FICC Markets Standards Board

Surveillance Core Principles for FICC Market Participants:

Statement of Good Practice for Surveillance in Foreign Exchange Markets

December 2016

Contact Details for further information:

FICC Markets Standards Board
63 St Mary Axe, London EC3A 8AA
Website: http://www.fmsb.com

Table of Contents

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 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 Statements of Good Practice (SGP) are issued by the FMSB from time to time. SGPs do not form part of the FMSB Standards and they are not binding on FMSB members; rather they reflect the FMSB's view of what constitutes good or best practice in the areas covered by the SPG in question. FMSB members are expected, and other firms are invited, to consider their own practices in light of the SGP and any amendments that may 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.

As at the date of the publication of this Statement of Good Practice, some 41 firms had become members of the FMSB. Full details of those firms are available at http://www.fmsb.com. Statements of Good Practice will be shared with Non-Member firms and their associations, who are encouraged to consider them. Information on Statements of Good Practice 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.

3. Relationship with law and regulation

FMSB Statements of Good Practice 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 Statements of Good Practice, relevant regulators will in many cases have commented on their drafting, alongside FMSB member firms and other bodies, such that the Statements of Good Practice once finalized and published are intended to represent an authoritative statement of global good practices and processes.

4. Relationship with other codes

Other codes already exist in relation to certain FICC markets, or 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 Statement of Good Practice where the subject matter is already covered adequately by existing regulation or a code issued by another body. It may, however, draw attention to Members of an existing Code and request adoption, once appropriate steps have been taken to confirm its applicability.

5. Periodic review

The FMSB plans periodically to review its published Statements of Good Practice and any other materials it produces to ensure that they continue to be relevant and appropriate for the markets and products to which they apply.

II. Preface

1. Background

The Fair and Effective Markets Review ("FEMR") was launched by the Chancellor of the Exchequer and the Governor of the Bank of England in June 2014 to reinforce confidence in the wholesale FICC markets in the wake of the serious misconduct seen in recent years; and to influence the international debate on trading practices. The FEMR Final Report published on 10 June 2015 set out a number of areas where firms needed to improve, which specifically included '…substantial further development of firms' misconduct surveillance is required to deliver fully effective oversight of FICC markets…'.

This paper has been developed by member firms of the FMSB to:

- Set out core principles for surveillance for all FICC markets;
- Set out Statements of Good Practice for surveillance of foreign exchange markets;
- Highlight areas of emerging practices for surveillance for the industry to be cognisant of in the future; and
- Make available this information to the industry.

2. Scope and applicability

Surveillance, for the purposes of this document, is defined as post-trade surveillance tools used to detect potential instances of insider dealing, market manipulation and other transaction based conduct risks[1]. The sophistication of each individual firm's trade, electronic communication (eCommunications) or voice communication surveillance will depend upon the size and scale of each individual firm. The information contained in this document should be used as guidance for firms when reviewing the extent, comprehensiveness and capabilities of their own surveillance.

The scope of surveillance, for the purposes of this document, is limited to insider dealing and market manipulation (as defined in the EU Market Abuse Regulation) and other transaction based conduct risks in foreign exchange markets. The information contained within this document can be applied by buy-side firms, sell-side firms, venues and other intermediaries operating in, or executing transactions related to, foreign exchange markets.

Notwithstanding that the information contained herein is specific to foreign exchange markets, firms should read across surveillance good practices to other asset classes or products that those firms have an exposure to. The 'Core Principles' set out in Section IV are considered by FMSB member firms to have an industry wide application, and are therefore not limited to a particular asset class or product.

[1] For the purposes of this paper, 'other transaction based conduct risks' are limited to abnormal trading; churning; transaction window rates; partial fills; unsupported 'last look' practices; indefensible mark-ups; coordinated trading; and upholding your axe. These risks were either raised by FMSB members as specific risks that are (or are planned to be) partially mitigated through the use of automated surveillance, or risks that were raised by the FCA ('FCA Specified Risks') in their letters to firms on their mandated 'FX Remediation Programme'

3. Definitions

Buy-Side – (*'Glossary and Acronyms', FEMR Final Report*[2]) Financial institutions holding and dealing in financial instruments for investment or asset management purposes. Examples include mutual funds, pension funds and insurance funds.

Electronic communications surveillance – (*Defined by FMSB Surveillance Working Group*) Monitoring, analysis and escalation (as required) of electronic communication including the use of emails, internal and external messaging services. Electronic communication is frequently operated on an alert basis through specified lexicons and dialogue patterns.

First/Second/Third Lines of Defence – (*'Glossary and Acronyms', FEMR Final Report*) The lines of defence are the governance and controls to protect against risks in an organisation. The First Line of Defence is risk mitigation and control within the business function that generates the risk, in particular through policies and procedures, training and line management oversight. The Second Line of Defence is an independent oversight function – commonly the risk functions monitoring each key risk category. The Third Line of Defence is an independent assurance function – the internal audit function.

Foreign Exchange market participants – (*Defined by FMSB Surveillance Working Group*) Buy-Side, Sell-Side and Venues trading and providing liquidity and operating trading venues for FX.

Market Abuse – (*Market Abuse Regulation (7)*)[3] This is a concept that encompasses unlawful behaviour in the financial markets… it should be understood to consist of insider dealing, unlawful disclosure of inside information and market manipulation.[4]

Misconduct – For the purposes of this document, 'Misconduct' refers to non-market abuse concerns as set out in Appendix 1 'Inventory of Risks'.

Sell-Side – (*'Glossary and Acronyms', FEMR Final Report*) Financial institutions (predominantly banks, broker-dealers and interdealer brokers) involved with the creation, promotion, analysis and sale of securities and other financial instruments.

Surveillance - (*Defined by FMSB Surveillance Working Group*) The systematic monitoring and analysis of trade activity ("Trade surveillance") and communications ("Voice surveillance" and "Electronic communications surveillance").

Trade Life-cycle – (*Defined by FMSB Surveillance Working Group*) An approximation of the processes and acts which cover the life-cycle of a trade from origination to settlement. For the purposes of this document the Trade Life-cycle has been specified as three distinct stages: Order Flow and management, Trade execution and Post trade monitoring.

Trade surveillance – (*Defined by FMSB Surveillance Working Group*) Monitoring, analysis and escalation (as required) of trading activity and patterns across the trade life-cycle. Trade surveillance is frequently operated on an alert basis through specified algorithms.

Venues – *(Page 23, figure 1 of FEMR Final Report)* Include Voice Broking and the activities and associated risks in respect of operating: All-to-all platforms, Multi-dealer platforms and Single-dealer platforms; Electronic Communication Network ("ECN"); Exchanges,

---

[2] Fair and Effective Markets Review, Final Report, June 2015.

[3] Market Abuse Regulation (EU No 596/2014).

[4] This document further categorises Market Manipulation as: Distorting Market Price, Disrupting Market Participants and Predatory Tactics. These categories are not included within the Market Abuse Regulation. A Glossary has been prepared that includes a list of the Market Abuse behaviours identified (together with the corresponding source document indicating their provenance). A Market Abuse behaviour is an act or conduct which is, or has the potential to be, an offence under the Market Abuse Regulation.

Multilateral trading facilities/venues/systems, Electronic Trading Platforms and Organized Trading Facilities/Dark Pools (as applicable) where services is provided for FX trading.

Voice surveillance – (*Defined by FMSB Surveillance Working Group*) Retrospective monitoring, analysis and escalation (as required) of all business voice communications on firm devices.

4. Qualifications

This document outlines Statements of Good Practices for surveillance of foreign exchange markets at the time of publication.

Statements of Good Practices contained within this document do not include aspirational surveillance practices, including those enabled by Financial Technology ("FinTech"), that are not considered to be established and operating as effective surveillance by firms at the time of publication. Statements of Good Practice contained within this document are also not intended to provide direction on the use of technology and / or the appropriate target operating models for each firm.

Each individual firm should undertake their own risk assessment to understand their inherent risk of insider dealing, market manipulation and other transaction based conduct manifesting in foreign exchange markets given the nature of their business. Firms may then consult the Statements of Good Practice herein to support them in determining the sophistication, nature, extent and timing of surveillance that they would undertake to sufficiently mitigate the risk of insider dealing, market manipulation and other transaction based conduct risks going undetected.

III. Process to agree Statements of Good Practice

Firms operate systems and controls across their business to identify and manage risk, including the risks of insider dealing, market manipulation and other transaction based conduct risks. Surveillance is one mechanism, but not the only mechanism, by which firms can detect potential instances of insider dealing, market manipulation or other transaction based conduct risks in foreign exchange markets.

