FICC Markets Standards Board

Monitoring of written electronic communications

Statement of Good Practice for FICC Market Participants

September 2017

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 ("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 SGP 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. SGP will be shared with Non-Member firms and their associations, who are encouraged to consider them. Information on SGP 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 SGP 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. Rather they serve as a supplement to any and all applicable law, rules and regulation. In developing Standards and SGPs, 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 therefore some 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.

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 attention to Member Firms of an existing Code and request adoption, once appropriate steps have been taken to confirm its applicability.

II Monitoring of written electronic communications

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 recommendations, which specifically stated that '… Firms active in FICC markets should take greater collective responsibility for developing and adhering to clear, widely understood and practical standards of market practice…'.

Wholesale market participants are required to implement and maintain controls to aid in the detection of misconduct which may include real or attempted incidents of market abuse and manipulation, bribery, fraud and other inappropriate behaviours as set out in firms' Codes of Conduct. This requirement is covered by a range of regulation covering banks, buy-side and other market participants.

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.

2. Scope and applicability

This document outlines SGP for the surveillance of written electronic communications on firm-owned devices, and "bring your own devices" (e.g. desktops, laptop computers, mobile phones) when using applications and software approved by the firm for the conduct of business activity on such devices. Personal communications which occur on firm devices may fall into the scope of monitoring by virtue of the communication channel. Written electronic communications conducted on personal devices for personal purposes and not conducted using applications and software approved by the firm for the conduct of business activity on such devices (e.g. personal email accounts, personal social media accounts, texting on own mobile devices etc.) are not within the scope of this document.

Note that lexicons may be applied to text transcribed from voice communications should firms have this capability in place. However, this is not within the scope of this document.

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, in particular their scale and complexity.

III Good Practice Statements and Commentary

1. Organisation, roles and responsibilities

Good Practice Statement 1: *Firms should have a clear organisational structure and senior ownership in place for proactive and reactive monitoring of electronic communication, ensuring that surveillance activities are appropriately independent and proportionate to the activities of the firm, taking into account the business model, client service and execution model, scale and complexity.*

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

Surveillance activities, both proactive and reactive should wherever possible be owned by a function which is independent from the first line business activities and/or independent business controls in the first line of defence, which have sufficient expertise 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

Firms should ensure that surveillance output is reported into the necessary individuals and governance functions in the organisation to ensure appropriate senior visibility, understanding and oversight of potential suspicious behaviour. Reporting routes should include:

- Specific senior management roles (e.g. Business Heads, Head of Compliance, Head of Risk)
- Necessary 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 breach which are fit for purpose, formalised and documented. The FMSB notes that the following models are 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 partners as appropriate, per the judgment of the surveillance function

- 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: *Firms should ensure that roles and responsibilities for monitoring of written electronic communications are clearly 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 of written electronic communications should be clearly defined and documented for in-scope communication channels (see Section II.2 "Scope and Applicability") with clear ownership aligned to the organisational model of the function.

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

- *Surveillance policies and procedures:* Ownership of documentation, the standards documented and regular review and updating of documentation
- *Design and implementation of tools:* Design and testing of the functionality of surveillance tools
- *Lexicon:* Initial lexicon design, construction and associated analytics, ongoing periodic and event-driven lexicon updates
- *Day to day monitoring:* Automated and manual proactive and reactive monitoring of electronic communication across in-scope communication 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 proactive detection capabilities to minimise volume of false positives
- *Reporting and MI:* Daily and consolidated 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

Good Practice Statement 3: *Firms should have appropriate measures in place to promote compliance with data privacy and data protection laws and regulation, taking into account local jurisdiction requirements.*

Data privacy and data protections laws differ between firms' operating jurisdictions and it is critical that firms put in place appropriate safeguards to promote adherence to these. Beyond implementing measures to comply with legal and regulatory requirements, the following measures should be considered to promote appropriate data access and control:

- *Disclosures:* Clear communication to employees regarding the nature, scope and purpose of firm recording and monitoring of employees' communications
- *List of Monitored Users:* Documented list of monitored users which is kept up to date
- *"Need to know" basis:* Clear definition of who can view written electronic communications data based on the need to perform their role in the organisation. Where possible, this should be supported by appropriate systems controls to limit access
- *Hierarchy of access:* Categorisation of individuals to determine levels of communications data access. This is to ensure that individuals only monitor communications according to their

respective business coverage area and do not see communications that may be inappropriate to their business coverage in the firm
- *Data access logs*: Individual-level records of access to communications data
- *Retention*: Appropriate retention periods that are documented and adhered to

Good Practice Statement 4: *Firms should have in place appropriate preventative measures such as policies or structural controls, to reduce the risk of inappropriate written electronic communications on business communication channels on firm owned devices and to deter the use of un-monitored personal devices or unmonitored applications and software on bring your own devices for business purposes. These controls should be subject to ongoing monitoring and enforcement.*

The preventative controls that firms have in place will vary according to the organisational structure, policy and technological capabilities of, and laws applicable to, the firm in question. Practices are also noted to differ between sell-side, buy-side and infrastructure firms.

