Technological Challenges to Effective Market Surveillance Issues and Regulatory Tools

Final Report

THE BOARD
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR04	**APRIL 2013**

Copies of publications are available from:
The International Organization of Securities Commissions website www.iosco.org.

Contents

Chapter 1 Introduction

Background

In November 2010, the G20 Seoul Summit launched an action plan with the purpose of achieving strong, sustainable and balanced growth.[1] The commitment called for significant policy actions in several areas. Reforming the financial sector is a central element of the action plan. With the aim of enhancing the stability of financial markets, the Summit "…called on IOSCO to develop by June 2011 and report to the FSB (Financial Stability Board) recommendations to promote markets' integrity and efficiency to mitigate the risks posed to the financial system by the latest technological developments." The G20 mandate meshed closely with work that IOSCO's Technical Committee already had underway examining the emergence and impact of high frequency trading on the markets. In consequence, the Technical Committee published in October 2011 a Final Report entitled *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency*,[2] having consulted in July/August 2011.[3]

The Final Report was welcomed by the G20 and the FSB, which committed to implement the report's recommendations. In addition, a follow-on request was made that IOSCO undertake "further work by mid-2012."[4] The Chairman of the Technical Committee responded in a letter to the FSB Chairman, dated 5 July 2011, in which he stated that IOSCO would assess the new challenges that technological changes pose for regulators in their market surveillance, which include (1) the fragmentation of markets and the resulting dispersal of trading information; and (2) the increased speed of trading and regulators' ability to gather and process the increased volume of trading data.

A. Concerns Raised by the Absence of Certain Market Surveillance Tools

Securities markets have experienced a dynamic transformation in recent years. Rapid technological advances and regulatory developments have produced fundamental changes in the structure of securities markets, the types of market participants, the trading strategies employed, the increase in the speed of trading and the array of products traded. Trading of securities has become more dispersed among exchanges and various other Trading Venues. The markets have become even more competitive, with exchanges and other Trading Venues aggressively competing for order flow by offering innovative order types, new data products and other services, and through fees charged or rebates provided by the markets.

---

1 The G20 Seoul Summit Leaders' Declaration November 11 – 12, 2010 available at http://www.g20.org/Documents2010/11/seoulsummit_declaration.pdf.

2 FR09/11 *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency* Final Report. October 2011 Report of the Technical Committee, available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD361.pdf.

3 CR02/11 *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency* Consultation Report, Report of the Technical Committee of IOSCO, January 2011, available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD354.pdf.

4 Paragraph 31 of the G20 Leaders Summit Communiqué at Cannes (http://www.g20-g8.com/g8-g20/g20/english/for-the-press/news-releases/cannes-summit-final-_declaration.1557.html).

Risks posed to markets by illegal or otherwise inappropriate conduct can be substantially increased by automation, as market participants have the ability to trade numerous products and enormous volume in fractions of a second. In addition, the speed at which trading occurs impacts the ability to monitor effectively markets in the traditional sense. Moreover, because trading has become more dispersed across multiple trading centers, it has become more difficult to monitor and trace orders and transactions. These developments have also posed challenges to regulators in conducting market analysis and surveillance, and in reconstructing important trading events.

The current absence in many jurisdictions and within geographical zones of certain market surveillance tools (e.g., an audit trail system) is potentially one of the more significant problems facing the markets in light of technological developments, such as the rapid speed of trade execution and increase in order volume. Indeed, as trading strategies become more sophisticated across multiple markets and national borders, the potential for sophisticated fraud also increases. In particular, effective surveillances relating to insider trading or market manipulation can be hindered because away-market order information may not be available electronically within a reasonable time to a regulator (including a self-regulatory organization (SRO)). Some Market Authorities[5] are considering ways to deal with these issues by, e.g., consolidating surveillance data on orders or transactions in as close to real-time as reasonably possible. They believe that this could facilitate the ability of regulators to detect and review immediately aberrational activity in multiple market centers, which could significantly deter or prevent illegal or inappropriate activity.

To the degree that some SROs and/or regulators or Trading Venues may have in place certain audit trail requirements, there may be significant differences within a jurisdiction in those requirements, especially with respect to the information captured by each, the timing of receipt of the information and the breadth of the information received. To the degree that such information is even captured, it may be provided in different formats. These differences may result in inconsistent requirements imposed on Trading Venues and their members and also make it difficult to view trading activity across multiple markets. The lack of uniformity in and cross-market compatibility of, audit trails may make detection of illegal or inappropriate trading activity carried out across multiple markets and multiple products more difficult. These differences may hinder the ability of regulators to view and regulate effectively trading activity across markets within a jurisdiction and within geographical zones. The absence of uniform order and transaction data may create regulatory gaps and provide incentives for market participants to conduct activities on markets where less regulatory data is collected on an automated basis.

B. The Goals of Market Surveillance

The goals of market surveillance are primarily twofold.

One goal is to seek to ensure that trading in the given market is fair and orderly. To achieve this, market surveillance is undertaken to identify rule breaches, erroneous activity (e.g., order entry arising from a malfunctioning algorithm or *fat finger* error) or other forms of activity that may be

---

[5] In this paper, a Market Authority refers to the Statutory Regulator, a SRO or the operator of a Trading Venue, which is responsible for conducting and/or overseeing market surveillance efforts. See Section C. Report Goals and Structure, *infra*.

deemed inappropriate (e.g., the deliberate submission of excessive numbers of orders and cancellations) or disruptions to orderly trading (e.g., the *flash crash* of May 2010). Such surveillance would be expected to provide the Market Authority with sufficient information upon which the Market Authority can act to halt the given problem in a timely fashion and to provide the information necessary for a Market Authority to understand within a reasonable time the underlying causes of a material market disruption. This may involve the Market Authority communicating directly with market participant(s) whose activity gives rise to concerns. This sort of surveillance may be undertaken on a real-time basis and helps to maintain ongoing confidence in a market's orderly operation. It may also allow the Market Authority to intervene proactively – e.g., based on automated alerting functionality being built into the surveillance system – rather than being purely reactive (e.g., responding to complaints from participants).

A second goal of market surveillance is to have the ability to detect or uncover market abuse. This includes the ability to detect possible instances or patterns of market abuse and to investigate referrals from market participants and the public. The former may be undertaken in real-time through the utilization of alert functionalities built into surveillance systems to help flag suspicious activity. It may also involve non-real-time analysis, such as the running of periodic reports, or trend analysis to help detect unusual patterns of behavior over the period of seconds, hours, days or even weeks. The investigation of alerts and allegations of abuse in response to tip-offs and referrals is similarly undertaken on a non-real-time basis. In order to investigate and bring cases, it is necessary to conduct surveillance that focuses on possible centers of market abuse and on gathering relevant information of such abuse.

Both of these goals are in place to help to protect the integrity of the markets and the participants within them. IOSCO has long recognized the importance of these goals. IOSCO has identified the following three objectives of securities regulation:

- **Protecting investors;**
- **Ensuring that markets are fair, efficient and transparent; and**
- **Reducing systemic risk.**

IOSCO has expanded on these objectives by developing 38 principles of securities regulation. The IOSCO *Methodology for Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation* (the Methodology)[6] discusses these objectives and principles at length. Market surveillance is a key component to attaining the IOSCO objectives and principles of securities regulation.[7] In particular, several principles are relevant to market surveillance and an audit trail; the following are the most pertinent to this report:

- **Principle 10: The regulator should have comprehensive inspection, investigation and surveillance powers.** The Methodology states "reflecting a broad definition of enforcement, Principle 10 is designed to address whether a regulator has the powers to conduct surveillance, undertake inspections, obtain information, undertake investigations

---

6 FR08/11 *IOSCO Methodology for Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation*, IOSCO Report, September 20122. The document is available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD359.pdf.