Firms may wish to determine how surveillance across foreign exchange markets that they contribute to, in an active or passive capacity, can be effective as part of a robust set of systems and controls that sufficiently mitigates the risks of insider dealing, market manipulation or other transaction based conduct risks to an acceptable level.

Establishing core principles for surveillance

In advance of determining Statements of Good Practice for surveillance in foreign exchange markets, FMSB member firms established 10 Core Principles for surveillance. These are a set of fundamental principles that firms may consider in advance of designing and implementing their surveillance capabilities. The Core Principles have been set at an industry wide level and are considered by FMSB member firms to apply to surveillance holistically, and not limited to a particular asset class or product.

Risk identification

FMSB member firms constructed a lifecycle of a foreign exchange trade (Appendix 2) in order to identify relevant insider dealing and market manipulation risks that could manifest in foreign exchange markets. This formed the basis of the inventory of risks set out in Appendix 1.

The inventory of risks set out in Appendix 1 also includes nine ‘other transaction based conduct risks’ (away from insider dealing or market manipulation) that regulators have identified, or members of the FMSB have self-identified, as conduct risks pertaining to foreign exchange businesses that firms should manage.

The inventory of risks is not intended to be a comprehensive set of insider dealing, market manipulation and other transaction based conduct risks for those enacting foreign exchange businesses, or businesses related to foreign exchange, over which to provide surveillance. The inventory of risks comprises a set of insider dealing, market manipulation and other transaction based conduct risks that members of the FMSB have identified as those that could potentially manifest in foreign exchange markets. These risks have been considered in the context of buy-side, sell-side and venues market participants. Whilst some of these risks may not be applicable to all of these three market participants, to the extent that they are applicable, the relevant good practice surveillance solutions have been presented in this report.

Consumers of this paper may use the lifecycle of a foreign exchange trade and the inventory of risks to support and inform their own insider dealing, market manipulation and other transactional conduct risk assessment.

Defining and agreeing Statements of Good Practice

Members of the FMSB reflected upon each of the insider dealing, market manipulation and other transaction based surveillance risks relevant to foreign exchange markets and set out to define and agree Statements of Good Practice for surveillance in foreign exchange markets.

Statements of Good Practice for surveillance in foreign exchange markets have been agreed by members of the FMSB, individually and collectively. The Statements of Good Practice represent surveillance practices currently undertaken by one or more market participants where members of the FMSB agreed that those practices provided effective surveillance to sufficiently mitigate a specific (or combination of) insider dealing, market manipulation or other transaction based conduct risks set out in Appendix 1.

Statements of Good Practice are set out in the Appendices to this document. Consumers of this paper may wish to use the Statements of Good Practice for surveillance in foreign exchange markets to:

- Benchmark their own surveillance capabilities and coverage to industry good practice;
- Adopt good practices, at a minimum, to align with industry good practice; or
- Review good practices in foreign exchange markets and use this to support read across exercises to other asset classes or products.

Emerging practices

Firms' ability to perform effective surveillance is continually evolving and developing as a result of clearer surveillance operating models, better quality of internal data and more mature technology. Emerging areas of consideration that may enable better surveillance and emerging risks where surveillance could act as an effective control are set out in Section VI of this paper.

Consumers of this paper may wish to use the information contained in Section VI to support the development of their own plans on where and how they can perform effective surveillance in the future.

This paper specifies a set of Core Principles for consideration by all market participants. The guidance includes a defined population of insider dealing, market manipulation and other transaction based conduct risks relevant to foreign exchange markets that could be mitigated through the use of effective surveillance practices. Statements of Good Practice for surveillance in foreign exchange markets are set out the Appendices and demonstrate where market participants are currently able to perform effective surveillance.

IV. Surveillance Core Principles for all FICC markets

1. Overview of Surveillance

Industry leading practice is to deploy effective automated surveillance to form part of a robust systems and controls landscape.

Surveillance, for the purposes of this document, is defined as post-trade surveillance solutions used to detect potential instances of insider dealing, market manipulation and other transaction based conduct risks in foreign exchange markets. **The design and sophistication of each individual firm's trade, electronic communication (eCommunications) or voice communication surveillance will depend upon the size, scale and complexity of each individual firm and its function in the market.** The information contained in this document should be used as guidance for firms when reviewing the extent, comprehensiveness and capabilities of their own surveillance.

Set out below are a set of core principles for surveillance that firms may wish to adopt in order to identify, determine and establish an effective surveillance function, which includes, but is not limited to:

- Preserving independence from front office to allow a surveillance function to be effective;
- An effective surveillance operating model (including how responsibilities and interactions occur between the first and second lines of defence);
- An understanding of where surveillance can be used as an effective control and would strengthen the overall control environment;
- A determination of where automated surveillance would provide a more comprehensive and effective control than manual surveillance; and
- An appreciation that an effective surveillance function will differ depending on the nature, extent and sophistication of the business conducted by each market participant.

The Core Principles have been set at an industry wide level, are considered by FMSB member firms to apply to surveillance holistically, and not limited to a particular asset class or product.

2. Core Principles

Core Principle 1: *Firms must undertake a risk assessment on an ongoing basis to understand the inherent risk of insider dealing, market manipulation and other transaction based conduct risks manifesting given the nature of their business. The risk assessment should be tailored to consider each insider dealing, market manipulation or other transaction based conduct risks in the context of the specific asset classes or products that the firm has an exposure to.*

In identifying insider dealing, market manipulation or other transaction based conduct risks, firms should consider their:

- Clients and counterparties, traders, fund managers and markets (including the motives and incentives of each party)
- Trading role and strategy (active, passive, hedging, market making and so on)

The specific asset classes and products they have an exposure to (size, scale and complexity)

Core Principle 2: *Surveillance is one mechanism of mitigating the risk of insider dealing, market manipulation and other transaction based conduct risks. Firms should consider the output of their risk assessment when determining the cases by which surveillance could be deployed as an effective control. As a minimum expectation, firms operating in FICC markets should consider whether the inventory of risks set out in Appendix 1 is relevant and material to their firm, and whether surveillance could act as an effective control in each case.*

Core Principle 3: *Firms need to establish governance and oversight over their surveillance which:*

- *Establishes a set of resources to performing surveillance activities;*
- *Ensures that surveillance is only performed where legally permitted and subject to relevant local regulations;*
- *Ensures that surveillance alerts are appropriately escalated, investigated and reported (as necessary) including investigation units and regulatory reporting (e.g. STOR reports);*
- *Manages the risk of conflicts of interest in the surveillance operating model;*
- *Continually assesses whether the extent of surveillance is adequate given the nature of the firm's business (e.g. electronic or manual trading); and*

Provides appropriate training to staff operating surveillance and staff within the front office in respect of their role supervising, monitoring and escalating potentially suspicious activity.

Core Principle 4: *Automated post-transaction surveillance for insider dealing, market manipulation or other transaction based conduct risks should be performed by a function independent of the front office. The design of the surveillance framework takes input from the front office on the risks that could manifest in the trading environment, however the independent function assesses those risks identified by the front office and determines the nature and extent of post-transaction surveillance that is required to be performed to mitigate the risk of insider dealing, market manipulation or other transaction based conduct risks going undetected.*

Core Principle 5: *Firms should determine how (trade surveillance, electronic communications surveillance or voice surveillance) and when to employ surveillance across the spectrum of insider dealing, market manipulation or other transaction based conduct risks relevant to their business, such that surveillance acts as a meaningful and effective control. Surveillance for a particular product should cover all front office and any other relevant staff that deal in or support the specific product as appropriate. The inclusion of individuals, and the extent of surveillance conducted thereon, should follow a documented risk based approach.*

Core Principle 6: *The First Line of Defence should supervise front office staff and monitor client activity as part of BAU. In doing so, the First Line of Defence performs an important role in identifying and escalating potentially suspicious activity indicative of insider dealing, market manipulation and other transaction based conduct risks.*

Core Principle 7: *Quality Assurance. Firms should regularly review and evaluate the effectiveness of their surveillance function to ensure that surveillance is fit for purpose, which includes, but is not limited to:*

- *Revisiting thresholds for surveillance scenarios and assuring that they are appropriately calibrated;*
- *Reviewing the methodology for alert closure and escalation;*
- *Reviewing the timeliness of surveillance alert review and closure;*
- *Independently testing that alerts have been closed appropriately;*
- *Reviewing the ratio of surveillance alerts to STORs; and*

Independently testing that documentation has been appropriately retained to evidence closure or escalation.