Examples of good practice for preventative measures related to the access of electronic communication, to the extent permitted by applicable laws, include:

- Firm policies which restrict communications to channels and applications on firm-owned devices (and approved applications and software on approved 'bring your own' devices) to limit the use of unmonitored personal devices for business purposes. Employees may for example engage on social media in their private capacities on their personal devices but this is typically out of scope of firms' monitoring activities. Training on these policies may include guidance on the perimeter of communications that are deemed to be for 'business purposes'.
- Where firms allow "bring your own device" there should be clear policies in place which communicate the level of surveillance on the communications by employees on those devices and guidance on whether and how different types of communications should be carried out on those devices.
- Channels of communication should only be approved for business use if they can be appropriately secured and monitored. The IT application onboarding process is a useful control to ensure this requirement is captured.
- Where there are exceptions to policy, they should be proportionate to the business rationale and signed off by senior management for the relevant activity. For example, in extremis, a business continuity event may require staff to temporarily use communication channels that cannot be monitored. This should include an activity and risk assessment to determine which communication channels or applications each business needs to use and provide these on an "opt-in" basis.

The preventative measures that firms put in place are varied and will also depend on the nature and risks of the business conducted. Some examples of preventative measures to reduce the risk of communications through unapproved channels include:

- Policies limiting access to multi-lateral chatrooms
- Policies regarding mobile phone usage on the trading floor (firm owned or personal device)
- Policies regarding availability of messaging platforms on firm-owned devices (e.g. WhatsApp, Viber, messaging features on LinkedIn)
- Policies regarding personal email and social media access on firm-owned devices (e.g. Facebook, LinkedIn, Twitter)

Firms should consider where it may be appropriate to implement tranches of restrictions (for example, according to seniority or role in the firm). However, these instances should be kept to a minimum and on an exception basis in order to keep the control environment streamlined.

2. Processes for maintaining effective lexicons

Good Practice Statement 5: *Firms should have in place appropriate lexicons and related analytics which reflect the inappropriate behaviour and risks in firm activities that the firm is attempting to prevent and/or detect. These should include, but are not limited to, real or attempted market abuse, bribery, fraud and inappropriate behaviours.*

Lexicons should be developed and maintained by individuals and/or functions who are appropriately independent (as described in Good Practice Statement 1) of the population under surveillance to maintain integrity of the lexicon. A range of approaches exist to developing lexicons but the following practices should be used to construct lexicon and identify keywords:

- Lexicon 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)
- Lexicon construction should use a number of sources, which may include:
  - Internal policies, procedures and guidelines
  - Systematic review of identified themes or risks (e.g. market manipulation, collusion, bribery 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
- Individuals under surveillance should not have visibility of the lexicon although they may provide input and perspectives on risks and themes which may require attention
- Potential for select first line manager sample testing of the lexicon under senior compliance supervision, ensuring that they do not have undue insight into the full lexicon

Developed lexicons should be structured to allow effective challenge, review and maintenance. Some examples of the lexicon structures that firms use are:

- By thematic tranche (e.g. market manipulation, conflict of interest, AML, profanity, mis-selling etc.)
- By population (e.g. sales, trading, fund managers, relationship managers)
- By policy type (e.g. code of conduct, regulatory non-compliance, internal policies, principles or guidelines documents etc.)

As a global industry, the wide range of spoken languages used by staff under surveillance is an ongoing challenge for firms. Firms should consider how their own controls can most effectively monitor the languages used by their business. This requires the development of language coverage capabilities, where necessary, that is prioritised based on the volume of language usage and the risk of the environment in which it is used. Examples of good practice include the use of multi-language lexicons and the restriction of languages that should be used to conduct business activity.

Good Practice Statement 6: *Lexicons and related analytics should be regularly reviewed and updated to ensure that suspicious behaviour is being detected and to reduce the number of false positives and false negatives with appropriate governance in place to oversee and track changes.*

Lexicons should be updated and maintained by individuals and/or control functions who are appropriately independent of the population under surveillance to maintain integrity of the lexicon.