7 Specifically, IOSCO noted in the Methodology that "matters such as thorough surveillance and compliance programs, effective enforcement and close cooperation with other regulators are necessary to give effect to all three objectives."

and take corresponding enforcement action in relation to *regulated entities* to ensure that they comply with relevant securities laws. It covers the circumstances where, and methods by which, the regulator may obtain information from those entities in the course of its inquiries. Principle 10, in particular, addresses the regulator's authority to conduct ongoing oversight and supervision of regulated entities as preventative measures."

- **Principle 12: The regulatory system should ensure an effective and credible use of inspection, investigation, surveillance and enforcement powers and implementation of an effective compliance program.** The Methodology states that "Principle 12 requires the regulator to demonstrate how the regulatory system in place, and its own organization, provides for an effective and credible use of supervisory and enforcement powers. In particular, the regulator should be able to demonstrate that there is a system to take effective inspection, investigation and enforcement actions and that, where necessary, such actions, have been undertaken to address misconduct or abuses. An effective program, for example, could combine various means to identify, detect, deter and sanction such misconduct. […]"

- **Principle 33: The establishment of trading systems including securities exchanges should be subject to regulatory authorization and oversight.** To implement this principle, IOSCO noted that, among other things, full trade documentation and an audit trail should be available to the regulator.[8]

- **Principle 34: There should be ongoing regulatory supervision of exchanges and trading systems, which should aim to ensure that the integrity of trading is maintained through fair and equitable rules that strike an appropriate balance between the demands of different market participants.** The Methodology states that "orderly smooth functioning markets promote investor confidence. Accordingly, there should be ongoing supervision of the markets."

- **Principle 36: Regulation should be designed to detect and deter manipulation and other unfair trading practices.** The Methodology states that "market manipulation, misleading conduct, insider trading and other fraudulent or deceptive conduct may distort the price discovery system, distort prices and unfairly disadvantage investors." The Methodology further noted that "the Regulator must ensure that there are in place arrangements for the continuous monitoring of trading. These arrangements should trigger inquiry whenever unusual and potentially improper trading occurs."

- **Principle 37: Regulation should aim to ensure the proper management of large exposures, default risk and market disruption. In particular, the Methodology provides that Market Authorities should have mechanisms to monitor large exposures, and have an effective compliance and enforcement system that includes surveillance of short selling activities.**

In addition, Principles 13 to 15 require that regulators should have the authority to share both public and non-public information with domestic and foreign counterparts and have mechanisms in place to do so, and that the regulatory system should allow for assistance to be provided to

[8] See Key Issue 11 under Principle 33.

foreign regulators who need to make inquiries in the discharge of their functions and exercise of their powers.[9]

C. Report Goals and Structure

The above indicates that IOSCO has already undertaken considerable work to establish principles that reflect minimum expectations with regard to market surveillance and audit trail capabilities. These minimum expectations include that the relevant Market Authorities will have the capability to:

- Conduct market surveillance on a timely basis.
- Conduct post-trade analytics.
- Reconstruct trade events (whole of market view) or be able to obtain such reconstructions from another suitable authority.
- Ensure data quality.
- Access information about particular trades/positions or any other information reasonably needed for effective market surveillance. This would also include the capability to obtain information in order to have a sensible view of larger traders in particular.
- Obtain certain minimum information fields, including audit trail data for orders and trades of equities and derivatives.

In addition, it is expected that Market Authorities will have staff sufficiently skilled to achieve the above objectives, and that their surveillance and audit trail systems are able to adapt to technological changes, including having adequate *systems capability* (e.g., the ability to keep up with the volume of message traffic). This is particularly important to facilitate market reconstructions and analyses involving numerous stocks during peak trading volume periods.[10]

It is nevertheless important, as recognized by the G20, to review existing market surveillance capabilities and audit trail quality in light of more recent technological developments and related regulatory experiences, in order to consider appropriate additional international guidance that may be helpful to improve surveillance capabilities. In response to the G20 request, IOSCO directed its Committee 2, IOSCO Policy Committee on Secondary Markets (C2), to undertake a new work project to examine the possible development of high-level principles or recommendations with respect to the development of tools to address the technological challenges to effective market surveillance. C2 was also directed to examine the development

---

[9] Further to the above, FR07/11 *Principles for the Regulation and Supervision of Commodity Derivatives Markets.* Final Report, Report of the Technical Committee of IOSCO, September 2011, established new principles that, although specific to the commodities markets, are nonetheless relevant to a consideration of principles that may guide surveillance of securities markets and the development of appropriate audit trails for trading on those markets. Principles of the Commodities Markets Report that may be relevant are cited in Appendix A. The report is available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD358.pdf.

[10] The U.S. Securities and Exchange Commission (SEC) has expressed the belief that "[a] consolidated audit trail will significantly improve the ability of regulators to reconstruct broad-based market events so that they and the public may be informed by an accurate and timely accounting of what happened, and possibly why. The sooner a reconstruction can be completed, the sooner regulators can begin reviewing an event to determine what, if any, regulatory responses might be required to address the event in an effective manner." See SEC Adopting Release for Rule 613, at http://www.sec.gov/rules/final/2012/34-67457.pdf, p. 40-41.

(and cost) of the systems/tools that would be helpful to make effective use of information relating to market transactions.

To carry its work forward, C2 circulated a survey among Market Authorities that oversee markets (IOSCO Survey). The IOSCO Survey contained questions under the following headings: Organization of Market Surveillance; Collection of Audit Trail Data for Single Asset Classes Traded on a Single Exchange; Monitoring/Analysis of Audit Trail Data; Collection and Analysis of Cross-Market or Cross-Asset Audit Trail Data Domestically/Cross Jurisdictional; and Challenges to and Cost of Monitoring.

A total of 42 responses were submitted to the survey questionnaire, broken down as follows: 21 from Statutory Regulators; 19 from Trading Venues (some of which were also SROs); and two from SROs that not Trading Venues. In terms of geographical breakdown, 10 responses were submitted from the Asia-Pacific region, 17 from Europe, and 15 from the Americas. The results of the IOSCO Survey are set forth below.

In addition, C2 met with several Trading Venues, market participants and other industry representatives to discuss current surveillance practices and the areas of concern set out in this report. Their views were also taken into consideration in the drafting of this report.

For the purposes of the survey (and this report), the scope of the project was defined to examine the trading of securities and derivatives on securities and commodities Trading Venues (as defined below). It also includes an examination of other exchange-traded financial instruments, such as corporate bonds, municipal bonds, asset-backed securities, other debt instruments. Finally, it also includes an examination of swaps in those jurisdictions where they are exchange-traded (referred to collectively in this report as the "covered asset classes" or simply as "asset classes.")

Finally, the following terms are defined for the purposes of this report:

1. **"Trading Venue"** refers to exchanges or other trading facilities, including alternative trading systems (ATSs) and Multilateral Trading Facilities (MTFs). It also refers to the operator of that particular exchange or trading facility.

2. **"Statutory Regulator"** means supervisors of the securities Trading Venues that are established by statute, but are not Trading Venue operators or self-regulatory organizations (SROs).

3. **"Market Authority"** refers to the Statutory Regulator, a SRO or the operator of a Trading Venue, which is responsible for conducting and/or overseeing market surveillance efforts.

4. **"Market Surveillance"** refers to the following broad function: monitoring Trading Venue activity using automated or manual means, and collecting and analyzing information either on a real-time, near real-time, T+1 or historical basis for the purpose of detecting, deterring and taking action with respect to disorderly markets, market "abuse" or other suspicious activity (as all defined by laws, regulations and practices within a jurisdiction) that affects the integrity of the trading or price formation process of a market.

5. **"Audit Trail"** refers to the information needed to monitor effectively market activity (orders and trades), including all records that are available to reconstruct trading activity within a reasonable time. The term may include information possessed by intermediaries, e.g., customer identifiers. However, the term does not cover the audit trail necessary to monitor intermediary compliance with conduct of business rules, or other rules focused specifically on intermediary conduct.

6. **"Cross-Asset Surveillance"** means surveillance that occurs across the covered asset classes.

7. **"Cross-Market Surveillance"** means surveillance that occurs across multiple Trading Venues trading the same securities.