Core Principle 8: *Trade, electronic and voice communications records and data (including alerts) must be retained. Complete and accurate data is fundamental to support effective surveillance; as such, firms must obtain assurance over the completeness and accuracy of the data; both at design and on an ongoing basis. Additionally, algorithms designed to generate automated surveillance alerts should be documented and subjected to independent design and effectiveness reviews on a periodic basis. The documentation of each alert should be dispositioned to the extent that it could be independently reviewed and audited by a third party.*

Core Principle 9: *Firms should conduct ongoing horizon scanning that monitors for market incidents or developments to inform their risk assessment and enhance their surveillance capabilities (as necessary).*

Core Principle 10: *On an on-going basis, firms should review the combined outputs of their different surveillance activities to identify trends and abnormal behaviour, considering relevant market data (where possible).*

V. Statements of Good Practice for FX markets

This section of the paper explicitly sets out Statements of Good Practice for surveillance in FX markets ('Surveillance Good Practices'). Surveillance Good Practices are limited to the most effective surveillance practices currently undertaken by market participants for the risks of insider trading, market manipulation and other transaction based conduct risks.

Surveillance Good Practices encompass the set of core principles for surveillance set out in Section IV of this paper. There is a direct correlation between Core Principles 1, 2, 4, 5 and 8 and the Surveillance Good Practices set out below.

1. Sell-Side firms:

The insider dealing, market manipulation and other transaction based conduct risks to which Sell-side firms are exposed are an outcome of several factors including:

- Access to client information and client discussions as liquidity provider;
- Discretion or role in pricing, interest (request for quotes and expressions of interest) and order handling and execution;
- Role in setting prices during fixing windows;
- Ability to execute on both sides of a transaction;
- Trading volumes; where traditionally sell-side firms have generated the largest trading volumes;
- Ability to transact with a wide range of market participants via voice and electronically (direct Buy-side firms, in electronic venues, with brokers); and
- Information within the organisation (for example within order books and independent research functions (where applicable)).

The table below provides an overview of the Surveillance Good Practices that we have identified as providing the most effective surveillance which can currently be enabled in relation to the risks of insider dealing, market manipulation and other transaction based conduct risks that members of the FMSB have identified as those that could potentially manifest in foreign exchange markets.

The following table should be read alongside Appendix 3, which further defines specific situations where the good practices apply.

Key			
Symbol	Trade	eCommunications	Voice
●	Automated surveillance detection logic	Specific lexicon in place	Automated solution
◐	Human analysis	General lexicon in place	Manual solution
○	No automated or manual surveillance deployed at present	No automated or manual surveillance deployed at present	No automated or manual surveillance deployed at present
-	Not applicable to the risk	Not applicable to the risk	Not applicable to the risk

Risk	Surveillance Channel		
	Trade	**eCommunications**	**Voice**
Insider dealing			
Insider dealing using Material Non-Public Information (“MNPI”)	○	○	○
Personal Account Dealing	●	○	-
Recommending or including others to engage in insider dealing	○	●	○
Front running/pre-positioning	●	○	○
Unlawful disclosure of Insider Information			
Improper disclosure (covering inappropriate sharing of information between fund managers and dealers; to brokers and intermediaries; or internally)	-	●	○
Market Manipulation			
Attempts to manipulate fixes; Marking a reference price (which is derived from a transaction window)	●	●	◐
Artificially increasing/price; Artificially stabilising price; Triggering [client] stop loss orders or barrier options (or other optional redemptions or related derivatives); Banging the a reference price (other than that derived from a transaction window)	●	-	-
Layering & Spoofing	●	-	-
Creating/enhancing arbitrage possibilities between a financial instrument and another related financial instrument	●	-	-
Cross market/venue manipulation/internal cross trades	○	-	-
Ramping indicative pricing (published bid/offer spreads)	●	●	-
Wash trades/Improper Matched Orders	●	○	○
Dominant trading/cornering the market/abusive squeeze	●	-	-
Dissemination of false rumours	-	●	○
Use of non-specific trade information flow to manipulate the market (e.g. buy-side regular FX patterns)	○	○	○
Recommending or inducing others to engage in market manipulation	-	●	○

Other transaction based conduct risks			
Abnormal trading	●	○	○
Transaction window rates	○	○	○
Partial fills	○	○	○
Unsupported ‘Last Look’ practices	◐	◐	◐
Indefensible mark-ups	●	○	○
Coordinated trading	○	●	○

The table above provides examples of where firms have found deploying automated and manual solutions particularly effective; it is not a minimum standard, firms must continue to exercise judgement and consider the full range of potential Surveillance methods, tools and ideas at their disposal.

2. Buy-Side firms:

Overview of Surveillance

The buy-side risk profile for insider dealing, market manipulation and other transaction based conduct risks manifesting in foreign exchange markets is limited due to low relative volumes of activity undertaken by the buy-side within a highly liquid market.

Foreign exchange products traded by buy-side firms are often a by-product of other investments and have a functional role to protect the value of funds rather than an outright exposure for alpha generating purposes. As such, they are predominantly used for hedging and currency overlay and, in such cases, the incentive to manipulate the market is limited. Specific trade surveillance is applied by buy-side firms to portfolios conducting alpha-generating trading within foreign exchange.

While foreign exchange trading volumes of buy-side firms are comparatively lower than sell-side firms, the larger buy-side firms may generate volume which creates opportunities for firms to benefit from currency price movements. In conjunction with this, other market events, such as international cross currency mergers and acquisitions may also create opportunities to use inside information to benefit from rate movements, if the deal itself creates the need for a large exchange of currencies at payment date. As such, firms need to remain mindful when designing their surveillance programmes that situations not normally associated with foreign exchange business may still have an impact.

The table below provides an overview of the Surveillance Good Practices that firms view as providing the most effective surveillance which can currently be enabled in relation to the risks of insider dealing, market manipulation and other transaction based conduct risks that members of the FMSB have identified as those that could potentially manifest in foreign exchange markets. Firms should apply surveillance against those risks identified as both relevant and material to their firm, where surveillance can be deployed as an effective control. The design of buy-side firms' surveillance programmes acknowledge that the potential for these risks to manifest in foreign exchange is less than in Equities and Fixed Income asset classes.

Corporate institutions with trading desks (outside of a treasury function) actively trading FX and other products need to determine, through an assessment of their operations within the Risk Assessment, which of the risks and good practices set out below for the Financial Sector apply to them.

The following table should be read alongside Appendix 4, which further defines specific situations where the good practices apply.

Key			
Symbol	Trade	eCommunications	Voice
●	Automated surveillance detection logic	Specific lexicon in place	Automated solution
◐	Human analysis	General lexicon in place	Manual solution
○	No automated or manual surveillance deployed at present	No automated or manual surveillance deployed at present	No automated or manual surveillance deployed at present
-	Not applicable to the risk	Not applicable to the risk	Not applicable to the risk

Risk	Surveillance Channel		
	Trade	eCommunications	Voice
Insider dealing			
Insider dealing using Material Non-Public Information (“MNPI”)	●	●	○
Personal Account Dealing	●	●	○
Recommending or including others to engage in insider dealing	●	●	○
Front running/pre-positioning	●	●	○
Unlawful disclosure of Insider Information			
Improper disclosure (covering inappropriate sharing of information between fund managers and dealers; to brokers and intermediaries; or internally)	-	●	○
Market Manipulation			
Quote stuffing	●	-	-
Wash trades/Improper Matched Orders	●	●	-
Market Manipulation risks with heightened application to buy-side firms employing algorithmic or high frequency trading strategies			
Cross market/venue manipulation	○	●	○
Layering & Spoofing	●	-	-
Other transaction based conduct risks			
Coordinated trading	○	●	○
Portfolio Allocation	●	-	-
Cross Trades	●	-	-

The table above provides examples of where firms have found deploying automated and manual solutions particularly effective; it is not a minimum standard, firms must continue to exercise judgement and consider the full range of potential Surveillance methods, tools and ideas at their disposal.

3. Venues:

As market facilitators, venues have a view of activities conducted by sell-side and buy-side market participants, including line of sight of RFQs, orders, transactions; and who trades with whom. Venues surveillance can also extend to cover price commitments and indicative pricing to assess market participants' behaviours.

In establishing and maintaining their platforms venues establish pre-trade and order controls, venue rules and otherwise design their platforms with the objective of minimising, and in some cases eliminating, the risk of insider dealing and market manipulation. Following a risk based approach the extent and focus of venue's surveillance models focus on the resultant residual risk.

The availability of information supports venues in performing surveillance at an aggregated level, where venues can profile market participants by reviewing their market activity and their trading relationships with each other. Venues can use this information to derive expected behavioural 'norms' and detect deviations from the norm ('unusual behaviour'). Like other market participants, venues conduct risk assessments of their business activities, and the parameters in which they operate, in order to determine which risks are relevant to them.

Venues' view of the market is predicated on the access to data that they are privy to. While venues do not necessarily have access to the pre-trade cycle decision making process, or written or voice communication data,[5] they do have the ability to provide surveillance across institutions that have traded on their venue. They bring a broader surveillance perspective to the industry and could identify market wide issues before individual firms due to their access to data.

Venues' surveillance typically covers transactions, orders, Request for Quotes (RFQs), price commitments and indicative pricing to assess market participants' behaviours. Venues use surveillance to identify usual behaviour and support their obligations to identify and report:

- significant breaches of their rules;
- disorderly trading conditions; and
- conduct that may involve market abuse.[6]

The table below provides an overview of the Surveillance Good Practices that we have identified as providing the most effective surveillance which can currently be enabled in relation to the risks of insider dealing and market manipulation that members of the FMSB have identified as those that could potentially manifest in foreign exchange markets.

The following table should be read alongside Appendix 5, which further defines specific situations where the good practices apply.

[5] eCommunication and voice surveillance channels are applicable to Voice Brokers only. The eCommunication and voice surveillance channels do not apply to venues whose staff do not take or receive orders through voice or electronic communications channels from venue participants.

[6] FCA MAR 5.6.1(1)R - Reporting requirements applicable to MTFs.

Key			
Symbol	Trade	eCommunications	Voice
●	Automated surveillance detection logic	Specific lexicon in place	Automated solution
◐	Human analysis	General lexicon in place	Manual solution
○	No automated or manual surveillance deployed at present	No automated or manual surveillance deployed at present	No automated or manual surveillance deployed at present
-	Not applicable to the risk	Not applicable to the risk	Not applicable to the risk

Risk	Surveillance Channel		
	Trade	eCommunications *	Voice
Insider dealing			
Insider dealing using Material Non-Public Information ("MNPI") **	●	○	○
Recommending or including others to engage in insider dealing **	○	●	●
Front running/pre-positioning	◐	○	○
Unlawful disclosure of Insider Information			
Improper disclosure (covering inappropriate sharing of information between fund managers and dealers; to brokers and intermediaries; or internally)	-	●	●
Market Manipulation			
Attempts to manipulate fixes; Marking a reference price (which is derived from a transaction window)	●	○	○
Layering & Spoofing (& Spivving)	●	-	-
Artificially increasing the price	●	-	-
Artificially stabilising the price	●	-	-
Cross market/venue manipulation	○	-	-
Ramping indicative pricing (published bid/offer spreads)	●	-	-
Parking	◐	-	-

Risk	Surveillance Channel		
	Trade	eCommunications *	Voice
Quote stuffing	●	-	-
Dissemination of false rumours	-	●	●
Wash trades/ Improper Matched Orders	●	●	●
Trade information leakage	-	●	●
Dominant trading/ cornering the market / abusive squeeze	●	-	-
Use of non-specific trade information flow to manipulate the market (e.g. buy-side regular FX patterns)	-	●	●
Other transaction based conduct risks			
Unsupported 'Last Look' practices	◐	○	○
Coordinated/ concurrent trading	●	○	○
Abnormal trading	●	-	-

*eCommunication and voice surveillance channels are applicable to Voice Brokers only. The eCommunication and voice surveillance channels do not apply to venues whose staff do not take or receive orders through voice or electronic communications channels from venue participants.

**'Insider dealing' and 'Recommending or including others to engage in insider dealing' risks do not apply to those venues whose staff do not communicate with front office staff of venue participants.

The table above provides examples of where firms have found deploying automated and manual solutions particularly effective; it is not a minimum standard, firms must continue to exercise judgement and consider the full range of potential Surveillance methods, tools and ideas at their disposal.

VI. Emerging Practices

Members of the FMSB consider that surveillance for insider dealing, market manipulation and other transaction based conduct risks is an evolving area, where:

- New risks continue to emerge that require a level of surveillance to mitigate those risks to an acceptable level; and
- Surveillance technology capabilities are evolving that may provide better quality surveillance in the future.

A list of emerging industry practices are set out below; this is not an exhaustive list. Consumers of this paper may wish to use the information contained in this section to support the development of their own plans on where and how they can perform effective surveillance in the future.

1. Emerging risk: the use of personal mobile devices

The scope of a firm's e-communications and voice surveillance capabilities is currently limited to surveilling devices owned by the firm and issued to members of staff and other parties contracted to work with the firm. Many market participants are concerned that the risk of insider dealing, market manipulation and other transaction based conduct risks could be facilitated or undertaken through devices not issued by the firm, such as personal mobile phones.

In addition, the proliferation of social media and mobile application (Apps) channels used for instant communication exacerbates the risk of confidential information being inappropriately shared outside of recorded channels.

In order to mitigate this risk, many market participants have:

- Mandated, through policy, the use of only firm issued devices for conducting business on behalf of the firm;
- Prohibited the use of personal mobile devices on the trading floor and in other risk generating areas as a preventative control; and
- Prohibited access on firm infrastructure to any Social Media (and equivalent websites or electronic communication channels) that cannot be effectively recorded and surveilled.

At this time, for the majority of market participants, surveillance does not extend to systematically searching messages on publically available social media channels as an input to each market participants' suite of surveillance capabilities.

2. Emerging technology: voice communication surveillance

Voice surveillance technology is in its infancy and, for many firms, the technology is not mature enough to be an effective primary surveillance capability. Voice surveillance technology principally adopts one of the two approaches set out below:

- 'Phonetic Searching', which searches for words based upon their sound or pronunciation; or
- 'Voice to Text Transcription', which converts spoken words into written text that can subsequently be searched.

A number of market participants and regulators are undertaking proof of concepts with voice surveillance vendors, and a minority of firms have purchased automated voice surveillance solutions that now form part of their overall surveillance capabilities.

Member firms of the FMSB expect technology in this area to improve and for voice surveillance to move from manual review (current market practice) to automated, electronic surveillance in the future. This will provide for greater coverage of surveillance of voice communications and should strengthen firms' overall surveillance control environments.

3. Emerging technology: natural language processing techniques

Natural Language Processing (NLP) techniques allow computers to understand human language and, through the use of a sophisticated set of algorithms, can enable computers to identify sentiment and context (amongst other things) within written text. NLP techniques are designed to form associations between disparate data sets in unstructured (communications) data and, as a result, may allow for early detection of issues before they come to fruition.

NLP techniques have been used effectively in other industries, but are relatively new to the financial services sector. A number of market participants are conducting proof of concepts with vendors that can perform NLP techniques across written electronic communications data; with a view to reducing the rate of false positive alerts and identifying more subtle indicators of potential insider dealing, market manipulation and other transaction based conduct risks.

4. Emerging technology: ambition to achieve holistic surveillance

Many firms are working towards achieving holistic surveillance, bringing together trade, written communications data, voice communications data and other relevant data points to build an overall picture of the firm's activity. The ambition is to use holistic surveillance to:

- Identify and detect potential instances of insider dealing, market manipulation, other transaction based conduct risks and general misconduct; and
- Look forward to proactively mine for potential risks, identify them and address them before they manifest as major issues for the firm.
- Firms are seeking to achieve holistic surveillance through the use of technology, such as:
  - Joining the dots by running sophisticated algorithms in data analytics engines that sits over the top of individual surveillance alerts; or
  - Purchasing newer technology that enables firms to bring data together in a single view (e.g. trade, written communications and voice communications data).

5. Emerging capability: cross market and cross venue manipulation

Firms wish to operate automated trade surveillance to identify any firm activity that has been intentionally conducted across markets or across venues with the aim to manipulate the market. Many firms expect that the increased transparency brought by MiFID II will improve each firms' ability to provide effective automated surveillance across multiple markets and venues.

6. Emerging capability: surveilling for suspicious quotes or expressions of interest

A number of firms are in the process of implementing internal standards to systematically record Request for Quotes (RFQs) and expressions of interest. For example, firms have mandated that traders record RFQs on trade blotters, enabling the RFQ to subsequently be manually uploaded to a firm's internal systems. The timely recording of RFQs and expressions of interest will enable both more advanced surveillance of potentially suspicious quotes or expressions of interest and also timelier reporting of suspicions to third parties.

7. Emerging capability: surveilling for churing and 'upholding your axe'

Some venues are considering creating reviews to identify outlier of dealers that do not uphold their stated intentions. Thematic assessments over a longer duration could be conducted to establish consistent behavioural patterns. For churning, automated trade surveillance will be instated to identify situations where several small trades executed by one participant net to zero.

8. Emerging practice: near-shoring, off-shoring and outsourcing surveillance

A number of larger sell-side firms have begun or completed the process of near-shoring, off-shoring or outsourcing parts of their surveillance activities to other group entities or external service providers. Typically, the activity that has been passed on to another group entity or external service provider is the initial review of alerts arising from searching for a lexicon (a series of words or phrases) across written electronic communications for any given day. The level of initial alerts arising from this process tend to be high due to the large volume of written communications originated from individuals working for their respective firms.

Where firms have undertaken arrangements to relocate part of its surveillance function internally or to an external party, they have constructed clear and specific Service Level Agreements and Business Requirement Documents to govern the out-sourcing or co-sourcing of their surveillance activities; including where surveillance is to another group entity.

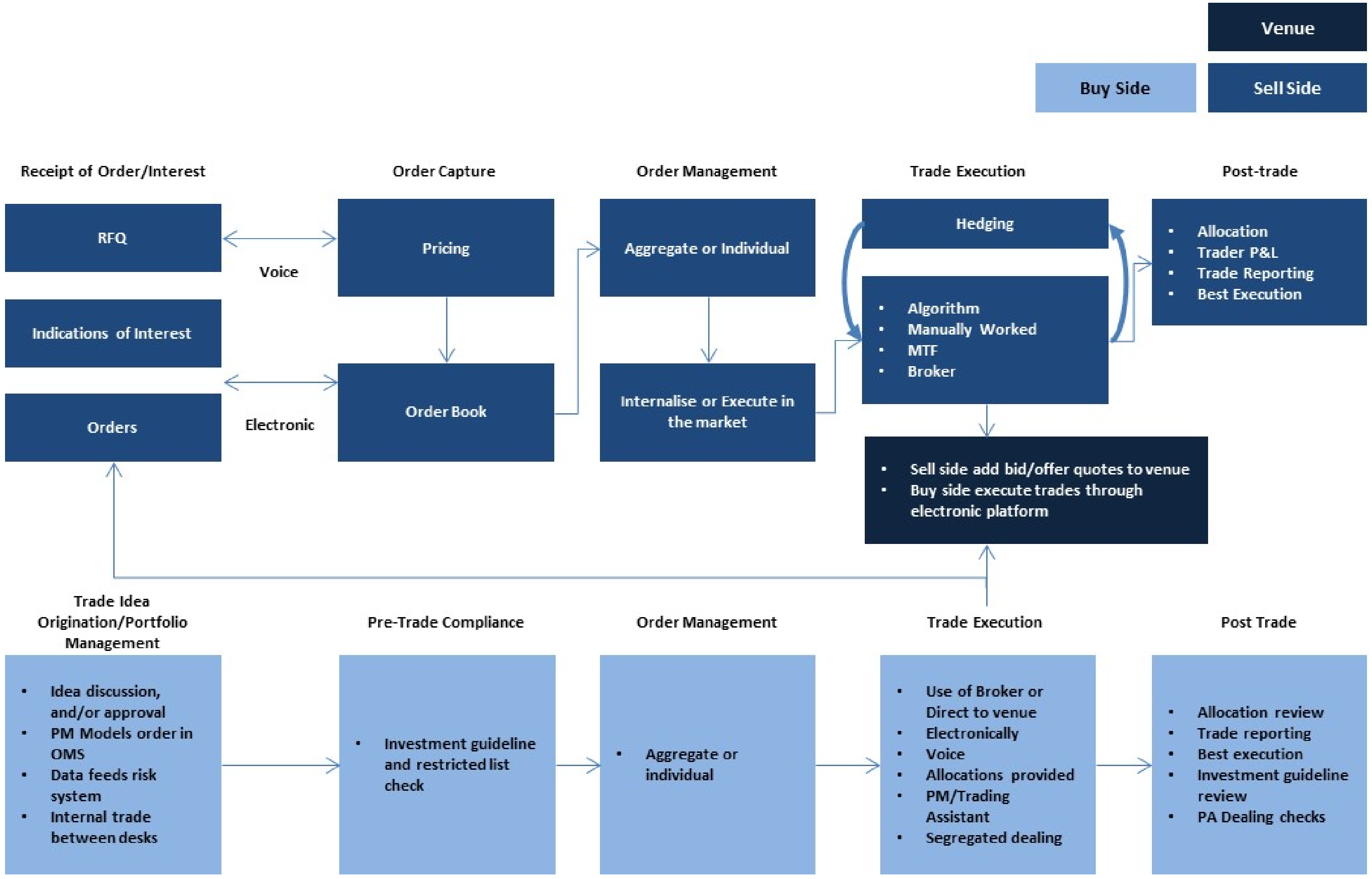
Firms put in place clear process documentation such that the operation, analysis and escalation of surveillance alerts is robust, repeatable and evidenced. Some firms employ case management tools to record their monitoring activities, investigative work and potential (and actual) referrals. These tools support the production of Management Information and overall oversight that the firm has over other group entities or third parties.

I. Appendix

1. Index of Risks

<table>
<tr><th>Insider dealer</th><th>Unlawful disclosure of insider information</th><th colspan="2">Market manipulation (*Assigned sub-category headings)</th><th>Other Transaction Based Conduct Risks</th></tr>
<tr>
<td>Insider dealing using MNPI
Personal Account Dealing)
Recommending or inducing others to engage in insider dealing
Front running/pre-positioning</td>
<td>Inappropriate sharing of information between fund managers and dealers
Inappropriate sharing of information with brokers and intermediaries
Inappropriate sharing of information internally</td>
<td>Distorting market price
Banging the close/marking a reference price
Layering & Spoofing
Artificially increasing/stabilising price
Cross venue manipulation (same product)
Ramping indicative pricing (published bid/offer spreads)
Parking
Benchmark Manipulation/Attempts to manipulate fixes
Disrupting market participants
Dissemination of false rumours
Quote stuffing
Wash trades/Improper Matched Orders
Trade information leakage</td>
<td>‘Predatory’ tactics*
Dominant trading/cornering the market/abusive squeeze
Triggering [client] stop loss orders or barrier options (or other optional redemptions or related derivatives)
Creating/enhancing arbitrage possibilities between a financial instrument and another related financial instrument
Use of non-specific trade information flow to manipulate the market (e.g. buy-side regular FX patterns)</td>
<td>FCA Specified Risks
Indefensible mark-ups
Unsupported ‘last look’ practices
Transaction window rates
Coordinating trading (including Recommending or inducing others to engage in market manipulation)
Partial fills
Personal dealing accounts
Other observed behaviours
Abnormal trading (e.g. Quote to trade ratios)
Employee profiling versus market activity
Upholding your axe
Churning
Portfolio Allocation
Cross-trades</td>
</tr>
</table>

2. Illustrative trade life-cycle for a foreign exchange trade



3. Good Practices for FX markets: Sell-Side

Risk	Statements of Good Practice
Insider dealing using MNPI and Personal Account Dealing	**Trade Surveillance** structured with respect to two types of information: • Macro (e.g. Monetary Policy Decisions). • Price sensitive trading Information – e.g. firms wall cross traders who are required to execute FX transactions related to deals. • A risk based approach is adopted and targeted surveillance performed against specific instances, for example, Monetary Policy announcements or significant spikes in trade volumes/market price (independent or in advance of market data). • Firm, client and Personal Account Dealings in scope. • Determination of a 'normalised data' and surveillance parameters set to identify abnormal behaviour. Trade surveillance of Personal Account Dealing is only possible to the extent that staff PA trade using firm processes and systems. **eCommunications** • eCommunications surveillance is performed across electronic communications of sales and trading staff in foreign exchange markets. • The lexicon used is informed by the nature of information likely to be held within the firm - covering words or phrases that may be indicative of inside information. • Lexicons are refined with additional words or phrases that could be indicative of inside information, especially when there has been a market incident. **Voice** • Voice surveillance is performed on a manual basis, if there is an indication of potentially suspicious activity in relation to insider information.
Recommending or including others to engage in insider dealing	This risk is addressed by the same practices outlined above for the risk of insider dealing using MNPI. In addition, firms use workshops with the Business to inform components of the lexicon to ensure that it is appropriately tailored to capture suspicious activity. Specific e-communication lexicons are used by some firms. It is important that the Business subject to surveillance does not have knowledge or control of the design of surveillance tools enabling them to know precisely how to avoid them.

Risk	Statements of Good Practice
Front running/pre-positioning	Firms operate product specific **trade surveillance** on front running in relation to foreign exchange trading: • Specific trade surveillance is applied to fixing windows where the firm is an active or passive participant; • Targeted trade surveillance around large/material client orders; • Running of automated trade surveillance algorithms which identify correlation/'tailgating' between client orders and activity on firm, client and Personal Dealing Accounts. To deliver this surveillance effectively firms define "request for quote", "expressions of interest" and "orders" (in relation to foreign exchange markets) within an Order Management Policy and that information is captured in an Order Management System. Targeted reviews of **eCommunications** and **voice** data are performed if unusual or suspicious activity is identified from trade surveillance alerts.
Improper disclosure (covering inappropriate sharing of information between fund managers and dealers; to brokers and intermediaries; or internally)	**eCommunications** • eCommunications surveillance is performed across electronic communications of sales and trading staff in foreign exchange markets. • The lexicon used is informed by the nature of information likely to be held within the firm - covering words or phrases that may be indicative of inside information. • Lexicons are refined with additional words or phrases that could be indicative of inside information, especially when there has been a market incident. Targeted listening of **voice** calls are performed if unusual or suspicious activity is identified from trade or eCommunications surveillance alerts.
Attempts to manipulate fixes Marking a reference price (which is derived from a transaction window)	Firms apply automated **trade surveillance** to fixes on a risk based approach considering: • Market liquidity (where different risks apply dependent on levels of liquidity); • The firm's activity - whether the firm was active during the fixing window and assessing how this compared to market liquidity; • The firm's activity - assessment to whether the firm passive during the fixing window and assessing how this compared to market liquidity; • The firm's activity in illiquid fixes; • The firm's change in behaviour e.g. contributing to new fixes. **eCommunications** • Firms review all communications originated by the individual trading during the fixing window, and for a time period pre and post the fixing window. • The lexicon also encompasses words or phrases that could be indicative of attempting to manipulate fixes. **Voice** • Firms listen to a sample of calls originated by the individual trading during the fixing window, and for a time period pre and post the fixing window.

Risk	Statements of Good Practice
Artificially increasing/price Artificially stabilising price Triggering [client] stop loss orders or barrier options (or other optional redemptions or related derivatives) Banging the a reference price (other than that derived from a transaction window)	Targeted **trade surveillance** is performed on a manual basis to cover the specified risks. Trade surveillance focusses on desk trading contributing towards a price drift to (or maintaining) the price point of the Stop Loss trade and/or Barrier Option (or Large Position). • Firms operate "Large Movements Report" to identify trading occurring during large price movements. • Firms operate Significant Trading Reports to identify sudden growth in trading volume/interest.
Layering & Spoofing	**Trade surveillance** is performed on a manual basis, taking a risk based approach for each currency pair. Firms surveil using Order to Trade ratios and trade volume alerts (i.e. low volume; high frequency) to identify suspicious activity.
Creating/ enhancing arbitrage possibilities between a financial instrument and another related financial instrument	**Trade surveillance** is performed on a manual basis with reference to existing positions and on a risk based approach.
Cross market/venue manipulation/ internal cross trades	Manual approach to **trade surveillance**. Please see Emerging Practices section of this document.
Ramping indicative pricing (published bid / offer spreads)	Manual approach to **trade surveillance** informed by: • Review of exception reports from order management systems e.g. large movement reports. • Review of Order to Trade ratios scenarios against a specified threshold tolerance. **E-Communication** with a specific lexicon.
Inappropriate use of Personal Dealing Accounts ("PAD") (including spread betting)	**Trade surveillance** of PAD is performed on a manual basis. This considers (at a minimum) the following information: • the employee's role; • the size of their trading activity; • whether the size of their trade is within internal restrictions; • whether they are seeking to undertake a trade in an approved product; • whether they trade in that product for clients of the firm; • whether they have been privy to inside or confidential information in relation to the product they are seeking to trade.

Risk	Statements of Good Practice
Wash trades/Improper Matched Orders	• Firms operate automated trade surveillance scenarios to identify single party wash trades. • Firms have assessed the risk of wash trades occurring based on the firm's activity in particular currency pairs. • Firms have implemented trade surveillance capabilities to identifying wash trades pre-arranged and conducted by two or more parties across all relevant currency pairs.
Dominant trading/cornering the market/abusive squeeze	Firms employ **trade surveillance** to identify where their activity constitutes a significant amount of trading and/or open market interest. Good practice includes a firm's trading activity, product trading protocol and market volumes as a key input into surveillance. In the foreign exchange market, this risk is considered to be lower in liquid currency pairs (e.g. G10) and consequently higher risk in non-G10 spot markets, foreign exchange NDFs and other derivative products.
Dissemination of false rumors	**E-Communication** with a general lexicon. Additionally, retrospective targeted reviews around identified known rumours are also performed.
Use of non-specific trade information flow to manipulate the market (e.g. buy-side regular FX patterns)	**Trade surveillance** monitors for trading inferences drawn from executed transactions. This process tends to be through manual review of trade data. Firms also operate surveillance over the effectiveness of their information barriers to assess the effectiveness to which non-specific trading information is controlled and distributed. **E-Communication** with a general lexicon.
Recommending or inducing others to engage in market manipulation	**E-Communication** with a general lexicon.
Abnormal trading	Risk mitigated through manual review. Some firms deploy statistical / algorithmic analytics to identify transactions for manual review.
Transaction window rates	Risk mitigated through manual review. Some firms deploy statistical / algorithmic analytics to identify transactions for manual review.
Partial fills	Risk mitigated through manual review. Some firms deploy statistical / algorithmic analytics to identify transactions for manual review.
Unsupported 'Last Look' practices	Risk mitigated through manual review. Some firms deploy statistical / algorithmic analytics to identify transactions for manual review.

Risk	Statements of Good Practice
Indefensible mark-ups	Trade surveillance monitors for pricing discrepancies including off-market prices. Additionally risk mitigated through manual review.
Coordinated trading	Firms use **eCommunications** surveillance with a specific lexicon to identify instances where one or more party may be seeking to coordinate their trading activity.

4. Good Practices for FX markets: Buy-Side

Risk	Statements of Good Practice
Insider dealing using MNPI and Personal Account Dealing	**Trade surveillance** Trade surveillance for insider dealing focusses on instances where foreign exchange transactions differ from normalised trading activity for funds and fund managers when the firm may have been in receipt of relevant inside information. For example, significant inter-country M&A deals may create situations where information, such as the specific time and currency of the deal, may give an asset manager access to rate sensitive information. Additionally firms' trade surveillance scenarios are focused on trading ahead of M&A public announcements. Trade surveillance of Personal Account Dealing is only possible to the extent that staff people PA trade through the firm processes and systems. **eCommunications surveillance and voice surveillance** Firms operate specific eCommunications lexicons targeted at Insider Trading risk. Additionally voice and eCommunications data is used to support the manual further investigation of activity identified through trade surveillance.
Recommending or inducing others to engage in insider dealing	**Trade surveillance** As per Insider Dealing above.
Front running/pre-positioning	**Trade surveillance** Review foreign exchange trade data and external markets data to identify trades that have been placed ahead of an event, such as a large contracts rolls or M&A public announcements. **eCommunications** Firms apply automated eCommunication surveillance lexicons to search for words or phrases in electronic written communications that may give rise to instances of potential front running.
Improper disclosure (covering inappropriate sharing of information between fund managers and dealers; to brokers and intermediaries; or internally)	Firms mitigate this risk through review of the outcomes from specific eCommunication lexicons.
Layering/Spoofing	**Trade surveillance** Alerts specifically designed to search for high volumes of cancels and amendments of orders.

Risk	Statements of Good Practice
Wash trades/Improper Matched Orders	**Trade surveillance** Firms operate trade surveillance on a T+1 basis to identify possible wash trades. **eCommunications surveillance and voice surveillance** Firms operate specific eCommunications lexicons targeted at wash trading. Targeted voice and eCommunications surveillance and data is used to support the reviews / further investigation of activity identified through trade surveillance. This is a manual process.
Cross market/venue manipulation	**eCommunications surveillance and voice surveillance** Firms operate specific eCommunications lexicons targeted at cross market / venue manipulation.
Quote Stuffing	**Trade Surveillance** Firms operate automated surveillance on RFQs and Orders. Additionally, teams manually review RFQs in electronic platforms that are not executed or cancelled.
Coordinated trading	Firms use **eCommunications** surveillance to identify instances where one or more party may be seeking to coordinate their trading activity.
Portfolio Allocation	**Trade Surveillance** Larger buy-side firms operate automatic allocation rules through their Order Management Systems to ensure that once the trades are combined and as orders are filled in the market the allocation will automatically pro-rata the allocation across the relevant portfolios, based on their relative order size. Firms' surveillance focuses on evaluating the equitability of manual allocations.
Cross-trades	**Trade Surveillance** Firms may require Portfolio Managers and Traders to label cross trades within Order Management Systems which provides a mechanism for identifying cross-trades within surveillance tools. Firms use external market data to assess cross-trades to identify potentially unfair prices. Some firms use surveillance to compare their buy and sell transactions for the same financial instruments to identify cross trades which may not have been correctly labelled. Firms run the same surveillance mechanisms over these trades.

5. Good Practices for FX markets: Venues

Risk	Statements of Good Practice
Insider dealing using MNPI	Venues surveil for insider dealing by employing **trade surveillance** to monitor for: • unusual volumes • unusual orders • large trades • large orders • unusual bid/offer spreads, including deep dive analysis of RFQs and off-market transactions and orders. Venues supplement their transactions based surveillance with external information, such as market news, to identify unusual trading around specific events. Venues conduct 'thematic reviews' of trading data based on known behaviours and interactions of certain market participants over a period of time to identify potential instances of insider dealing.
Recommending or inducing others to engage in insider dealing	Venues employ **eCommunication** and **voice surveillance** as relevant to their business practices. eCommunication and voice surveillance channels are applicable to Voice Brokers only. The eCommunication and voice surveillance channels do not apply to venues whose staff do not take or receive orders through voice or electronic communications channels from venue participants.
Front running/pre-positioning	Venues have **trade surveillance** alerts in place for the portion of the trades that they can view on their platform. At some venues trade surveillance alerts designed to identify 'unusual trades' that consider, amongst other factors, the sequencing and correlation of trades.
Improper disclosure (covering inappropriate sharing of information between fund managers and dealers; to brokers and intermediaries; or internally)	See 'Recommending or inducing others to engage in insider dealing'.
Attempts to manipulate fixes	Averages can be assessed during the fixing window via codes calibrated to detect price anomalies. **Trade surveillance** scenarios applied to fixing windows include, but are not limited to: • Large and/or unusual trades and orders; • Off market trades; • Unusual bid/ask spread; • Abnormal Daily Benchmark Price Change Alert; • Marking/Reverse marking the close alert; • Quote stuffing; • Potential collusion among regional branches of same contributor; and • Wash/Money Pass alerts.

<table>
<tr><th>Risk</th><th>Statements of Good Practice</th></tr>
<tr><td>Layering/Spoofing/Spivving</td><td>Venues deploy trade surveillance scenarios over quote or transaction data to detect:
RFQ to quote ratios; looking at the number of inquiries or RFQs placed, versus the number of trades actually done. This pattern alert should be set at the individual participant level whereby ‘minimum criteria’ for the alert is set per participant to avoid unnecessary false positives in respect of activity assessed as legitimate.
Message uptick scenarios that flag if there is an unusually large volume of trades within a given time window.
Trading away from a composite price.
Alerts calibrated to review for excessive amounts of orders by specific traders or credit codes away from market level or near top of book.
Alerts calibrated to review for patterns conducted by specific traders or credit codes with a simultaneous imbalance of Bid/Offer interest in the market, with subsequent order cancelation of a fill, or reestablishment of entire bid/order interest for unsuccessful fills.</td></tr>
<tr><td>Artificially increasing price</td><td>Automated trade surveillance alerts are constructed to detect an artificial increase in the price. For example, the scenario may assess traded price against last traded price in a particular product to identify exceptions.

Venues also construct trade surveillance scenarios to identify firms that may be ‘ramping the composite’ then they stream prices into the venue.</td></tr>
<tr><td>Artificially stabilising the price</td><td>Automated trade surveillance alerts are constructed to detect artificial price stabilisation. For example, venues operate ‘message uptick scenarios’ that flag if there is an unusually large volume of trades within a pre-defined time window. This is determined per product and per participant.</td></tr>
<tr><td>Cross market/venue manipulation</td><td>Please see Emerging Practices section of this document.</td></tr>
<tr><td>Ramping indicative pricing (published bid/offer spreads)</td><td>Automated trade surveillance scenarios for ramping the composite price is defined by the RFQ to quote ratio.

Venues have rulebooks in place which include ratio rules to thresholds to detect and ‘throttle’ behaviour viewed as excessive.</td></tr>
<tr><td>Parking</td><td>Manual trade surveillance is performed thematically by some venues whereby transactions with the same market participants are reviewed and assessed around times considered to be of higher risk periods, such as calendar quarter ends. Correlation (including inverse correlation) is considered at some venues as a risk input.</td></tr>
<tr><td>Quote stuffing</td><td>Venues use trade surveillance scenarios based upon ‘RFQ to quote ratios’ to identify potential instances of quote stuffing. Venue rules specify minimum standard rules in respect of order fill ratios and quote life.

Venues also use abnormal message alert scenario which capture instances of an ‘unusually high’ number of cancellations within a given time window; where unusually high is defined (and refined) based upon an analysis of trading patterns.</td></tr>
<tr><td>Dissemination of false rumours</td><td>Venues employ eCommunications and voice surveillance as relevant to their business practices.</td></tr>
</table>

Risk	Statements of Good Practice
Wash trades/Improper Matched Orders	Venues have established automated **trade surveillance** alerts for wash trading; conducting targeted analyses on shorter-term defined activity windows. Thresholds for alerts are set per product and based on the expected/average liquidity in that market.
Trade information leakage	Venues employ **eCommunications** and **voice** surveillance as relevant to their business practices.
Dominant trading/cornering the market/abusive squeeze	Automated **trade surveillance** scenarios have been configured for 'abnormal trading', where trading activity deviates from a normalised trading pattern. This alert is used to identify potential instances of dominant trading, cornering the market and abusive squeezes.
Use of non-specific trade information flow to manipulate the market	Venues employ **eCommunications** and **voice** surveillance as relevant to their business practices.
Indefensible mark-ups	Automated **trade surveillance** scenarios of 'trade price vs. last trade' and 'off-market' are designed to challenge transactions where there is a significant deviation.
Unsupported 'last look' practices	Venues conduct thematic last look reviews to ensure transparency of 'last look'. This provides monthly alerts identifying which dealers may be 'over using' the last look function and consistently returning with lower prices. The alert looks for outliers in how often this function is being used. Some venues provide reports to participants to allow them to make trading decisions based on data.
Coordinated/concurrent trading	A thematic 'network view' of participant relationships is taken. Statistics on trade count and volumes are monitored daily to identify connections that require investigation. Some venues have highlighted that outputs within the following alerts may consequentially identify coordinated / concurrent trading: Wash trades; Off market trades; Large trades (including) Excessive volume between certain market participants; Benchmark fixes and 'A money pass/capital exchange'.
Abnormal trading	Automated **trade surveillance** alerts for large and unusual orders, quotes, trades and prices, split by product type to identify instances of abnormal trading. The alerts highlight the volume and value of trading over a specified time window per product. Venues also include the outstanding issuance amount of a security, market interest and liquidity to determine 'abnormal' trading activity.
Upholding your axe	Monthly reviews are performed to identify outliers of dealers that do not uphold their stated intentions. Thematic reviews over a longer duration are conducted to establish patterns. This is performed on a manual basis.
Churning	An automated **trade surveillance** alert is in place to identify situations where several small trades executed by one participant net to zero.

6. Glossary of Sub-Risks

Risk category	Specific Sub-Risk Categories	Description	Source
Insider dealing	Insider dealing using MNPI	Where an insider deals, or attempts to deal, or cancel or amends an order, in a qualifying investment or related investment on the basis of inside information.	FCA Handbook (MAR 1.3) / Market Abuse Regulation (Article 8.1)
	Personal Account Dealing	The risk that a person enters into a transaction on their own account which involves the misuse or improper disclosure of confidential information; or conflicts, or is likely to conflict, with an obligation of the firm to a client or another obligation of the firm.	Informed by FCA COBS 11.7.1 R
	Recommending or inducing others to engage in insider dealing	Recommending that another person engage in insider dealing, or inducing another person to engage in insider dealing, arises where the person possesses inside information and recommends another to conduct Insider dealing (as defined above).	Market Abuse Regulation (Article 8.2)
	Front running / pre-positioning	A transaction for a person's own benefit, on the basis of and ahead of an order (including an order relating to a bid) which he is to carry out with or for another (in respect of which information concerning the order is inside information), which takes advantage of the anticipated impact of the order on the market or auction clearing price.	FCA Handbook (MAR 1.3.2) FCA specified risk
Unlawful disclosure of inside information	Improper disclosure (covering inappropriate sharing of information between fund managers and dealers; to brokers and intermediaries; or internally)	Where an insider discloses inside information to another person otherwise than in the proper course of the exercise of his employment, profession or duties. Criticism within the enforcement notice that emails drafted by corporate broking and research staff detailing initial information on potential investment opportunities were not reviewed by the compliance department prior to circulation to ensure that they did not contain inside information; and the compliance department did not monitor calls made between staff and third parties to ensure that wall-crossing was happening appropriately and/or whether market abuse was occurring.	FCA Handbook (MAR 1.4.5) Description also informed by FCA Market Abuse Enforcement (W H Ireland Limited) (Article 4.23.3-4.23.4)

Risk category	Specific Sub-Risk Categories	Description	Source
Manipulating transactions	Attempts to manipulate fixes	Trading, and other behaviours, undertaken with the intention of influencing the price of a fix. Example At 1pm Trader A accepts a large order from Client A to buy GBP at the 1:15pm fix price. Trader A accumulates directionally similar information from other market participants. This is done in order to build Trader A's position and increase Trader A's ability to influence the 1:15pm fix price. Trader A uses the accumulated position to trade during the 1:15pm fix window in a manner designed to influence the price fixed.	FCA Specified Risk
	Layering & Spoofing	Entering orders into an electronic trading system, at prices which are higher than the previous bid or lower than the previous offer, and withdrawing them before they are executed, in order to give a misleading impression that there is demand for or supply of the qualifying investment at that price, and Submitting multiple orders often away from the touch on one side of the order book with the intention of executing a trade on the other side of the order book. Once that trade has taken place, the manipulative orders will be removed. Indicative behaviour: "(f) the extent to which orders to trade given change the representation of the best bid or offer prices in a financial instrument, a related spot commodity contract, or an auctioned product based on emission allowances, or more generally the representation of the order book available to market participants, and are removed before they are executed".	FCA Handbook (MAR 1.6.2(4)) ESMA Automated Trading Guidelines (Article 5.2) FCA specified risk
	Artificially increasing price	Entering small orders into an electronic trading system, at prices which are higher than the previous bid or lower than the previous offer, in order to move the price of the qualifying investment, other than for legitimate reasons.	FCA Handbook (MAR 1.6.4(3))
	Artificially stabilising price	Transactions or orders to trade employed so as to create obstacles to the price falling below a certain level, in order to avoid negative consequences for the issuer, for example a downgrading of its credit rating.	FCA Handbook (MAR 1.6.4(6))
	Cross market/venue manipulation	Trading on one market or trading platform with a view to improperly influencing the price of the same or a related qualifying investment that is traded on another prescribed market.	FCA Handbook (MAR 1.6.4(7))

Risk category	Specific Sub-Risk Categories	Description	Source
	Ramping indicative pricing (published bid/offer spreads)	An individual dealer submitting a significant level of quotes to affect the published bid or offer.	Other observed behaviours
	Parking	Selling to another party to constrict the market with the understanding that the original owner will buy the instrument back after a short time.	Other observed behaviours
	Dissemination of false rumours	The dissemination of information by any means, including the dissemination of rumours, which gives, or is likely to give, a false or misleading impression as to the supply of, demand for, or price of qualifying investment (including impacting the price to an abnormal or artificial level) by a person who knew or could reasonably be expected to have known that the information was false or misleading. "Indicators of manipulative behaviour relating to the employment of a fictitious device or any other form of deception or contrivance (a) whether orders to trade given or transactions undertaken by persons are preceded or followed by dissemination of false or misleading information by the same persons or by persons linked to them; and (b) whether orders to trade are given or transactions are undertaken by persons before or after the same persons or persons linked to them produce or disseminate investment recommendations which are erroneous, biased, or demonstrably influenced by material interest."	FCA Handbook (MAR 1.8.1) / Market Abuse Regulation (Annex I, B)
	Quote Stuffing	Entering large numbers of orders and/or cancellations/updates to orders so as to create uncertainty for other participants, slowing down their process and to camouflage their own strategy.	ESMA Automated Trading Guidelines (Article 5.2)
	Wash trades/Improper Matched Orders	A sale or purchase of a qualifying investment where there is no change in beneficial interest or market risk, or where the transfer of beneficial interest or market risk is only between parties acting in concert or collusion, other than for legitimate reasons; Indicative behaviour: "(c) whether transactions undertaken lead to no change in beneficial ownership of a financial instrument, a related spot commodity contract, or an auctioned product based on emission allowances;".	FCA Handbook (MAR 1.6.2(2)) FCA Specified Risk Market Abuse Regulation (Annex I, A(c))

Risk category	Specific Sub-Risk Categories	Description	Source
	Trade information leakage	The sharing of confidential information including client identities, client orders, proprietary orders and client spreads with other market participants.	FCA Specified Risk
	Dominant trading/cornering the market	Conduct by a person, or persons acting in collaboration, to secure a dominant position over the supply of or demand for a financial instrument, related spot commodity contracts or auctioned products based on emission allowances which has, or is likely to have, the effect of fixing, directly or indirectly, purchase or sale prices or creates, or is likely to create, other unfair trading conditions; Indicative behaviour: "(a) the extent to which orders to trade given or transactions [or orders cancelled] undertaken represent a significant proportion of the daily volume of transactions in the relevant financial instrument, related spot commodity contract, or auctioned product based on emission allowances, in particular when those activities lead to a significant change in their prices".	Market Abuse Regulation (Article 12.2(a), Annex I.a)
	Triggering [client] stop loss orders or barrier option (or other optional redemptions or related derivatives)	Transactions or orders to trade which have the effect of, or are likely to have the effect of increasing/decreasing/maintaining the price of a financial instrument (or the underlying financial instrument of a derivative) preceding the issue, optional redemption or expiry of a related derivative or convertible; or payout determination (e.g. in respect of client stop loss or barrier options).	MiFID II MAR Annex (Section B.25)
	Creating/enhancing arbitrage possibilities between a financial instrument and another related financial instrument	Creating or enhancing arbitrage possibilities between a financial instrument and another related financial instrument by influencing reference prices of one of the financial instruments can be carried out with different financial instruments.	MiFID II MAR Annex (Section B.31)
	Use of non-specific trade information flow to manipulate the market	The disclosure of non-specific, confidential information, such as buy-side trading patterns, to potentially affect the trading decisions of market participants.	Other observed behaviours

Risk category	Specific Sub-Risk Categories	Description	Source
Other transaction based conduct risks	Indefensible mark-ups	Deliberately misleading a client as to the nature of a spread being charged. Example: Client A makes a request to Salesperson A to hear Trader A's price. Salesperson A agrees to this request, but instructs Trader A to widen the spread when quoting the price.	FCA Specified Risk
	Unsupported 'last look' practices	Refers to the ability that liquidity providers have to reject an order even when the order matches the liquidity provider's quoted price. The liquidity provider has one last chance or 'look' to decide whether they want to accept the order.	Other observed behaviours
	Inappropriately assigning transaction window rates to client orders	Not assigning the appropriate transaction rate to a client who has placed an 'at best' or 'transaction window' order. Example: Client A leaves an order with Trader A to buy 100 'at best' with 10 minutes to execute the order. Trader A buys at 15, 16 and 17 for a 16 average (inclusive of any costs to transact the order). The trading range over the 10 minutes was 14/24. Trader A fills Client A's order above the 16 average but within the trading range, for example, at 22.	FCA Specified Risk
	Coordinated trading	Organised or coordinated trading between market participants. Example: Trader A at Firm A advises Trader B at Firm B to trade in a particular manner as a result of confidential client, or proprietary, order information. Trader A may, but does not necessarily disclose the specific information to Trader B.	FCA Specified Risk
	Performing 'partial fills' of client orders	Client orders not being filled in line with the amount or volume actually transacted. Example: Trader A receives a client order to buy 100 at 15. Trader A bids 15 and receives 50, before the market moves higher. Trader A books 30 (of the 50 bought) to the client, keeping 20 on his or her own book. If the market falls Trader A will book the 20 to the client at 15 with no risk, if the market moves higher Trader A retains the 20 and profits from the trade.	FCA Specified Risk

Risk category	Specific Sub-Risk Categories	Description	Source
	Portfolio Allocation	Where multiple buy-side portfolios within a firm transact in concert to achieve a better price in trying to trade the same financial instrument/product on the same day, there is a conflict of interest risk where orders filled or partially filled may not be allocated equitably such that a portfolio may unduly benefit to the detriment of others.	Other observed behaviours
	Inappropriate use of personal dealing accounts (including spread betting)	Individuals within a firm using personal dealing accounts to profit from confidential information acquired in the course of their employment. Example: Trader A receives a large client order that is likely to move the market. Prior to executing the client order, Trader A places an order via their personal dealing account that will profit from the likely market movement. Trader A executes the client order, moving the market in the anticipated direction, and then closes their personal dealing account position for a profit.	FCA Specified Risk
	Cross-trades	Where a buy-side firm is seeking to buy a financial instrument/product in one portfolio and sell the same in another portfolio, the two portfolios may elect to complete the transaction between themselves. There is a conflict of interest risk whereby the transaction may be completed at an unfair fair price for the behalf of one both side to the detriment of the other.	Other observed behaviours
	Abnormal trading	Instances where trading does not match normal behaviour as determined within a firm or on an on-going basis with reference to market data, for example, an unusual level of quotes submitted when compared to executed trades.	Other observed behaviours
	Upholding your axe	Dealer not executing on an instrument they are axed to when a client attempts to trade with that dealer.	Other observed behaviours
	Churning	Excessive trading in a client's account to generate commissions while doing little to meet the client's investing objectives.	Other observed behaviours