Lexicon review generally falls into two types of activity:

- *Periodic review:* periodic review of lexicons should take place at least annually, although some firms may review lexicons more frequently across the whole lexicon or for certain parts of the lexicon
- *Event-driven review:* Ad hoc review of lexicons can be triggered by a number of events which may include the number (or lack of) alerts, number of false positives, an internal breach event or external event which requires read across to the organisation

Firms should consider which internal events and circumstances should be used to instigate ad hoc lexicon review and update. These circumstances may include, for example:

- Updates to policies, procedures and guidelines
- Workshops or interviews with experts in the organisation and external to the organisation
- Analysis of alerts and flagged messages, investigations and breaches
- Analysis of peers and industry events
- Regulatory enforcement orders
- Regulator thematic reviews

Firms should undertake lexicon reviews with the aim of maximising the effectiveness of risk identification and therefore increasing the amount of resource time that can be dedicated for each genuine alert. It is important that a lack of alerts is also proactively reviewed and investigated to mitigate the likelihood of potential false negatives.

Appropriate governance should be in place to ensure appropriate oversight of decision making with regard to changes in lexicons and an audit trail recorded to track changes between iterations of lexicons.

Good Practice Statement 7: *Firms should ensure appropriate control, oversight and reconciliation of data ingests and supporting infrastructure for written electronic communications surveillance.*

Quality of data ingests into the written electronic communications surveillance tools is critical to the effective operation of the surveillance effort. Data that is feeding written electronic communications surveillance tools should accurately reflect data that is being generated on various in scope communications platforms. Key issues that firms have observed with regard to data quality include missing messages, missing metadata (e.g. name of trader, time of message etc.), blank content, scrambled content etc.

Firms should have controls and processes in place to proactively and periodically monitor data completeness and quality as well as a clear statement of tolerance around data quality.

Some examples of practices that firms have implemented are:

- **Definition and publishing of an approved communications platform "whitelist**": the purpose of the whitelist is to mitigate the risk of employees communicating on platforms which cannot be recorded and monitored. Managing a clear "whitelist" is likely to be more effective than managing than a "blacklist" of banned communications platforms given the number of communication platforms available. Consistent with Good Practice Statement 4, good practice is to have policies and controls that disallow and disable where possible, communications on platforms that are not on the whitelist.
- **Data validation tool:** Automated tools which monitor and reconcile data at a high level (e.g. reconciliation of number of messages, testing that metadata fields are populated etc.).
- **Sample based data reconciliation:** More detailed sample testing of messages for content quality.
- **Use of a dummy test account:** Some firms have set up dummy accounts which are used to periodically plant trigger words phrases to test that data is feeding through to tools and the lexicon is working.

3. Reactive controls and processes

Good Practice Statement 8: *Firms should have surveillance processes in place using lexicons to monitor written electronic communications carried out by employees on in-scope communications platforms reasonably designed to detect real or potential inappropriate behaviours. These should include, but are not limited to, real or attempted market abuse, bribery, conflicts of interest, fraud and inappropriate behaviours.*

All relevant written electronic communications messages should be subject to a baseline level of reactive surveillance using the lexicons discussed in Good Practice Statements 5 to 7, regardless of risk level of the individuals, seniority of the individuals or the platform on which the electronic communication is conducted.

It is noted that there are some platforms, such as communications platforms ancillary to some trading applications or social media, where firms may not have the capabilities in place to monitor and store the communications. In general it is expected that firms should have the appropriate policies and, where appropriate and practical, additional controls in place to restrict communications on these platforms to reduce the risk of inappropriate communications on these channels. Additionally, firms should be mindful of their record-keeping activities and obligations.

Reactive surveillance tools should produce an alert if suspicious and/or inappropriate communications have occurred, in line with the lexicons in place, for review and investigation by surveillance officers.

Good Practice Statement 9: *Alerts arising from reactive surveillance processes should be processed, investigated and closed out in a diligent and, as far as possible, timely manner in alignment with agreed process and governance by appropriately trained surveillance officers.*

Alerts must be processed by the appropriate surveillance officers, compliance officer or control staff in the firm who are not compromised by the nature of their involvement in the activities under review. Alerts should be directed to, and reviewed and investigated as required by the most appropriate

function for the nature of the breach (e.g. Compliance Officers, HR, Audit, Fraud teams etc.). Front Office representatives should be engaged in review and investigation of escalations as required and at the discretion of the appropriate compliance or control officers leading the reviews.

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 activity may be deemed sufficiently suspicious to report to the relevant authorities.

Example tier approach to processing surveillance alerts

- *Level 1 Reviewed and closed:* 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 concluded that no breach had occurred, alert is closed with no further action taken.

- *Level 2 Reviewed, escalated and closed:* Alert is reviewed by the appropriate surveillance officer, compliance officer and/or first line of defence control officer and found that there was a potential breach. Case is escalated to concerned staff members to obtain further information and/or escalated to relevant parties (e.g. staff line manager, compliance officer, HR) for review, after which it was concluded that no breach has occurred. 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 and addressed by the business/compliance:* Alert is reviewed by the appropriate surveillance officer, compliance officer and/or first line of defence control officer and found that there was a potential breach. Case is escalated to relevant parties for review, after which it was concluded that a material breach had occurred. Disciplinary action is required, delivered by the business and/or compliance.

- *Level 4 Reviewed, escalated and addressed with HR involvement:* Alert is reviewed by the appropriate surveillance officer, compliance officer and/or first line of defence control officer and found that there was a potential breach. Case is escalated to relevant parties for review, after which it was concluded that a material breach had occurred. HR is engaged by the business and/or compliance to explore disciplinary actions due to the nature of the case circumstances.

4. Proactive controls and processes

Good Practice Statement 10: *Firms should complement reactive lexicon-based monitoring by proactively performing focused review of written electronic communications on a risk-based approach, which may be complemented with random checks. All relevant parties in the organisation, regardless of seniority, are in scope of the surveillance programme. The allocation of proactive surveillance activities should be allocated to surveillance officers, compliance officers and/or business controls appropriately based on their level of authority and information access rights.*

A critical pillar of the surveillance toolkit is proactive focused review by surveillance officers of a set of written electronic communications. These reviews allow for lessons to be learnt on the effectiveness of reactive monitoring; for new risks to be identified; and for communications information to be reviewed on a more holistic basis, together with other sources of information available, such as trading alerts and compliance metrics.

The approach that firms take to sampling and the periodicity of surveillance should be proportionate to the activities and risk level of the firm. Some common examples of drivers of risk-based proactive surveillance are as follows:

- *High risk individuals*: Focused review of specific individuals; some firms may categorise individuals into risk buckets for this purpose. This may extend to review of communications around one individual for periods up to one year
- *High risk business*: Focused review of specific desks or business lines
- *High risk time periods*: Focused review of communications leading up to, during and after specific high risk time periods (e.g. bond issuances, fixing times etc.)
- *Major event*: Major event or announcement within the firm or in the industry

The above targeted proactive surveillance may also be supplemented by random sample testing of communications from across the firm as well as sample testing by business heads.

Firms should carefully consider the allocation of proactive surveillance cases or escalations to ensure that only the appropriate individuals are accessing required communications files. This requires due consideration of surveillance officers' access rights to information relative to insider lists and sensitive information etc. For example:

- *Clear access rights*: Access to communications files based on the surveillance officers' business coverage and monitoring requirements
- *Material Non-Public Information (MNPI):* Cases regarding MNPI should be allocated to individuals in accordance with the firm's MNPI Policy

Surveillance officers should be appropriately trained to conduct proactive surveillance activities.

If there are specific jurisdictional considerations firms should be mindful of any restrictions on access to data within a specific jurisdiction.

IV. Emerging practices

There are a number of areas where market practices around written electronic communication monitoring continue to evolve, driven by a combination of market-wide developments (particularly technology-related) and a transition from implementation to business-as-usual mode within individual firms. Some examples are highlighted below:

1. **Advanced analytical techniques** – Basic, single word searches typically result in a large number of false positives as they do not take account of the context of a word or different meanings etc. This can result in a large manual workload to investigate and close such alerts. More sophisticated approaches take account of the grammatical context of lexicon terms to filter out non-suspicious contexts, reducing the number of false positives and enabling increased focus on remaining alerts. Other advancements include other types of pattern or vector analysis, links to points in time (e.g. fixing windows), trend analysis (e.g. new words and terms being used by individuals, which could represent a form of code to communicate inappropriately) and network analysis (e.g. pattern changes in which individuals are communicating). It is expected that analytics in this area will continue to develop and improve, which will improve the ability to identify potentially suspicious communications and reduce the number of false positives, with implications for resources required for manual investigation of alerts.

2. **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 across written electronic communications for any given day. The level of initial alerts/flagged messages 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.

3. **Integration across surveillance areas** – There are also benefits from integration with other forms of surveillance, including trading surveillance, pricing surveillance and behavioural surveillance. An integrated approach could be more effective at identifying potentially suspicious situations based on a combination of alerts, patterns or trends across different forms of proactive surveillance, as well as providing a richer set of information for use in reactive investigation of alerts. Achieving an integrated approach is difficult due to the fragmentation of data sources and need to develop smart algorithms which recognise patterns across different areas. This is another area where developments in data management and analytical techniques are likely to enable progress over time.