8. **"SRO"** means a self-regulatory organization that is a non-governmental entity and is registered with and regulated by the Statutory Regulator. When referenced in this report, the term does not include Trading Venue operators. Exchanges that may in a jurisdiction be considered SROs are simply referred to in this report as Trading Venues, while stand-alone SROs (such as the Investment Industry Regulatory Organization of Canada -IIROC- and the Financial Industry Regulatory Authority -FINRA-) are described as SROs.

On August 22, 2012, IOSCO published its related consultative report entitled *Technological Challenges to Effective Market Surveillance, Issues and Regulatory Tools* (Consultation Report).[11] Seventeen comments letters were received from individuals, associations, markets and regulators. This Final Report discusses and incorporates, as appropriate, those comments. A complete summary of the comments and feedback statement is attached as Appendix G.

Like the Consultation Report, this Final Report examines current regulatory market surveillance and audit trail capabilities and is based upon the IOSCO Survey results, along with presentations made to C2 by operators of Trading Venues, Market Authorities and industry representatives. It considers the feasibility of additional regulatory tools to deal with the challenges arising from market surveillance, some of which may include additional audit trail or surveillance data that permits the reconstruction of trades and order books; a single reporting point for transactions within a jurisdiction; and unique entity identifiers.

[11] CR12/12 *Technological Challenges to Effective Market Surveillance, Issues and Regulatory Tools Consultation Report*. Report of the IOSCO Board, August 2012. Available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD389.pdf. The consultation period ended on 10 October 2012.

Chapter 2 Current Regulatory Capabilities

This section is divided into two parts: Part A addresses general market surveillance and data collection practices and part B addresses in particular cross-market and cross-asset surveillance and audit trail data. Although there is some overlap between the topics, C2 felt that it was important to address the latter issue separately, as cross-market and cross-asset surveillance seem to present the greatest challenges and are potentially the areas where substantial regulatory gaps that merit increased regulatory attention may exist.

A. General Market Surveillance

1. Who Conducts Market Surveillance?

Although some variability exists in the actual organization of market surveillance, the majority of jurisdictions have adopted a tiered system through which responsibility for market surveillance[12] is split among the Statutory Regulator, the SROs, and/or Trading Venues.[13] Their particular roles are described immediately below. Many of the Statutory Regulators do not monitor the markets in real-time, but can obtain information from the Trading Venues upon request.[14] Others look to Trading Venues not only to monitor the markets but also to report suspicious or wrongful conduct to the Statutory Regulator.[15] Details of regional approaches to surveillance are set forth in Appendix B.

(a) Statutory Regulator

In most jurisdictions, the legal framework and/or the Statutory Regulator establish(es) requirements for ensuring fair and orderly markets. In these jurisdictions, the Statutory Regulator plays the primary role in seeking to ensure that market rules are adequately designed to prevent manipulative and fraudulent trading practices, promote equitable principles of trade, foster cooperation with regulatory, clearing and processing entities, and protect investors and the public. In nearly all jurisdictions, the Statutory Regulator's responsibilities extend to all financial instruments and all on-venue markets, sometimes including the over-the-counter (OTC) market. Moreover, Statutory Regulators generally retain and exercise ultimate regulatory power with respect to investigating/bringing market abuse cases,[16] ensuring compliance of /Trading Venues' rules with the regulatory framework, and maintaining fair and orderly markets. Notwithstanding the above, very few Statutory Regulators engage in comprehensive, real-time surveillance of the markets and instead rely on the *front-line* surveillance roles played by Trading Venues, and SROs, as described below.

---

12 Several different functions fall within the concept of market surveillance, such as: maintaining fair and orderly markets; preventing market abuse; managing trading halts and suspensions; ensuring timely disclosure of price sensitive information; and compliance with markets rules.

13 In one jurisdiction (US), the derivatives regulator (CFTC) conducts an independent surveillance function in addition to overseeing the surveillance functions of regulated exchanges.

14 E.g., Japan: SESC; U.S. securities sector: SEC.

15 E.g., Switzerland: FINMA; Malaysia: SC; U.S. securities sector: SEC.

16 Indeed, while Statutory Regulators generally perform a supplementary role in market surveillance, they play a leading role in investigations and enforcement.

Statutory Regulators either receive or have access to order, trade, and other data for their investigations and enforcement activities. This work is largely done on a post-trade basis, although some Statutory Regulators receive audit trail data in real-time. In most jurisdictions, Statutory Regulators analyze historical information collected from SROs, Trading Venues, and/or investment firms. In addition, in some jurisdictions, market participants are encouraged to submit "suspicious transaction reports" to the Statutory Regulator and to flag possible instances of market abuse.[17] In all jurisdictions, Statutory Regulators (or SROs, where tasked with the role) receive suspicious activity referrals from Trading Venues or other market participants. Most Statutory Regulators retain some responsibility for enforcement of securities laws and civil or administrative prosecution, but domestic judicial (or other *criminal*) authorities may have separate authority to investigate and prosecute potential criminal violations arising from misconduct. Indeed, in most jurisdictions, Statutory Regulators collaborate with other domestic agencies and authorities (particularly with respect to criminal violations). Finally, Statutory Regulators often refer suspicious activity to appropriate authorities in other jurisdictions.

In a few jurisdictions, a single Statutory Regulator is responsible for carrying out both Cross-Market and Cross-Asset Surveillance on a domestic level, either on a real-time or delayed basis. In so doing, the Statutory Regulator typically consolidates data feeds and information from various Trading Venues and participants. In some jurisdictions, market surveillance is shared by more than one Statutory Regulator, depending, for example, on the nature of the instrument (e.g., cash or derivatives), the market in question (wholesale or retail markets), or the various layers in the organization of a federal state.[18]

(b) Trading Venues and SROs

Trading Venues generally have *front-line* responsibility for market surveillance. They generally enforce day-to-day compliance with regulatory requirements and market rules. The surveillance function of Trading Venues relies on the analysis of order and trade information from various sources. In some cases, this is supplemented by clearing data and position related information.

In many jurisdictions, it is the Trading Venue, in discharging the obligation to maintain fair and orderly markets, which is responsible for real-time monitoring because they are better able to deal with, respond to, and resolve situations as they arise in a live market. To monitor the market effectively, most Trading Venues monitor their markets on a real time basis, usually through automatic systems developed in-house or by third-party providers that provide alerts or post-trade

---

17 For example, the U.K.

18 In Germany, market surveillance is undertaken at both the federal and state level. At the federal level, the BaFin is responsible for the supervision of insider trading and market manipulation on and off the stock exchange, and is responsible for monitoring compliance with directors' dealings and disclosure of material information. At the state level, the "stock exchange supervisory authorities" of the Federal States, in collaboration with the Trading Surveillance Office (TSO) of a registered exchange (e.g., of the Frankfurt Stock Exchange (FSX)), supervise the orderly conduct of trading on the individual exchanges. The main duty of TSOs is to collect, record, and evaluate data regarding exchange trading and the settlement of exchange transactions. For example, the TSO of the FSX supervises price fixing and the proper conduct of floor trading as well as electronic trading via Xetra® and Eurex®. The FSX TSO analyzes irregularities and notifies the supervisory bodies and the management boards of the exchanges; it also informs BaFin of matters that fall within the BaFin's statutory responsibilities.

reports designed to identify patterns.[19] In some jurisdictions, this is done by SROs. Specifically, there are a few jurisdictions within which stand-alone SROs perform market surveillance, either on a delegated or outsourced basis or by virtue of their own regulatory mandate. In those circumstances, the SRO may monitor trading for compliance with the SRO's own rules, those of the Statutory Regulator or those of the market that has retained the SRO to perform its surveillance function.[20]

2. Cost of Surveillance Systems

In response to IOSCO's survey, only a minority of respondents provided data from which one could at least infer the costs associated with their surveillance efforts. Even then, the data provided was insufficient for IOSCO to reach any conclusions regarding costs related to performing surveillance functions. The reasons provided for not providing surveillance cost data included confidentiality requirements and the inability to separate out the surveillance cost from the respondent's overall operating cost. In light of the above, we included some questions related to the cost of surveillance in the Consultation Report.

3. How is Market Surveillance Conducted?

(a) General

As indicated, the Market Authority conducting market surveillance, whether a Statutory Regulator, Trading Venue or SRO, utilizes various tools to conduct market surveillance, which may include the use of automated systems collecting real-time or delayed data. These automated systems may issue real-time alerts or post-trade reports that identify erroneous trades, patterns of market abuse or insider trading.

Where Market Authorities have real-time, automated alerts, the main method used to eliminate false positives is to evaluate alerts regularly and, if necessary, recalibrate the applicable alert system. This is the same for T+1 reports that are automated. The experience and expertise of market surveillance staff is critical to be able to *weed out* the false positives, both where automated systems conduct monitoring and where manual monitoring is conducted without an automated system.[21]

---

19 For real-time surveillance (generally done by Trading Venues and SROs, but not Statutory Regulators) an equal number of respondents to the IOSCO survey (19) used either predominantly in-house developed market surveillance systems or predominantly third-party developed systems. For post-trade surveillance (which may also be conducted by Statutory Regulators), there were slightly more respondents utilizing an in-house system (15) compared to a third-party developed system (11). Of the few (5) respondents who had provided additional information with respect to plans for their next generation market surveillance systems, most stated their intention is to utilize a third-party system and to customize the system according to their required specification.

20 For example, in Canada, IIROC, a SRO, performs real-time market surveillance for ATSs. In addition, the equity exchanges operating in Canada have outsourced this surveillance to IIROC.

21 Some Market Authorities use *scoring* to eliminate false positives. These scoring techniques are designed to apply predetermined percentage weightings to specified attributes and thereby produce an overall score for each alert generated by the pattern in question. Depending on the selection methodology utilized for the review of alerts, those alerts at or above a certain score may be prioritized for review.

Market Authorities also collect transaction and order data for the purpose of undertaking market surveillance of their derivatives markets. In many jurisdictions, position data is also collected on a routine basis to monitor position limits and concentration risk.

While much of the surveillance is done using automated systems, some rules cannot be monitored completely or effectively through automated means and must be supported or validated by examinations of the market participant (e.g., the review of order tickets and supervisory procedures).[22] Whether suspicious activity is discovered via alerts or via manual monitoring, a Market Authority's surveillance staff will often contact traders/compliance staff at firms and ask for explanations of the suspicious behavior and/or apparent trading violations.

For those that receive real-time alerts, there is no consistency with respect to what Market Authorities do with them. Some Market Authorities review all alerts and others just review a portion. Generally, automatically generated alerts and T+1 reports are examined manually by experienced surveillance staff who subsequently evaluate the need for further analysis or investigation. Where there is credible evidence of improper behavior in some jurisdictions, the matter, if initially investigated by an SRO or Trading Venue, may be referred to the Statutory Regulator for further action.

(b) Market Surveillance of Different Asset Classes

Different assets have unique characteristics and, as a result, may require different surveillance techniques. In some jurisdictions, the applicable regulatory regime may differ depending on the asset class, e.g., cash (securities) as opposed to the derivatives markets.

For example, certain types of market abuse are dependent on:

(1) Whether it takes place on a regulated market or OTC (e.g., layering manipulation is based on a public order book);

(2) Whether it involves physical assets and delivery issues (e.g., commodities manipulation); and

(3) On the liquidity and the efficiency of the market (e.g., bonds).

As a result, there may be certain alerts or reports that are only run on specific asset classes. In addition, there may be different parameters, pricing models, algorithms, and thresholds for

---

[22] Some examples provided by Market Authorities of activities that must be monitored manually include:
(1) Trading related to futures expiry and index re-balancing, which the ASX (Australia) monitors as part of ensuring that its market is orderly. These activities occur infrequently but are too complex to program into a system. Consequently, they are only monitored manually by specialized staff members;
(2) Reports that track the trading being conducted by insiders;
(3) Extended trade settlement failure (trades that fail to settle within ten days of the regular settlement date);
(4) Certain rule violations such as: (a) The failure to properly designate a short sale; the failure to properly designate an inventory/proprietary trade; or the failure to properly identify a trade as jitney, etc.; or (b) Rules of the U.S. exchanges that operate physical trading floors that govern trading behavior of members operating on the floors. Such rules must be reviewed through an examination program;
(5) Trading of illiquid assets where trading occurs infrequently;
(6) Trade adjustments; and
(7) Reviews relating to the time that a decision was made to exercise or not exercise an option.

derivatives in the alerts. For example, some alert/behavioral modules are generic, i.e., they can be effectively used for both cash and derivatives markets, while others are used for derivatives only (e.g., volatility or open interest related modules).

(c) Monitoring High Frequency Trading (HFT)

HFT is a phenomenon in the financial markets that gives rise to high volumes of activity and messaging and has, in the last several years, garnered substantial international attention.[23] HFT poses potential challenges to existing surveillance systems; for instance, can surveillance databases handle the volume of information generated by HFT, and are surveillance alerts suitable (and suitably calibrated) for this type of trading?

In many cases, there is no difference between the monitoring conducted for HFT and the monitoring done with respect to trading generally. In particular, many Market Authorities have indicated that their real-time surveillance is focused on all types of electronic trading.

In jurisdictions where Market Authorities conduct real-time surveillance, the Market Authority generally receives alerts relating to looping algorithms, order-to-trade ratios, unusual order and trade alerts, and pattern recognition. Some Market Authorities have, or are developing, specific alerts that are more tied to low latency trading, such as layering, quote stuffing, momentum ignition, and other pattern recognition alerts.

Recently, in some jurisdictions there have been new regulatory requirements introduced or proposed or guidance provided on existing requirements that:

---

[23] See FR09/11 *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency* Final Report. Report of the Technical Committee of IOSCO, October 2011 (*Market Integrity Report*), p. 22 - 23, available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD361.pdf. HFT does not lend itself to a universally accepted definition. As stated by IOSCO, however, HFT is frequently equated to algorithmic trading. However, while HFT is a type of algorithmic trading, not all forms of algorithmic trading can be described as high frequency. Algorithmic trading predates HFT and has been extensively used as a tool to determine some or all aspects of trade execution like timing, price, quantity and venue. Algorithmic trading is used by many intermediaries for their own proprietary trading or offered to their clients and has also become a standard feature in many buy-side firms, mainly with the purpose of devising execution strategies that minimize price impact or to rebalance large portfolios of securities as market conditions change. Nonetheless, a number of common features and trading characteristics related to HFT can be identified. These characteristics include:

(1) The use of sophisticated technological tools for pursuing a number of different strategies, ranging from market making to arbitrage;
(2) Employment of algorithms along the whole investment chain: analysis of market data, deployment of appropriate trading strategies, minimization of trading costs and execution of trades;
(3) A high daily portfolio turnover and order to trade ratio (i.e., a large number of orders are cancelled in comparison to trades executed);
(4) Flat or near flat positions at the end of the trading day, meaning that little or no risk is carried overnight, with obvious savings on the cost of capital associated with margined positions. Positions are often held for as little as seconds or even fractions of a second;
(5) Mostly employed by proprietary trading firms or desks; and
(6) Latency sensitive.

The implementation and execution of successful high frequency trading strategies depend crucially on the ability to be faster than competitors and to take advantage of services such as Direct Electronic Access (DEA) and co-location. See *Market Integrity Report* at p. 22-23.

(1) Require more information to be provided to Market Authorities on algorithms and their strategies;

(2) Introduce more requirements related to *fair and orderly trading*; and

(3) Place more responsibility on those using algorithms to trade.

For example, in Europe, the European Securities and Markets Authority (ESMA) published guidelines on *Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities*.[24] Some Statutory Regulators and SROs are also conducting studies that will attempt to examine and measure the impact of HFT on market quality and market integrity, including volatility.[25]

There are only a few jurisdictions that can or will be able to monitor trading by HFT firms using real-time alerts or automated post-trade reports across multiple Trading Venues.[26] For example, while FINRA has not developed a specific regulatory program solely to oversee HFT activity,[27] it nonetheless has multiple automated surveillance patterns that will assess HFT activity along with that of other market participants engaging in the same conduct that the pattern is designed to detect.[28] In addition, as a result of FINRA's regulatory services agreements (RSAs) with the NYSE in June 2010, FINRA developed a cross-market initiative. In particular, FINRA is in the process of developing a suite of comprehensive cross market surveillance patterns that leverage and build upon existing patterns that will run against a combined data set from all markets overseen by FINRA (i.e., markets operated by the NYSE and NASDAQ).

---

24 European Securities and Market Authority Guidelines: Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities, 24 February 2012 | ESMA/2012/122 available at: http://www.esma.europa.eu/system/files/esma_2012_122_en.pdf.

25 Italy: CONSOB; Australia: ASIC; Canada: IIROC; U.S.: CFTC.

26 E.g., Australia; Canada (IIROC); and U.S. (securities sector: FINRA). For example, IIROC in Canada can generally track HFT firm trading either through marketplace participant identifiers or DMA client identifiers.

27 FINRA's automated surveillance patterns are conduct-driven scenarios and largely agnostic to the type of market participant in question, outside of those designed to monitor particular behaviors or obligations of registered market participants (i.e., registered market makers).

28 Using a working definition of HFT activity as "any technology-enabled trading strategies that are generally focused on liquidity provision or the detection of minute market inefficiencies or trading patterns that are utilized by entities trading on a proprietary basis and characterized by extremely high order entry and cancellation rates, as well as rapid turnover of positions (usually small in size) obtained through such trading," FINRA has multiple automated surveillance patterns that can be used to detect suspicious activity conducted by member firms and their customers that fall under this definition. It should be noted, however, that FINRA's surveillance alerts for market abuse, including HFT type manipulation, are generated in non-real-time. Oversight of HFT-type firms is included in and accomplished through its multiple surveillance patterns that can detect firms that appear to be engaged in manipulation or fraud in connection with the use of so-called *momentum ignition strategies*, or other *layering activity* that HFT traders may use, among other activities that could be potential violations of FINRA, client exchange, or SEC rules. Similarly, the French AMF does not have at this stage any automated alert targeting specifically potential abuses undertaken by HFT firms; it has, however, implemented detection tests (e.g., layering) for abuses undertaken on a high frequency as well as in a more *classical* manner.

B. Audit Trail Data

The collection of data is closely integrated with how market surveillance is conducted. There are various ways that data is collected – and there is little consistency across jurisdictions. For example, some jurisdictions collect orders and trades, others collect just trades. In some jurisdictions, data is collected in real-time, in others it is not. There is also wide variation regarding what data is actually collected. This section summarizes some of the findings of C2 in relation to the collection of audit trail data.

1. Sources and Types of Audit Data Collected

Trading Venues or SROs generally collect their audit trail data internally through trading or surveillance systems on a real-time basis. In the case of Statutory Regulators and some SROs, audit trail data is collected from various sources including: Trading Venues, market participants, investment firms, clearinghouses, settlement facilities, and other data providers (e.g., Bloomberg, Reuters or IRESS). The type of audit trail data collected and used by Market Authorities varies across the jurisdictions depending on the nature and scope of their respective market surveillance functions within their jurisdiction. Appendix C provides further details on the audit trail data that is collected by Statutory Regulators and some SROs in each jurisdiction. Appendix D provides a list of the typical audit trail data *fields* that are collected by Statutory Regulators and some SROs.

2. Collection, Timing and Use of Audit Trail Data

The nature and scope of the market surveillance function undertaken by Market Authorities within each jurisdiction influence whether audit trail data is collected on a real-time, near real-time (e.g., T+1), or historical basis. For example real-time data is generally used to monitor trading activities for unusual trading patterns including erroneous and anomalous trades caused by trade error, or malfunctioning algorithms.[29] While in most jurisdictions the Trading Venue would collect this data, in some jurisdictions the Statutory Regulator and SRO receive real-time electronic data feeds of these trading activities.

In most jurisdictions, automated systems are used to collect and monitor this real-time order and trade information. These automated systems generate real-time alerts and post-trade reports,[30] which detect unusual activity. Alerts, or, in some jurisdictions, a sample of the alerts, are then manually investigated by experienced surveillance staff and where the alert is generated by the

---

[29] In addition, the timing of data collection a may depend on its source. In particular, there are differences between Market Authorities with respect to whether the information from particular ***sources*** is collected in real-time. The AFM (Netherlands), for instance, collects all data, no matter what the source, in real-time. IIROC collects real-time data from exchanges and ATSs. In contrast, the SFC (Hong Kong) receives most trading data in real-time but must request clearing information and client level information. Similarly, the CONSOB (Italy) has access to order book data in real-time, and receives information on trades executed from banks and investment firms by T+2 and from non-domestic banks and investment firms by T+3. Most SROs note that they do not typically receive audit trail data from sources other than their own individual market (e.g., U.K.: PLUS Markets Group). With respect to derivatives markets, market operators/Trading Venues and Statutory Regulators generally use near real-time and T+1 data for monitoring trading activities and position limits.

[30] The real-time alerts generated may relate to price, volume, large position alerts, "marking the close," wash sales, trade throughs, pre-arranged trades, collusion, front running, algorithmic manipulation, double printing, spoofing, layering and/or quote stuffing.

system at a trading venue, may be referred to a Statutory Regulator for further investigation and analysis.[31]

In addition, some Market Authorities have automated surveillance systems that run post-trade reports on a T+1 or later basis. These reports may be used to identify patterns or particular scenarios (e.g., front-running or layering). Specifically, the reports may be used to identify:

- Potential insider dealing.
- Anything unusual in relation to participants such as volumes or trading patterns.
- Switching sides during, and subsequently trading, following an auction.
- Self-executions or wash trades (i.e., the same counterparty on both sides).
- Order book layering activity.
- Erroneous orders.[32]
- Manipulation of closing prices and auctions.
- The quality of trade reporting or the timeliness of trade reports (e.g., using correct information within trade reports or identifying delayed trades, etc.)
- Monitoring of settlement positions.

3. Time-Stamp

The role of a time-stamp is to establish evidence indicating that data existed or an event took place at a particular time. As such, it is an essential component of any surveillance system, especially for ensuring compliance with time sensitive regulatory requirements such as trade-through obligations or front running.

All jurisdictions have time-stamps attached to their audit trail data. Audit trail data time-stamps generally range from one nanosecond to one-second accuracy, although most are accurate to one millisecond. As most Statutory Regulators, Trading Venues and SROs collect their audit trail data for various purposes and from various sources, including multiple markets and member firms, the time-stamps attached to the information they collect may vary in precision.

Generally, Trading Venues' trading or surveillance systems automatically assign time-stamps. However, some SROs (e.g., Canada: IIROC; U.S. securities sector: FINRA) and regulators (e.g., Australia: ASIC) also attach a separate time-stamp to the data that they have received in real-time, usually based on their own system time.

To ensure the maintenance of accurate time-stamps, Market Authorities have integrated time synchronization into their system architecture. The mechanisms and sources for clock synchronization, however, vary between jurisdictions and are set forth in Appendix E.

---

[31] These systems may also reside in either the Statutory Regulator (Australia, France) or SROs (Canada, U.S.) or both (U.S. CFTC). However, in most jurisdictions, the Trading Venues perform this function for their particular market.

[32] IOSCO published *Policies on Error Trades*, Final Report, Report of the IOSCO Technical Committee, October 2005, available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD208.pdf.

4. Data Formats

Statutory Regulators and SROs collect audit trail data in electronic and, to a lesser extent, hard copy formats, depending on the type of data collected and the source. The most common formats for collecting audit trail data include CSV, PDF, XML, TXT, Excel, and *flat file*.[33] Trading Venues generally collect audit trail data from their trading engines in raw format; it is subsequently converted into proprietary data formats. The audit trail data that is collected by Market Authorities is usually uploaded onto a structured database (e.g., Oracle and SQL) for storage and future extraction/analysis.

Market Authorities maintain audit trail data for varying periods of time. Typically, audit trail data is stored for between five and ten years, with most storing data for five years.[34] In some jurisdictions, the length of time audit trail data is required to be stored is specified by statutory or regulatory policy (e.g., Canada, Singapore and Switzerland).

Due to the volume of audit trail data that is required to be stored, some jurisdictions have adopted the practice of storing the most current audit trail data in online databases (to ensure data can be quickly extracted if necessary) and archiving older data. While the archived data can be restored if necessary, restorations can take up to two to three days. For example, the ASX (Australian Securities Exchange) keeps raw audit trail data online in a compressed form for 30 days before the data is archived; archives are kept for a minimum of seven years.

5. Integrity and Quality of Data

All jurisdictions have processes and procedures in place that seek to ensure the quality and integrity of the audit trail data they collect, with various checks usually being undertaken at the Market Authority level. In some jurisdictions, error handling is built into their systems to detect incorrect data.[35] The Market Authority may also perform quality checking of the data to ensure the fields are populated correctly, or check the audit trail data against other sources, including vendor data or information provided by market participants.[36] Other methods include exception logging[37] as well as reviewing compliance by firms during compliance reviews.[38] In general,

---

33 Several Market Authorities have developed a bespoke format to standardize the transaction reports it receives from investment firms it authorizes/regulates.

34 However, a few respondents have indicated that they currently store audit trail data indefinitely (e.g., U.K: ICE Futures Europe; India: SEBI).

35 For example, in the U.K., market operators such as the LSE, BATS Europe, ICE Futures Europe, PLUS Markets, and Turquoise have *error handling* built into their audit trail mechanisms to detect trade or quote information which appear to be incorrect (e.g., alerts are triggered when orders or trades are incorrect; data is validated during overnight data processing to identify errors, missing, or duplicate data), while the FSA also performs quality checking of the audit trail data its receives to ensure fields have been populated correctly.

36 In Australia, although market operators/Trading Venues are responsible for ensuring the reliability of their audit trail data under the ASIC Market Integrity Rules, ASIC frequently compares the data in its integrated market surveillance system against other sources, including secondary data vendors and information provided by market participants and market operators/Trading Venues.

37 In Canada, the IIROC relies on a combination of real-time exception logging (at the gateway level as well as the SMARTS converter level) and off-line validation to ensure the quality and integrity of the data being provided by each market (e.g., various business logic, conditionally required field checking, etc.). In addition, the trade, order, and quote count totals for each market generated from the messages received in

when an error in the audit trail data is discovered, Market Authorities attempt to correct the data by reaching out to the source(s) of the problematic data so that the audit trail data is complete and accurate.[39]

6. Maintaining the Confidentiality of Audit Trail Data

Jurisdictions have implemented a variety of security protocols that seek to ensure the confidentiality of audit trail data. The measures taken include:

- Transmission and receipt of data using dedicated lines in a secure environment.
- Restricting internal access/use of the data to a small group of relevant employees/users with passwords and routine reviews/audits of users.
- Monitoring access to audit trail data.
- Confidentiality agreements with employees.
- Use of a secure environment to request and receive additional information.
- Segregation of the market surveillance function from the rest of the organization.
- Restricting the external transmission of data to limited user groups and only in response to federal or regulatory inquiry (e.g., domicile regulator, offshore regulator, Intermarket Surveillance Group (ISG) members).
- Utilizing firewalls to prevent external access; and
- Safeguarding information sharing by encrypting the information in password-protected files.

7. Market Participant and Customer Identifiers

(a) Market Participants

All jurisdictions currently use direct market participant (member) identifier codes (e.g., for intermediaries), which are generally assigned by the Trading Venue. In some jurisdictions with multiple Trading Venues, such as the U.S. and U.K., a single broker-dealer may have multiple market participant identifiers assigned to it by multiple Trading Venues, depending on the

---

the IIROC's primary environment are compared to those received in the backup environment to ensure the IIROC is receiving the same information in both environments. This process is automated through the use of a script.

[38] In the U.S., with respect to data received directly from FINRA members (i.e., registered broker-dealers), FINRA conducts surveillance of members to discern whether the firms are complying with their reporting obligations. In addition, FINRA also conducts an extensive on-site examination program at firms; a significant part of this risk-based examination program relies on statistically validated sampling techniques aimed at determining whether the firms are meeting their reporting obligations. Under the terms of the contract between FINRA and its SRO RSA-client exchanges, the client exchanges that submit data for use in FINRA's market surveillance are obligated to meet certain standards related to the accuracy, timeliness, and completeness of the data submitted. Finally, FINRA conducts various internal daily, automated data checks to validate the accuracy, timeliness, and completeness of the data being processed.

[39] For example, for the LSE (U.K.), if orders and/or trades are incorrect (i.e., outside of certain prescribed parameters), an alert will be generated in the surveillance system which will subsequently be investigated by one of the real-time market analysts. Once a suspected error has been confirmed to be incorrect, the LSE will contact the relevant member firm and take the appropriate action.

securities traded, the markets on which they are traded, and the number and functions of trading desks within a particular broker-dealer.[40]

In contrast, Canada and Australia require the same market participant identifiers to be used across multiple markets. In Canada, the Trading Venue or IIROC assigns a particular market participant identifier for trading on all equity markets; and the Montreal Exchange (MX) coordinates the assignment of a Unique Market Participant identifier with IIROC if a new approved participant is not already a participant of an equity market. Similarly, in Australia, Trading Venues are obliged under Australia's Market Integrity Rules to use a common unique identifier for a participant in multiple markets. In the United States, Rule 613, adopted by the SEC in July 2012, [41] provides that the National Market System (NMS) plan required to be submitted by the SROs pursuant to the Rule for consideration by the SEC must require that SROs and broker-dealers report a CAT-Reporter-ID that uniquely identifies the SRO or broker-dealer, for each reportable event that the member or SRO is reporting to the central repository.

(b) Identifiers for Customers

(i) C2 Member Approaches to Customer Identifiers

In some jurisdictions, the audit trail requirements include the requirement to provide a unique customer identifier.[42] Typically, the customer identifier does not identify the ultimate customer should the first-level customer be a firm acting for another customer or a foreign entity. In other jurisdictions, a customer identifier is not included in the electronic audit trail, but is available on request.

Below is a description of some of the approaches taken in different jurisdictions:

- The CFTC's large trader reporting system (LTRS) collects daily information on beneficial ownership of reportable futures positions. Since traders frequently carry futures positions through more than one reporting firm and since individuals sometimes control, or have a financial interest in more than one account, the CFTC routinely collects information that enables its surveillance staff to aggregate related accounts. Reporting firms must file a form, which identifies each new account with reportable positions for each futures contract. In addition, if a trader's position reaches a reportable level, the trader may be required to file a more detailed identification report to identify accounts and reveal any relationship that may exist with other accounts or traders.
- In July 2011, the U.S. SEC adopted a new rule establishing large trader reporting requirements to enhance its ability to identify large market participants, collect information on their trading, and analyze their trading activity. In particular, the rule requires large traders to identify themselves to the SEC, which will then assign each large trader a unique identification

---

40 In the U.K., identifiers are may also allocated at the trade group level (*second-level identifier*). A firm may have one or multiple trade groups allocated to the firm depending on its connectivity requirements and its business/organizational arrangements. In the U.S. securities sector, the exchanges also provide the identifiers to the broker-dealer for their *re-assignment to their customers* (so-called *sponsored access*). Similarly, in Hong Kong, the HKEx allocates identifiers at the broker-terminal level (e.g., a particular user group of the firm).

41 See footnote 10, *supra*.

42 In the U.S. securities sector, the exchanges also provide the identifiers to the broker-dealer for their *re-assignment to their customers* (so-called *sponsored access*).

number. Large traders must provide this number to their broker-dealers, who will be required to maintain transaction records for each large trader and report that information to the SEC upon request. In addition, Rule 613[43] provides that the NMS plan that must be submitted by the SROs pursuant to the Rule for consideration by the SEC must require every member of an SRO to report a unique customer identifier to a central repository upon origination or receipt of an order. Rule 613 defines *customer* as the account holder(s) of the account at a registered broker-dealer originating the order and any person from whom the broker-dealer is authorized to accept trading instructions for such account, if different from the account holder(s).

- In Hong Kong, for many years, it has been a statutory requirement for a person who holds or controls a reportable position in futures and options contracts to notify the relevant authority of that reportable position. This large positions data (up to ultimate client level) enables the authority to monitor market activities more effectively.

- In Canada, direct market access (DMA) clients, including sponsored access participants, must be assigned a unique client identifier. However, a DMA client who holds accounts at two separate dealers will have two separate identifiers. IIROC receives data that identifies all of the identifiers and matches all numbers to the specific client. With respect to clients that do not access markets through DMA, IIROC and the MX are not able to identify immediately the ultimate customer of an order with their real-time data feed. Both IIROC and MX can, however, retrieve client information on a post-trade basis from firms in a proprietary format, which allows the IIROC to match client data to order/trade data using a proprietary system called MICA.

- In 19 out of 29 European jurisdictions (27 EU plus Norway and Iceland), *client* information currently can be required in transaction reporting.[44] In the U.K., client information has been reported to the regulator since 1990. However, they are unable immediately to identify the ultimate customer if the customer (i) is not a European investment firm, or (ii) is a retail customer of an agent trader. As part of MiFID II, the European Commission has proposed revisions to the content of existing transaction reporting requirements, including a requirement to identify the customer who is making the underlying investment decision, and perhaps the individual trader involved.[45]

- In Australia, ASIC's equities surveillance audit trail system does not identify trades under common ownership and control or identify the ultimate customer connected with an order. As the Trading Venues in Australia provide a number of free text fields for market participants to use at their discretion, ASIC, in collaboration with market participants, is often able to infer from these fields the source of the audit trail flow, but not with any certainty.

- In Brazil, the identification of the accountholder of a trade is mandatory and must be sent to Trading Venues by the market participant by T+0 (derivatives) or T+1 (cash market). In the audit trail data, it is possible to identify a customer by his/her account number or tax ID number.

---

43 See footnote 10, *supra*.

44 See: http://www.esma.europa.eu/system/files/10_808_Technical_Advice_MiFID_Review_Transaction_Reporting.pdf.

45 In Germany, the transaction reports collected by the BaFin on all securities transactions from credit and financial services institutions include the identifier for the securities account holder/the securities account and an identifier for the executing firm (unless this is identical to the securities account holder). In Spain, existing audit trails facilitate identification of the client associated with a particular trade execution. A tax ID identifies Spanish natural or legal persons. Foreign investors are identified by their name and, in accordance with domestic law, are considered *ultimate* owners since there is no recognition of the nominees in its domestic legal framework.

- In India, SEBI has mandated that every client trading on stock exchanges should have a unique identity number, PAN (Permanent Account Number), which is also mandatory for holding shares in a deposit account. This helps to identify ultimate customer who has traded or is holding shares. If trading is done through foreign institutional investors, their PAN is also captured in the database. Furthermore, if these investors issue any offshore derivative instruments, such instruments are to be issued only after compliance with 'know your client' norms and details thereof are also required to be submitted to SEBI periodically.

(ii) International Initiatives

1. FSB Legal Entity Identifier Expert Group

The financial crisis renewed interest in the development of a global legal entity identifier (LEI) system and led the G-20 to mandate the FSB to lead the co-ordination of international regulatory work and to deliver concrete recommendations on a LEI system by June 2012.[46] The FSB has stated that there is widespread agreement among public authorities and financial industry participants on the merits of establishing a uniform global LEI[47] system that will uniquely identify parties (other than natural persons) to financial transactions.[48]

An "expert group of key stakeholders" with a mandate to deliver clear recommendations with respect to the implementation of a global LEI system to the FSB Plenary for endorsement[49] prepared a report[50] that provides an initial set of 35 recommendations. Those recommendations are set forth in Appendix F.

2. IOSCO-CPSS (Committee on Payment and Settlement Systems)

In the *Report on OTC Derivatives Data Reporting and Aggregation Requirements* (IOSCO-CPSS

---

46 'We support the creation of a global legal entity identifier (LEI) which uniquely identifies parties to financial transactions. We call on the FSB to take the lead in helping coordinate work among the regulatory community to prepare recommendations for the appropriate governance framework, representing the public interest, for such a global LEI by our next Summit.' (Cannes Summit Final Declaration, 4 November 2011).

47 It has also been defined as a standard reference code that would provide a universal method of identifying entities, including both financial and non-financial firms.

48 In the FSB's view, an LEI system would provide a valuable 'building block' to contribute to and facilitate many financial stability objectives, including: improved risk management in firms; better assessment of micro and macro-prudential risks; facilitation of orderly resolution; containing market abuse and curbing financial fraud; and enabling higher quality and accuracy of financial data overall. It would reduce operational risks within firms by mitigating the need for tailored systems to reconcile the identification of entities and to support aggregation of risk positions and financial data, which impose substantial deadweight costs across the economy. It would also facilitate *straight through* processing.

49 Recommendations were requested with respect to a governance framework for global LEI, an operational model, scope of LEI reference data, access and confidentiality, funding model, and implementation and phasing.

50 *A Global Legal Entity Identifier for financial markets*, Report to the FSB Steering Committee, June 2012, available at: http://www.financialstabilityboard.org/publications/r_120608.pdf. The Report was prepared by an *ad hoc* FSB LEI Expert Group from key stakeholders within the global regulatory community. Membership of the Expert Group comprised representatives from both FSB members and key non-members from the global regulatory community with a major stake in the initiative, such as the CFTC and ESMA.

Report),[51] an IOSCO-CPSS Task Force examined the issued raised by the possible development of LEIs to be used as a tool for data aggregation in the context of OTC derivatives trading (e.g., identifying counterparties to an OTC trade). At present, names or codes having several variations may actually reference a *single* firm, but an automated system may interpret these as references to *different* firms. The Task Force observed that the use of a standard, universal (i.e., global), alphanumeric reference code would therefore facilitate and improve the ability of authorities to attribute properly OTC derivatives activity to a party or group, in particular to identify counterparties to OTC derivatives transactions or other financial transactions, or that issue securities or other assets that are the subject of financial transactions.

The IOSCO-CPSS Report recognized that the principal challenge regarding identification of legal entities is that currently no global legal entity identification system is in use across the financial sector and regulatory community. In the absence of such a universal system, private firms and authorities have created a variety of limited or proprietary identifiers. The Task Force recommended the expeditious development and implementation of a standard LEI that is capable of achieving the data aggregation purposes discussed in its report, suitable for aggregation of OTC derivatives data in and across trade repositories (TRs) on a global basis, and capable of eventual extension to identification of legal entities involved in various other aspects of the financial system across the world financial sector. In order to promote harmonization of legal requirements for use of LEIs across different jurisdictions as phased implementation of LEIs occurs, and to help ensure that LEIs can facilitate aggregation of OTC derivatives data, the Task Force recommended that national authorities issuing or considering legislation or regulations requiring use of LEIs should take five basic principles into account. The five principles include:

> (1) *Uniqueness*: only one LEI should be assigned to any legal entity, and no LEI should ever be reused. Each entity within a corporate organization or group structure that acts as counterparty in any financial transaction should have its own LEI;
>
> (2) *Neutrality*: to ensure the persistence of the LEI, it should have a format consisting of a single data field, and should contain either no embedded intelligence or as little embedded intelligence as practicable. Entity characteristics should be viewed as separate elements within a reference data system that would be available to authorities to enable data aggregation needed to fulfill their regulatory mandates;
>
> (3) *Reliability*: the LEI should be supported by a trusted and auditable method of verifying the identity of the legal entity to which it is assigned, both initially and at appropriate intervals thereafter. The issuer of LEIs should maintain minimum reference or identification data sufficient to verify that a user has been correctly identified. Issuance and maintenance of the LEI, and storage and maintenance of all associated data, should involve robust quality assurance practices and system safeguards;
>
> (4) *Open Source*: the schema for the LEI should have an open standard, in order to

---

[51] *Report on OTC derivatives data reporting and aggregation requirements*, Report of the CPSS and the Technical Committee of IOSCO, April 2012, available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD356.pdf p. 28.

ensure to the greatest extent practicable that the LEI is compatible with existing automated systems of Financial Market Infrastructures (FMIs), market participants, and authorities, among others; and

(5) *Extensibility*: the LEI should be capable of becoming the single international standard for unique identification of legal entities across the financial sector on a global basis. Therefore, it should be sufficiently extensible to cover all existing and potential future legal entities of all types that may be counterparties to OTC derivative or other financial transactions, may be involved in any aspect of the financial issuance and transactions process, or may be subject to required due diligence by financial sector entities.

C. Cross-Market and Cross-Asset Surveillance and Audit Trail Data

The scope of the products and instruments monitored and the audit trail data collected varies among Market Authorities. In general, the key purpose of such monitoring and data collection is to detect potential breaches of market abuse regulations.[52] This section discusses Cross-Asset and Cross-Market Surveillance conducted within individual jurisdictions.

1. Monitoring Multiple Trading Venues

The approach to monitoring multiple Trading Venues within a jurisdiction varies. In some jurisdictions, multiple listings or trading on multiple markets is not permitted.[53] As a result, Cross-Market Surveillance is not an issue. In other jurisdictions, Trading Venues only monitor their own market.[54] Other Market Authorities are moving towards having a system that will allow for Cross-Market Surveillance domestically, but do not currently have such a system.[55]

Certain Market Authorities consolidate order and/or trade information across domestic Trading Venues to monitor those markets. In particular, IIROC in Canada (for equity trading) and ASIC (Australia) collect order and trade information across all Trading Venues operating in their jurisdiction in real-time.

The German BaFin receives and consolidates transaction data across domestic Trading Venues.[56] The SEBI (India) relies on the Trading Venues to *inter-link* across markets and products so as to avoid regulatory arbitrage. The Trading Venues in India are also required to coordinate and uniformly implement new policies related to inter-linkages and market surveillance.

---

52 For example, in the U.S. securities sector, SROs use cross-market data for review "beyond the scope of trading on the exchanges" (U.S. securities sector: Direct Edge). That is, the information is used to identify when a member of a particular exchange "locked or crossed another market's quotes or traded through another market" (e.g., U.S. securities sector: Direct Edge, ISE). The ISE (U.S. securities sector) notes that cross-asset audit trail information is used primarily to detect front running reviews "when an options trade precedes an equity trade."

53 E.g., Mexico: CNBV; Brazil: CVM; Hong Kong: SFC.

54 E.g., U.K.: IFEU, LIFFE, LME, LSE, TGHL; Netherlands: NYX, TOM MTF; Japan: TSE; Singapore: SGX, SMX.

55 E.g., U.K.: BATS Europe, Chi-X Europe.

56 Transaction data must be submitted to BaFin not later than the next working day after conclusion of the transaction.

Many of the surveillance patterns used to monitor activity in U.S. exchange-listed equity securities utilize audit trail data from multiple markets, including consolidated quote and trade data and the ISG audit trail data. With respect to monitoring conduct simultaneously across multiple markets, in conducting market surveillance, one of FINRA's main objectives is to integrate audit trail data from as many markets as possible to obtain the most comprehensive view of overall market activity by market participants, who may disperse their activity across the various exchanges, ATSs, and other trading centers operating in the United States. FINRA has therefore sought to integrate audit trail information from the quotation and trade reporting facilities it operates with the audit trail information that has become available to it through its entry into RSAs, to perform market surveillance services for U.S. exchanges. Finally, NASDAQ collects and stores all of its trading system internal data, which includes all order and execution data.

2. Monitoring Across Assets

A majority of Market Authorities have jurisdiction over most conventional financial products including listed securities, warrants, derivatives (options and futures), and exchange-traded funds.[57] For some Market Authorities, derivatives are typically monitored or analyzed with the underlying instrument,[58] i.e., they have a system that links derivative products to the underlying security, which facilitates monitoring across markets and products.[59] These systems often use a field in the Market Authority's database that defines the underlying of the derivative.[60] In contrast, other Market Authorities only monitor products traded on their specific Trading Venue[61] and/or perform cross product analysis on a case-by-case basis.[62] The CFTC (U.S. derivatives sector), for instance, aggregates positions in related contracts based upon the judgment of its surveillance staff.

In some jurisdictions, market surveillance is conducted across asset classes. In particular, the SEBI (India),[63] ASIC (Australia), U.S. CFTC, and most of the U.S. exchanges claim that they monitor across assets as well as across markets. In contrast, Canada splits its surveillance between assets.[64]

---

57 E.g., Australia: ASIC; Germany: BaFin; France: AMF; U.K.: BATS Europe, Chi-X Europe; India: SEBI; Hong Kong: SFC; U.S. securities sector: FINRA.

58 E.g., France: AMF; Japan: TSE.

59 E.g., Australia: ASIC; Germany: BaFin.

60 E.g., Brazil: CVM; Germany: BaFin. FINRA's system (U.S. securities sector) is capable of detecting manipulative activity between the equities and options markets including anticipatory hedging, pegging/capping, and layering.

61 E.g., U.S. securities sector: BATS; Singapore: SGX; U.K.: PLUS.

62 E.g., Canada: IIROC and the MX; Spain: CNMV; Italy: CONSOB.

63 In India, SEBI receives data from its stock exchanges for various assets (such as equity, equity derivatives and currency derivatives). SEBI monitors through its internal surveillance system across assets and across markets, although *not* in real-time. Stock exchanges are responsible for real-time surveillance and monitoring.

64 Specifically, IIROC monitors securities markets across all equity domestic exchanges while the MX, the only Canadian market for financial derivatives, monitors all financial derivatives activities. Neither IIROC nor the MX conducts real-time cross-asset surveillance, although they seek to coordinate their surveillance efforts.

Most Market Authorities do not monitor non-listed products. The IIROC (Canada) is in the early stages of developing a system to capture transaction data on fixed income products; and some provinces require the reporting of trades of unlisted equity securities. The U.S. CFTC (derivatives sector) noted that although it does not currently monitor OTC derivatives, it would on occasion make *special calls* to large traders when there is a need to assess the nature of such a trader's overall positions and market intentions. FINRA conducts electronic surveillance of the U.S. OTC markets for unlisted equity securities and corporate debt. Indeed, FINRA provides post-trade transparency for executed transactions in these OTC instruments and uses the transaction audit trail data to conduct surveillance.

3. Domestic (including EU) Single Reporting Point for the Audit Trail[65]

Jurisdictions vary as to whether (and how) they have implemented a single reporting point for the centralization of data associated with market activity, including with respect to the nature of the data that must be reported. In some jurisdictions, this is referred to as a *Central Reporting Point*. Currently, it appears that most jurisdictions that require data to be reported domestically to a single reporting point require the reporting of transaction (trade execution) data.

On 11 July 2012, the U.S. SEC approved a rule that requires U.S. exchanges and FINRA to jointly submit a comprehensive plan detailing how they would create, implement, and maintain a consolidated audit trail that must collect and accurately identify every order, cancellation, modification, and trade execution for all exchange-listed equities and equity options across all U.S. markets.[66]

A few jurisdictions, such as IIROC (Canada), ASIC (Australia), AMF (France) and SEBI (India), stated in their responses to the survey that they have a single reporting point and "integration of the data."[67] