing transactions shall establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders and transactions. Where such a person has a reasonable suspicion that an order or transaction in any financial instrument, whether placed or executed on or outside a trading venue, could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, the person shall notify the competent authority as referred to in paragraph 3 without delay.***
>
> *(3) Without prejudice to Article 22, persons professionally arranging or executing transactions shall be subject to the rules of notification of the Member State in which they are registered or have their head office, or, in the case of a branch, the Member State where the branch is situated. The notification shall be addressed to the competent authority of that Member State.*
>
> *(4) The competent authorities as referred to in paragraph 3 receiving the notification of suspicious orders and transactions ("STORs") shall transmit such information immediately to the competent authorities of the trading venues concerned.*

Commission Delegated Regulation 9/3/2016 supplementing MAR (the "Delegated Regulation") specifies that the obligations under Article 16(2) apply to orders and transactions relating to any financial instrument and shall apply irrespective of:

a) The capacity in which the order is placed or the transaction is executed;
b) The types of clients concerned;
c) whether the orders were placed or transactions were executed on or outside a trading venue – i.e. OTC[1].

The Delegated Regulation further clarifies that "persons professionally arranging or executing transactions shall ensure that the arrangements, systems and procedures are:

(i) appropriate and proportionate in relation to the scale, size and nature of their business activity;
(ii) regularly assessed, at least through an annually conducted audit and internal review, and updated when necessary;
(iii) clearly documented in writing, including any changes or updates to them, for the purposes of complying with the Delegated Regulation, and that the documented information is maintained for a period of 5 years; and
(iv) provided to the relevant competent authority upon request."[2]

To comply with Article 16(2) asset managers and other persons professionally arranging or executing transactions in the EU must put in place:

- **appropriate surveillance and monitoring systems (automated/human) to flag and identify potential suspicious orders and transactions in financial instruments traded on an in-scope market in the EU;**

- **appropriate policies to assess potential suspicious orders and transactions and to report such transactions and orders to the relevant competent authority without delay where appropriate;**

- **appropriate recordkeeping of decisions reached in relation to STORs, including both those reported to the competent authority and those where the suspicion was deemed not reasonable, such information to be retained for 5 years;**

- **regular training to ensure that all relevant staff understand their obligations and responsibilities and the policies of the firm in relation to STORs.**

[1] Delegated Regulation 3(2)
[2] Delegated Regulation 3(5)

The ESMA Technical Standards under MAR dated 28th September 2016 (the "TS") prescribe in further detail the requirements under Article 16 and can be viewed at the following link:

https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-esma-1455_-_final_report_mar_ts.pdf

Scope of MAR

The scope of the STOR regime includes suspicious orders as well as suspicious transactions.

MAR significantly extends the scope of financial instruments subject to the previous EU market abuse regime from (a) financial instruments traded (or which an application for admission to trading has been made) on a regulated market ("regulated market") in the EU, to also include (b) financial instruments traded (or for which a request for admission to trading has been made) on an MTF or OTF within the EU.

The scope of MAR also encompasses financial instruments not covered by (a) or (b) above, whose price or value depends on or has an effect on the price or value of a financial instrument in (a) or (b), including, but not limited to, feeder funds, credit default swaps and CFDs. The obligations include transactions conducted both on and off-exchange in the in-scope financial instruments.

OTFs will come within the scope of MAR with effect from 3rd January 2018, the implementation date of MiFID II. OTFs are likely to encompass some existing non-equity broker crossing networks and trading platforms. From January 2018 various types of cleared derivatives will also be traded on OTFs.

MAR also applies to any off-market trading in any of the instruments traded on a regulated market, MTF or OTF, including private trading in, for instance, debt securities admitted to trading on an MTF, such as the GEM market of the ISE.

A full list of relevant financial instruments will be published and updated by ESMA. It is unlikely that this list will be available until after the implementation of MiFID II in January 2018.

While the offenses of insider dealing, unlawful disclosure of inside information and market manipulation apply extra-territorially to include entities (and their personnel) from third countries trading in financial instruments within the scope of MAR, the provisions under 16(2) apply only to persons within the EU/EEA. It would not, for example, be expected that a US asset manager, trading in financial instruments listed on trading venues in the EU, have policies to detect and report market abuse under MAR. It would however be possible for a US manager to be guilty of market abuse offences under MAR in relation to such financial instruments – for example: a trade in the shares of a US company conducted on NADSAQ by a US individual on the basis of inside information where the shares of that company are also traded on a regulated market, MTF or OTF in the EU.

The obligation under 16(2) applies to those firms which are directly engaging in the relevant transactions and orders, such as discretionary asset managers. AIFMs and management companies which delegate the responsibility for investment management to another firm would not be within scope.

Obligation to Report

Article 16 of MAR imposes obligations on persons professionally arranging or executing transactions to establish and maintain effective arrangements, systems and procedures to detect suspicious transactions and orders and to report them to the relevant competent authority without delay.[3]

It will be necessary to report suspicious orders whether or not they have been executed (e.g. where an entity has refused to place an order for a client), as well as transactions that might constitute market abuse or attempted market abuse.[4]

The obligation to submit STORs also extends to OTC derivatives trading where the underlying instrument is traded on a regulated market, MTF or OTF[5]. The obligation also applies irrespective of the trading activity in which the order is entered or the transaction is executed (e.g. on own account, on behalf of a client), and irrespective of the types of client concerned (e.g. institutional, professional, retail).[6]

Regulators, including the FCA, have advised that they believe that many firms adopt a too-cautious approach to filing – for example, seeking a level of evidence or proof that market abuse has taken place before making a filing. Firms should be cautious of reasons not to submit. It is believed that there is a general under-reporting across most asset classes.

Detection and Systems

Article 16(2) imposes a requirement to establish and maintain effective arrangements, systems and procedures to be able to detect suspicious orders and transactions. These systems are expected to include granularity and detail on the information being reported, and effective record keeping.[7] Regular risk assessments are important, including detailed assessments of market abuse risks, key responsibilities or managing and mitigating those risks including the controls employed.

[3] TS 135
[4] TS 138, Recital 41 of MAR
[5] The definition of OTF will be effective on the application date of MiFID II, January 2018
[6] TS 139
[7] TS 148

In order to detect market abuse and attempted market abuse, entities will need to have in place systems capable of the analysis of every transaction and order, individually and comparatively, which produces alerts for further analysis. ESMA believes that in the large majority of cases this will necessitate an automated surveillance system. ESMA also recognises in the TS that, given the broad range of persons to whom Article 16(2) applies, an automated system may not be appropriate or proportional in every scenario. What is considered important is that the surveillance system in place is an effective form of monitoring for that entity given its size and the nature of its business.[8]

In considering whether an automated system is necessary and if so, its level of automation, entities are required to take into account the number of transactions and orders that need to be monitored, the type of financial instruments traded, the frequency and volume of orders and transactions, and the size, complexity and nature of their business. The surveillance system should cover the full range of trading activities undertaken by the entity. The entity should be able to explain to the relevant competent authority upon request how they manage the alerts generated by the system and why such a level of automation is appropriate and fit for purpose for their business.[9]

The TS provide that there should always be an element of human analysis in the detection of orders and transactions that could be market abusive and that the most effective systems are expected to be a mixture of both automated and human forms.[10]

In considering best practice, the FCA has advised[11]:

> off the shelf and in-house designed surveillance systems can be equally effective when used properly. In smaller firms, simple surveillance systems involving spreadsheet software are often used effectively.
>
> One of the most important aspects of a successful system is the manner in which it has been implemented, and on an on-going basis, constantly refined and tested. Alert parameter and logic should be carefully calibrated on an ongoing basis based on the surveillance officer's experience of the firms trading patterns and clients.
>
> analysts of alerts generated by systems should ideally have access to a wide range of the firm's data and be empowered to investigate each alert fully, maintain detailed audit trails and a clear process for closure of alerts.
>
> reliance on random sampling or investigation of unusual activity is not satisfactory.

[8] TS 149
[9] TS 150
[10] TS 151
[11] FCA – Market Watch – No. 48, 50, 51

many surveillance teams sit within the compliance function, providing detailed management information to front office. Where surveillance functions are within the front office/at management level, potential conflicts of interest should be considered.

the compliance team should be well-resourced and independent in order to provide a genuine challenge where necessary.

the most effective surveillance comes from an independent function with a reporting line to senior management that is, as far as possible, non-conflicted.

Delegation and Outsourcing

The TS provide for (a) delegation of the functions under 16(2) within the same group and (b) the outsourcing of certain analytics to third parties, however, in each case, the ultimate responsibility for compliance shall remain with the entity arranging or executing transactions.

Entities within a group may delegate the functions of monitoring, detection and identification of suspicious orders and transactions to another entity within the group. This should facilitate the sharing of resources, allowing for the central development and maintenance of monitoring systems and the building of expertise in the context of monitoring orders and transactions. In any case, the delegating entities will remain fully responsible for their obligations under Article 16 and should be the persons submitting any STOR to the competent authority. They should also still be able to conduct an analysis that complements any alert generated by the systems of the delegated entity.[12]

In addition to the possibility of delegating to entities of the same group, entities may outsource the performance of data analysis, including order and transaction data, and the generation of alerts necessary to conduct monitoring, detection and identification of suspicious transactions and orders. The outsourcing entities will remain fully responsible for all of their obligations under Article 16 and should:

a) retain the expertise and resources necessary for evaluating the quality of the services provided, the organisational adequacy of the providers, for supervising the outsourced services effectively and for managing the risks associated with the outsourcing on an ongoing basis;
b) have direct access to the relevant information of the outsourced data analysis and generation of alerts;
c) define in a written agreement their rights and obligations and those of the providers. The outsourcing agreement should allow the persons professionally arranging or executing transactions to terminate it.[13]

[12] TS 153
[13] TS 154

Example:

An Irish UCITS - Company A acts as Management Company, delegating investment management to Company B. Company B may be related or unrelated to Company A.

In this scenario, Company B is responsible under Article 16(2) as it is the person professionally arranging or executing transactions.

Company B may delegate, within its group, the function of surveillance, detection, and identification of possible suspicious transactions, but Company B will retain ultimate responsibility under Article 16(2) and should be the entity filing all STORs with the relevant competent authority.

Company B has a further option of outsourcing the data analysis to a third party, but retains full responsibility for compliance and filings under Article 16(2).

Company A has no responsibility under Article 16(2) as it is not professionally arranging or executing transactions.

In practice, many firms are moving surveillance teams offshore or near shore to serve as the first filter on generated alerts. It is important that firms have strong training and development programmes for offshore teams, ensuring that they are integrated with the onshore surveillance team and able to effectively challenge where necessary and escalate issues of concern. Onshore surveillance should conduct ongoing quality assurance as a key control to ensure the offshore teams consistency and compliance with standards. This can include regular visits by the compliance team. It is important that the offshore team has full access to the necessary system, information and data stores to allow them to properly assess any alerts generated.

Internal Procedures to facilitate detection and reporting

Entities are required to adopt systems and procedures to document, recall and review the analysis performed on STORs which have been submitted, as well as those suspicious transactions and orders which were analysed but in relation to which it was concluded that the grounds for suspicion were not reasonable. ESMA considers that this analysis will form an important part of detecting patterns and evidencing compliance with these requirements. Entities are not required to have procedures to document every alert – only those that were analysed and examined as being potentially suspicious of being sufficiently abusive to warrant a notification, even if later they were disregarded as being such.[14]

[14] TS 145

Timing of STORs

Reports should be made "without delay". Guidance under the previous market abuse regime that reports should be submitted within two weeks of the suspected breach (the transaction or order) is no longer acceptable.[15]

Entities should not only notify transactions and orders which they consider suspicious at the time of the relevant transaction, but also transactions and orders which become suspicious retrospectively in the light of subsequent events or information (such as new orders and/or transactions by the same person). Entities should not wait for a sufficient number of suspicious orders or transactions to accumulate before reporting.[16]

In cases where a suspicious transaction or order is detected some time after it has actually occurred, the reporting person should be able to justify to the relevant competent authority, if requested, the delay according to the specific circumstances of the case.[17]

Persons reporting suspicious orders or transactions by telephone must also report in full in writing using the appropriate template provided by the relevant competent authority.[18]

Where persons who have already submitted a STOR become aware of additional information that could be relevant, such additional information should be provided to the competent authority.[19]

Partial View

Entities subject to Article 16(2) of MAR should generally base their suspicion on what they see or know and should avoid presumptions about other activities. However, entities have to take into account all information available to them, such as public disclosure of other trades. Where there are circumstances where there are good reasons for, or certain indications for, suspecting something which the entity does not know for sure, this should be clearly stated on the STOR.[20]

[15] TS 141
[16] TS 143
[17] TS 142
[18] TS 144
[19] TS 145
[20] TS 146

Reporting by Multiple Participants in a Transaction

Where a chain of market participants are involved in a transaction, each person is subject to the requirement to submit a STOR in relation to their own suspicions. Reporting by one entity does not absolve another of its duty to report.[21]

Training

Effective monitoring must also include comprehensive training genuinely dedicated to monitoring, detecting and reporting suspicions of market abuse or attempted market abuse. Such training should take place on a regular basis[22] and should be tailored to the entity's business, having regard to, but not limited to, the firm's size, structure, systems and activities.[23]

Effective training should be provided to all relevant staff. The training programmes should ensure that staff, and in particular front office staff, are mindful of behaviours which could constitute attempted market abuse. [24]
Employees at all levels, and particularly compliance, management, trading and marketing teams, should understand their role in controlling flows of confidential and inside information, their obligations to report any suspicions and this should be implemented as part of how they carry out their work.

Effective training should involve scenario running, with face to face discussions of what suspicious transactions would look like, and how market abuse might present itself to a variety of roles within the firm.

Tipping Off

Reporting persons should not tip-off the person in respect of which the STOR was or will be submitted or anyone who is not required to know about the submission of a STOR.[25]

Content of a STOR and Template

The STOR should include clearly presented and accurate information, sufficient to enable the relevant competent authority to promptly assess the validity of the suspicion and to initiate a follow up investigation where appropriate.[26] The narrative should be used to provide as much relevant information as possible.[27] As many fields as possible should be completed. Every field will not be relevant for every report.[28]

[21] TS 147
[22] Delegated Regulation 4(1)
[23] TS 161
[24] TS 160
[25] TS 162
[26] TS 164
[27] TS 165
[28] TS 166

Personal information may be required to allow the competent authority to precisely identify the person in respect of which the STOR was submitted.[29] Any processing of personal data should be carried out in compliance with appropriate data protection legislation.

The template STOR issued by the Central Bank of Ireland is available at this link:

https://www.centralbank.ie/regulation/industry-market-sectors/securities-markets/market-abuse-regulation/suspicious-transaction-reports

Record Keeping

All entities should document any changes or updates to the policies, arrangements and procedures aimed at identifying and preventing market abuse, and ensure that the information is maintained for a period of five years.[30]

As part of these procedures, entities should keep record of every STOR submitted to the competent authority, including all the information considered in the preparation and notification of the STOR, for a period of 5 years from the relevant transaction.

All entities should also keep for five years the records and details of, and the analysis carried out with regard to, suspicious transactions and orders which have been examined but not reported to the competent authority due to the conclusion that the suspicion was not reasonable, together with a summary of the reasons for not submitting a STOR.[31]

Entities submitting STORs, as well as competent authorities receiving them, should ensure that records of reports are kept confidential.[32]

[29] TS 167
[30] TS 169
[31] TS 170
[32] TS 171

Sanctions

MAR provides for the following administrative sanctions and other administrative measures.

(i) Cease and desist conduct order;
(ii) Disgorgement of profits or losses avoided;
(iii) Public warning;
(iv) Withdrawal/suspension of authorisation of an investment firm;
(v) Temporary ban on a person discharging managerial responsibility in investment firms;
(vi) In the event of repeated infringements, a permanent ban on a person exercising managerial responsibility in investment firms;
(vii) Temporary ban on a person discharging responsibility within the issuer trading on own account;
(viii) Maximum sanction of 3 times profits gained or losses avoided resulting from the breach;

For individuals: Up to €1 million for failure to maintain adequate systems and controls to prevent market abuse or to report suspicious transactions or orders.

For legal entities: Up to €2.5 million or 2% of annual turnover in the preceding business year for failure to maintain adequate systems and controls to prevent market abuse or to report suspicious transactions or orders.

General Requirements under MAR

Further detail on the full requirements under MAR for listed issuers can be found at the link below:

http://www.dilloneustace.com/download/1/Publications/Financial%20Services/Market%20Abuse%20-%20A%20New%20Regime%20for%20Investment%20Funds%20(Nov%202016).PDF

For further information on MAR please contact the Listing Team or your usual Dillon Eustace contact.

Date: **June 2017**
Author: **Tara O'Callaghan**

CONTACT US

Our Offices

Dublin
33 Sir John Rogerson's Quay
Dublin 2
Ireland
Tel: +353 1 667 0022
Fax: +353 1 667 0042

Cayman Islands
Landmark Square
West Bay Road, PO Box 775
Grand Cayman KY1-9006
Cayman Islands
Tel: +1 345 949 0022
Fax: +1 345 945 0042

New York
245 Park Avenue
39th Floor
New York, NY 10167
United States
Tel: +1 212 792 4166
Fax: +1 212 792 4167

Tokyo
12th Floor,
Yurakucho Itocia Building
2-7-1 Yurakucho, Chiyoda-ku
Tokyo 100-0006, Japan
Tel: +813 6860 4885
Fax: +813 6860 4501

e-mail: enquiries@dilloneustace.ie
website: www.dilloneustace.com

Contact Points

For more details on how we can help you, to request copies of most recent newsletters, briefings or articles, or simply to be included on our mailing list going forward, please contact any of the team members below.

Tara.ocallaghan@dilloneustace.ie
E-mail: tara.ocallaghan@dilloneustace.ie
Tel : + 353 1 673 1831
Fax: + 353 1 667 0042

Fionnan Gannon
E-mail: fionnan.gannon@dilloneustace.ie
Tel : + 353 1 673 1867
Fax: + 353 1 667 0042

Helen Daly
E-mail: helen.daly@dilloneustace.ie
Tel : + 353 1 673 1830
Fax: + 353 1 667 0042

DISCLAIMER:
This document is for information purposes only and does not purport to represent legal advice. If you have any queries or would like further information relating to any of the above matters, please refer to the contacts above or your usual contact in Dillon Eustace.

Copyright Notice:
© 2017 Dillon Eustace. All rights reserved.

DILLON EUSTACE

DUBLIN CAYMAN ISLANDS NEW YORK TOKYO