FICC MARKETS STANDARDS BOARD

FICC Markets Standards Board

Suspicious Transaction and Order Reporting

Statement of Good Practice for FICC Market Participants

TRANSPARENCY DRAFT

May 2018

I Introduction

1. The FICC Markets Standards Board

The FICC Markets Standards Board ("FMSB") was established in 2015 in response to the Fair and Effective Markets Review in the UK with a mandate to issue Standards designed to improve conduct and raise standards in the wholesale Fixed Income, Commodity and Currency ("FICC") markets. The FMSB will work to build up a body of Standards and Statements of Good Practice ("SGPs" and each an "SGP") over time, prioritising those areas where its members consider there is a lack of clarity in the standards of behaviour expected of market participants, or a lack of understanding of the issues relevant to a product or transaction type, or evidence of poor conduct.

2. Applicability of FMSB Statements of Good Practice

FMSB SGPs are issued by the FMSB from time to time. SGPs do not form part of the FMSB Standards and they are not subject to FMSB's adherence framework. Rather they reflect FMSB's view of what constitutes good or best practice in the areas covered by the SGP in question. FMSB members are expected, and other firms are invited, to consider their own practices in light of the SGP and make any changes to such practices that they deem to be appropriate. Failing to do so will not, however, create any presumption or implication that a firm has failed to meet its regulatory or other obligations.

Full details of FMSB member firms are available at http://www.fmsb.com. SGPs will be shared with non-member firms and their associations, who are encouraged to consider them. Information on SGPs will be made available to users of the wholesale FICC markets (e.g. corporates and end investors) so that they may be made aware of their existence and FMSB expectation of market conduct.

The FMSB will, as part of its normal course of business, periodically review the applicability of its published SGPs to ensure they are relevant and up to date for market conditions.

3. Relationship with law and regulation

FMSB Standards and SGPs do not impose legal or regulatory obligations on FMSB members, nor do they take the place of regulation. In the event of any inconsistency, applicable law, rules and regulation will prevail. In developing Standards and SGPs, certain relevant regulators will in many cases have commented on their drafting, alongside member firms and other bodies, such that the Standards and SGPs once finalised and published are intended to represent an authoritative statement of global good practices and processes.

National laws on employee monitoring vary significantly and some of the monitoring requirements expressed in this guidance may conflict with local laws. As such, this guidance is intended to be considered to the extent it is possible to follow it in compliance with applicable laws. Laws governing data retention periods for documentation in general and suspicious transactions in particular vary between jurisdictions and readers are reminded to check applicable periods in the areas in which they operate.

4. Relationship with other Codes

Other codes already exist in relation to certain FICC markets, such as the FX Global Code, whilst others are in the process of being produced. There will be some overlap between the work of the FMSB and such other bodies and the FMSB will seek to ensure it adopts a consistent approach in cases of overlap wherever possible, and will seek to avoid issuing a Standard or SGP where the subject matter is already covered adequately by existing regulation or a Code issued by another body. It may, however, draw the attention of member firms to an existing code and request that members act in a manner consistent with it, once appropriate steps have been taken to confirm its applicability.

II Suspicious Transaction and Order Reports

1. Background

This SGP covers the identification of suspicious orders and transactions and their reporting to relevant regulators (the FCA in the case of the UK). Many of the practices described relating to the identification and investigation of suspicious activity will be relevant to many jurisdictions. This SGP is designed to be relevant to all front-office and control or support function personnel who are active participants in the FICC markets and to those who are engaged in the monitoring and surveillance of those activities. Where the document describes good practice in relation to submission and handling of reports specifically to the FCA, this is by definition limited in scope to entities regulated in the UK. Firms however may choose to extend or incorporate this practice to cover other jurisdictions where necessary or appropriate as part of a holistic approach to notification and analysis.

In the UK and other jurisdictions, regulated trading venues and market participants who professionally arrange or execute transactions have a regulatory obligation to: establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders[1] and transactions in financial instruments (including any cancellation or modification thereof); and 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 where they have formed the view that there is a reasonable suspicion that such order or transaction constitutes insider dealing, market manipulation or an attempt to commit either one. Please refer to Annex 2 for information for submission of STORs in the UK.

A firm which arranges or executes orders or transactions with or for a client must notify the relevant regulator without delay upon forming such view.

2. Scope and Applicability

This document outlines Statements of Good Practice for the identification of reportable transactions and orders and the associated processing of Suspicious Transaction and Order Reports. Initiation of an internal investigation into potentially suspicious activity can originate from alerts generated by trade or communications surveillance systems, direct escalation by individuals or by whistleblowing events. However, many of the good practices for undertaking the investigation and processing any resultant STOR are consistent across these different sources.

FMSB expects each firm to consider their own practices in light of this SGP and consider the extent to which any changes might be appropriate. FICC market firms are very diverse and therefore in considering the SGP firms should interpret them in light of their own circumstances and develop arrangements, systems and procedures which are appropriate and proportionate in relation to the scale, size and nature of their business activity.

Readers are reminded that the STORs regime in the UK and certain other reporting requirements in other jurisdictions apply to all market participants, and have wider applicability than just regulated firms.

[1] "Order" is defined in Commission Delegated Regulation (EU) 2016/957 to include quotes.

III Good Practice Statements and Commentary

1.1 Organisation, roles and responsibilities

Good Practice Statement 1: Firms should have a clear organisational structure in place to facilitate monitoring and reporting of suspicious orders or transactions. Surveillance activities should be appropriate, independent and proportionate in relation to the scale, size and nature of the business activities of the firm.

This Good Practice Statement is in line with Good Practice Statement 1 of the FMSB Statement of Good Practice for Monitoring of written electronic communications. Firms with voice business may wish to consider whether it is appropriate for them to adopt analogous practices for non-written communications. The concepts of good practice for organisation, roles and responsibilities are consistent for the various functions of surveillance and monitoring required across a firm.

The organisational structure and reporting lines for surveillance activities should be defined and documented across the three lines of defence such that there is demonstrable independence from the activities which are being monitored.

Surveillance activities should wherever possible be owned by a function which is independent from the first line business activities and/or controls in the first line of defence. The function should have competent expertise and experience to provide meaningful control. The FMSB notes that the following models are used in the industry for achieving this outcome:

- Surveillance activities to be driven in the second line of defence (for example, the Compliance Function).
- Surveillance activity to be driven from a control function in the first line of defence (sometimes referred to as Line "1B") provided that this function is able to demonstrate independence and ringfencing of surveillance output from the business, reasonably designed to perform the activities described in this document.
- Surveillance activity to be carried out in the first line of defence in addition to the surveillance by the second line of defence, including as part of periodic event-driven reviews.

Surveillance output and Management Information should be reported into the relevant individuals and governance functions in the organisation, as appropriate to their business models and compatible with the principle of confining sensitive information within the "need to know" group, to provide senior management with visibility, understanding and oversight of potential suspicious behaviour. Reporting routes could include:

- Specific senior management roles (e.g. Business Heads, Head of Compliance, Head of Risk).
- Relevant business as usual committees of sufficient seniority (e.g. Risk Committees, Compliance Committees, Audit Committees).

- Specific committees in the event of a breach occurring (e.g. breach committees, disciplinary committees).

Firms should make reasonable efforts to design escalation processes to be used in the event of a potential breach which are fit for purpose, formalised and documented. The FMSB notes the following examples of the types of models used in the industry for achieving this outcome:

- Categorisation of breaches into levels to determine the escalation requirement.
- Escalation within the second line reporting structure in the first instance (where the surveillance function sits in the second line).
- Subsequent further escalation to senior management and other control functions as appropriate, per the judgment of the surveillance function.
- Bilateral communication between the surveillance function and anti money laundering ("AML") group to cross-reference any potential suspicions between the two areas and ensure relevant reporting obligations STOR/SAR are identified.
- Escalation is achieved within formal governance structures or on an ad hoc basis through existing reporting lines in the organisation depending on the urgency, impact and/or nature of the relevant breach.

Good Practice Statement 2: Roles and responsibilities should be clearly defined for the monitoring and reporting of suspicious orders and transactions. They should be defined across the lines of defence, with appropriate allocation of resources and appropriate documentation of these roles and responsibilities.

Functional roles and responsibilities for monitoring orders and transactions should be clearly defined and documented with clear ownership aligned to the organisational model of the function. As outlined in Good Practice Statement 1, individuals should have the appropriate expertise and experience to perform the roles and responsibilities assigned to them.

This should include clear articulation of the roles and responsibilities as well as required sign-off procedures for the following processes:

- *Surveillance & Notification policies and procedures*: These should include guidance as to escalation, decision-making, record keeping and actual submission of notifications. Policies and procedures should be regularly reviewed and updated as necessary by defined staff.
- *Design and implementation of tools*: Design and testing of the functionality of surveillance tools.
- *Alert logic*: Initial alert design, construction and associated analytics, ongoing periodic and event-driven alert logic updates.
- *Day to day monitoring*: Automated and manual monitoring of orders, messages and transactions across in-scope trading channels.
- *Investigation*: Filtering, investigation and closing out of flagged suspicious activity cases.

- *Ongoing testing and calibration*: Periodic and event-driven testing of surveillance tools, ongoing calibration of tools to optimise detection capabilities to minimise volume of false positives.
- *Reporting and Management Information*: Reporting of day-to-day surveillance output (business as usual as well as in the case of breaches, ad hoc and event driven) as well as surveillance effectiveness.
- *External reporting*: including for the submission of STORs and/or SARs to regulatory authorities. Members of a control function team should be identified and documented to hold login details and abilities to submit a STOR.

Good Practice Statement 3: Surveillance capabilities should be supported by the firm's conduct risk framework.

Embedding a consistent understanding of conduct risks throughout the risk management framework of a firm can support the identification, assessment and monitoring of those risks. This approach supports the development and maintenance of risk-based automated surveillance as well as more manual monitoring programmes dependent on the area of risk.

1.2 Training

Good Practice Statement 4: Firms should have a regular training programme in place in which employees are educated on how to identify and escalate suspicious orders and transactions.

All in scope employees should receive regular training to promote understanding of their responsibility to be alert to and report any suspicious trading behaviour or patterns to the relevant function within their firm as described in Good Practice Statement 1. Escalation may be made to the Compliance Department, senior management or another identified independent function responsible for the monitoring of market abuse.

Employees should also be educated on internal whistleblowing procedures and any relevant independent regulator managed whistleblowing line (such as the one operated by the FCA) as a separate method for reporting suspicious trading behaviour or patterns should they feel uncomfortable escalating internally or wish to stay anonymous.

Training should be mandatory for all in-scope staff and should occur on a regular schedule appropriate for the firm. Records of all employee training should be retained and be available for review. Firms should regularly review and record which staff are in scope. Firms should satisfy themselves that the content of training materials are relevant and appropriate to the seniority of staff and the markets in which they operate.

1.3 Suspicions captured by the Surveillance System

Good Practice Statement 5: Firms should have a structured approach to calibrating their surveillance systems to identify suspicious orders and transactions. The analytics should be regularly reviewed and updated to improve the detection of potential suspicious behaviour.

Design and Calibration

Electronic surveillance systems should be appropriate and proportionate in relation to the scale, size and nature of the business activities of the firm. Electronic surveillance systems should be designed to analyse the in-scope daily trading data through a set of logic and look back scenarios searching for potential suspicious trading and/or messaging behaviour executed or attempted through the firm.

An analysis can be undertaken with the relevant business experts to determine which suspicious behaviours may have the potential to occur for certain products, departments, protocols and/or scenarios, and such findings should be fed back into the system design. If gaps are identified firms should consider whether additional steps are required to monitor for certain scenarios manually via spot checking or to build automated surveillance alerts for these areas.

A risk analysis should be undertaken to calibrate the surveillance system. The risk analysis will be proportionate for the firm and take into account the various products, market participants and protocols which can be rated against various market abusive behaviours. Some behaviours/alerts will be standard across asset classes. Other alerts may require individual calibration with in-house experts to mitigate the individual risk associated with each unique asset class, protocol and scenario. For example, alerts that look for specific behaviours for Equity products may be less valuable when applied to Fixed Income or derivative products.

As calibration of such systems is a continually evolving, complex and timely project, a staged approach should be planned and documented with areas representing the highest risk being calibrated first. Risk could be assessed by considering:

- Materiality of potential event to organisation
- Materiality of potential event to the market
- High risk time periods such as benchmark fixing/closes
- Areas/products with highest volumes
- Areas/products v behaviours/alerts rated as high risk of occurring

Feedback from thematic reviews and events

Ongoing thematic reviews of outputs should be communicated to the appropriate internal committees / management and evaluation of results should be fed back in to calibrate the system further. Any material event picked up by means other than the surveillance system, such as escalations or reports raised by employees, FCA or other regulator final notices or

market events should be recorded and reviewed as to whether it was captured in the automated surveillance system. If it was not, an analysis should be undertaken to discover why and to determine whether the system should be calibrated to promote the detection of a similar event in the future. This continuous feed-back loop is part of the ever-evolving nature of the automated surveillance system and should be subject to appropriate governance to oversee and track changes.

1.4 Controls and processes

Good Practice Statement 6: Alerts arising from surveillance systems should be processed, investigated and closed out in a diligent manner in line with agreed and documented processes and governance. Investigation should be conducted by surveillance or control officers with relevant expertise and experience as outlined in Good Practice Statement 1 with specific consideration for the targeted engagement with front office and other relevant areas of subject matter expertise to cater for appropriate and informed analysis.

Alerts should be reviewed by surveillance or control officers in the firm who are not compromised by the nature of their involvement in the activities under review as described in Good Statement Practice 1. Alerts should be directed to, and reviewed and investigated as required by the most appropriate function, such as the Compliance Department. Materiality of the risk should be used as a prioritisation tool for reviewing and investigating alerts. Front Office representatives should be engaged in review and investigation of escalations as required and at the discretion of the surveillance or control officers leading the review.

It is critical that case escalations are considered by appropriately independent parties within the organisation and allocated taking into account appropriate access to information (e.g. based on seniority of the individual involved, whether it involves Material Non-Public Information etc.).

Firms may employ a tiered approach to alert processing and investigation, similar to that described below, and firms should consider what variations are most appropriate for the nature and operating model of the firm. All alert resolution processes should have clear decision points at which a view can be formed on whether there is a reasonable suspicious of actual or attempted insider dealing or market manipulation to report to the relevant authorities.

Example tiered approach to processing surveillance alerts

- *Level 1 Reviewed and closed:*

  An alert is processed by the appropriate surveillance officer, compliance officer and/or first line of defence control officer to determine if an escalation is warranted. If it is concluded that there has not been any suspicious behaviour, the reasoning is recorded and the alert is closed with no further action taken.

- *Level 2 Reviewed, escalated and closed:*

An alert is reviewed by the appropriate surveillance officer, compliance officer and/or first line of defence control officer who form the view that there is a reasonable suspicion of actual or attempted insider dealing or market manipulation. Case is escalated to concerned staff members to obtain further information and/or escalated to relevant parties (e.g. staff line manager, compliance officer) for review, after which it is concluded that there is no such reasonable suspicion. At this level of the alert resolution process, there should be controls in place to avoid the individual that triggered the alert becoming aware, or being "tipped off" of the surveillance review until the appropriate time.

- *Level 3 Reviewed, escalated, investigated, addressed by the business/compliance and closed:*

An alert is reviewed by the appropriate surveillance officer, compliance officer and/or first line of defence control officer who form the view that there is a reasonable suspicion of actual or attempted insider dealing or market manipulation. Case is escalated to relevant parties for review, who agree with such view. An investigation ensues. Findings are distributed to relevant management who find no such reasonable suspicion. The event is recorded and closed. These events are sometimes referred to as 'near misses'. At this level of the alert resolution process, there should be controls in place to avoid the individual that triggered the alert becoming aware, or being "tipped off" of the surveillance review until the appropriate time.

- *Level 4 Reviewed, escalated, investigated, addressed by the business/compliance and reported to appropriate regulator:*

An alert is reviewed by the appropriate surveillance officer, compliance officer and/or first line of defence control officer who form the view that there is a reasonable suspicion of actual or attempted insider dealing or market manipulation. Case is escalated to relevant parties for review, who agree with such view. An investigation ensues. The findings are distributed to relevant management who also agree with such view and conclude that the behaviour should be reported to the regulator via a STOR. The event is recorded and reported to the regulator.

Complex and long-running cases

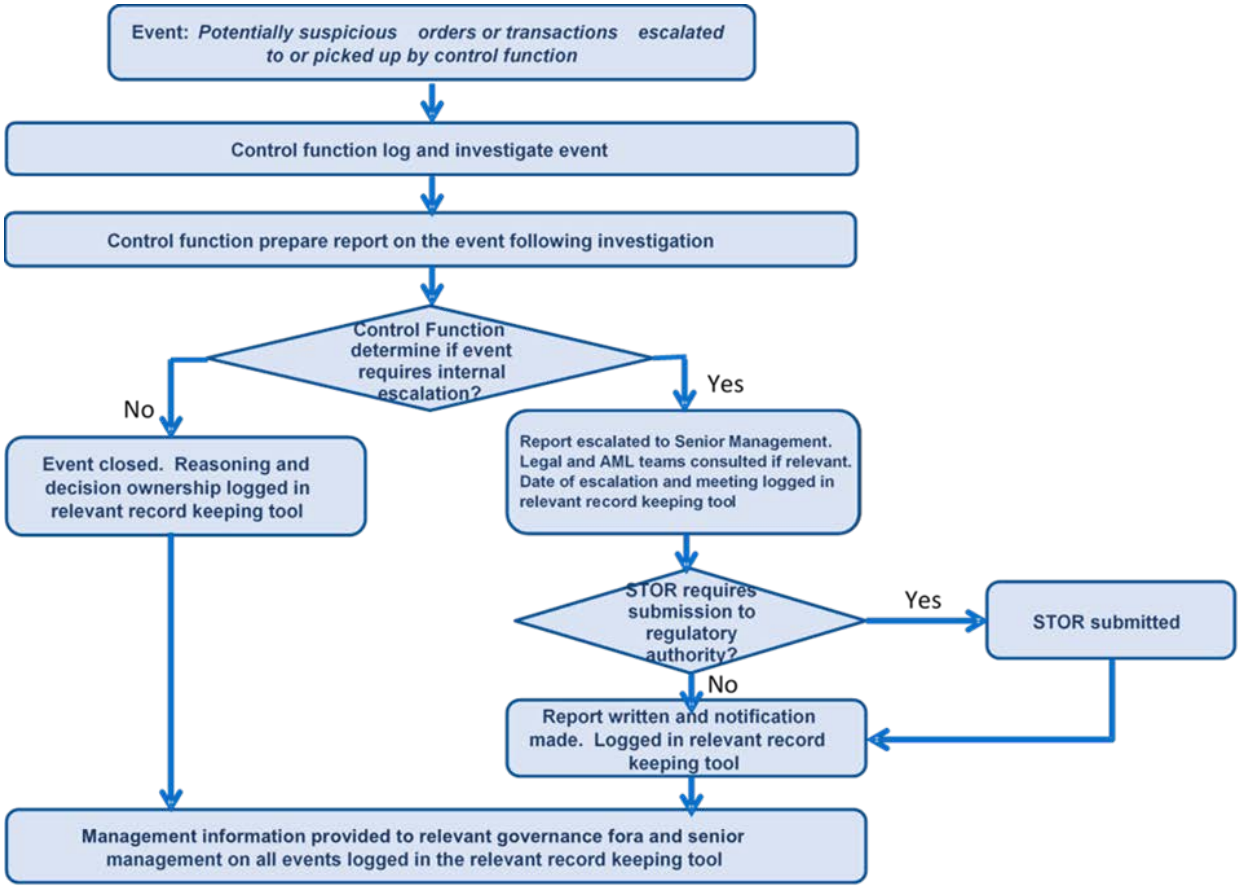
Some scenarios will be straightforward and submitted as a STOR promptly such as vanilla "Insider Dealing" or "Front Running" suspicions. Other cases will be far more complex and dependant on underlying instruments, strategies and numerous participants which will require a more thorough and lengthy trend analysis over a period of time. This gathering of data can be managed in "cases" in the surveillance system which will allow a full picture to be formed and "reasonable suspicion" to be reached in order to submit the findings to the relevant regulator. It is important to stress that a STOR should be submitted without delay once a reasonable suspicion of actual or attempted insider dealing or market manipulation has been formed and firms do not have an unlimited period of time to reach the point of reasonable suspicion. Moreover, where preliminary analysis is required, this should be conducted as quickly as possible. All alerts related to a suspicion should be stored in a case file with patterns and reasons recorded within the case for later recall. All such records should be retained for at least the minimum period required in the relevant jurisdiction.

There will be times when a suspicious transaction or order may only be detected sometime after it occurred. For example, where suspicion has arisen in the light of subsequent events; only after a pattern of behaviour has occurred over a period of time may a market participant become an outlier in comparison to other market participants in the frequency of the behaviour. This may then constitute the reason to initiate an investigation which may span back to messages over a long period of time. Firms should nevertheless report such orders or transactions without delay once the reasonable suspicion is formed. In such cases ESMA and the appropriate national regulator would expect the reporting person/firm to be able to justify, if requested, the delay according to the specific circumstances of the case. If the suspicious behaviour evolves or changes over time or additional information is discovered that could be relevant, then a further report should be made, referencing the earlier report.

All alerts investigated, outcomes and on-going trend analysis across clients, dealers and instruments (dependent on what is appropriate and relevant for the firm) should be documented. High level statistics should be reported in Management Information.

In some cases, further information gathering and analysis may be required. It may be necessary to make enquiries with clients and/or dealers. This should be approached carefully so as not to tip-off the person and/or firm in respect of which the STOR may be required to be submitted or anyone who is not required to know about the submission and firms must not delay submitting a STOR once a reasonable suspicion is formed.

Following this further analysis, the decision should be taken as to whether a view can be formed on whether there is a reasonable suspicion of actual or attempted insider dealing or market manipulation and if so to report it (See Good Practice Statement 8 on forming 'reasonable suspicion'). The event should be recorded with rationale as to why and by whom the decision was taken (see Good Practice Statement 10 on record keeping). This data should also be included in the relevant Management Information.



1.5 Processes for maintaining effective manual monitoring

Good Practice Statement 7: In addition to reactive alert based surveillance systems, firms should consider other monitoring programmes for manual surveillance which reflect the inappropriate behaviour and risks in firm activities that the firm is attempting to prevent and/or detect.

Monitoring programmes for additional trade surveillance independent of any automated alert based surveillance systems should be considered to be developed and maintained by individuals and/or functions who are appropriately independent (as described in GPS 1) to the population under surveillance. A range of approaches exist to developing programmes and logic but the following practices could be used:

- Monitoring programme development from design to implementation should be owned by the surveillance group (in the first or second line of defence depending on the organisational model)
- Systematic review of identified themes or risks (e.g. market manipulation, collusion etc.)
- Consultation of experts in the organisation (e.g. within compliance, operations, senior business people) and external to the organisation as appropriate
- Regulatory guidance
- Market or peer events

Developed monitoring programmes should be structured to allow effective challenge, review and maintenance.

Good Practice Statement 8: Firms should have a decision-making process in place to establish whether there is a 'reasonable suspicion' regarding an order or a transaction or a series of orders and transactions.

A suspicious transaction or order is one where there is a reasonable suspicion that such order or transaction (whether placed or executed on or outside a trading venue) could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation. If an order, transaction, trade, message or analysis of an amalgamation of certain behaviour involving these is investigated and the conduct or commercial rationale for the order or transaction is not clear or appropriate, there are a number of factors which may help to establish whether a firm is in a position of 'reasonable suspicion'.

1) One of the first steps for the alert processing staff member to consider is understanding of the behaviour and/or commercial rationale for the order or transaction. If this is not fully understood the officer should seek to discuss with internal relevant personnel as described in GPS 1.

2) Once escalated accordingly, should the commercial rationale of the behaviour still not be understood, clear or seem reasonable then it should be determined by the established relevant personnel defined by the firm, whether an investigation should be initiated or whether it is appropriate to open a case to monitor the behaviour further. This decision should be recorded and scheduled for review at an appropriate time in the future.

3) At the scheduled point for review, if further data has been collected this should be included in the investigation.

4) The investigation may take into consideration past behaviour and analyse patterns such as:

    a. Investigation of the firm undertaking the behaviour.
    b. Who the behaviour occurs with; is it commonly with a particular institution or specific trader.
    c. Does the behaviour occur around a certain time of day (e.g. the close).
    d. Is there a particular product or range of products included.
    e. In-house systems should be checked to verify outputs of surveillance system (times/dates/sequence of orders).
    f. Has the buy or sell occurred for no economic gain.
    g. If there are gains that are unusual for the particular product.

5) Consideration should be given to which type of notification may be necessary i.e. STOR and/or SAR. It may be pertinent to communicate with relevant personnel within the firm regarding activity from the perspective of AML activity.

The reporting obligation for firms and trading venues relates to orders in addition to transactions and is triggered once a reasonable suspicion of actual or attempted insider dealing or market manipulation is formed. All information and suspicion formed should be documented, explained and escalated to Senior Management / relevant personnel as set out in Good Practice Statement 1. If the behaviour cannot be reasonably justified, even if it is perhaps unintentional, should it give a misleading view to the market then this is reasonable grounds to submit a STOR.

1.6 **Post-submission actions**

Good Practice Statement 9: Firms should provide guidance to employees on required actions after a STOR is submitted. This will be dependent on the nature of communications with the regulator and the status of any consequent investigation.

The actions required by the firm and the employees involved will be dependent on the response by the regulator and the investigation status.

Guidance should include:

- Required actions to avoid tipping off. In particular, unless otherwise instructed firms should not desist or change their behaviour as a result of the suspicion. The decision to execute further transactions with the party under suspicion should be made without the suspicion being a factor in the decision-making process. If the behaviour evolves or changes, further reports should be made.
- Requirements for recording of on-going similar behaviour in new or existing cases in the event further reporting is required.
- If suspicious behaviour continues, the requirements for review by senior management to determine if actions need to be taken (e.g. change trading protocols, limits etc), however measures should be taken to avoid tipping off.
- Required actions related to the submission of relevant additional information which the firm becomes aware of after the initial report has been made.

1.7 Record Keeping

Good Practice Statement 10: Firms should deploy a relevant record keeping tool that is able to provide for the full life cycle of any suspicions. Every alert and case that is investigated or analysed should have a full audit trail which is recallable in the future.

The relevant record keeping tool should provide a full life cycle of any suspicions and can be recalled and reviewed. Every alert and case investigated and analysed in the surveillance system should have a full audit trail which is recallable in the future. This includes analysis performed on STORs which have been submitted, as well as those suspicious orders and transactions which were analysed, but in relation to which it was concluded that the grounds for suspicion were not reasonable. An example of relevant record keeping log for suspicions and notifications is included at Annex 1.

The relevant record keeping tool can provide a high-level overview. Granularity can be recalled and reviewed in the surveillance system. Firms are reminded that they should make copies of reports prior to submission as some regulators are unable to provide copies after reports are made.

Annex 1 – An example of a relevant record keeping log for suspicions and notifications

Internal Compliance Notification Report No.	Details of Event	Type of Notification	Appropriate Authority	Jurisdiction	Requires Internal Escalation	Escalated to	Internal discussion/s held (between & dates)	Notification to Authorities deemed appropriate	Rationale for decision taking	Date of Notification	Notification made by

This log should include not only submissions but also "near misses" with appropriate recording of decision makers and rationale as to why an event was considered for notification but may ultimately not have resulted in an external notification.

Annex 2 – Information for submission of STORs

Suspicious orders and transactions in the UK must be reported to the FCA via the online STOR submission portal "Connect" https://connect.fca.org.uk/firms/aupo_sitelogin. The STOR form should be completed in full and include the basis for reporting a suspicious transaction. Market participants should familiarise themselves with any equivalent systems in other jurisdictions in which they operate.

Firms and trading venues with questions about how to complete or submit a STOR can call The FCA STOR helpline on 020 7066 5577 or email storhelp@fca.org.uk.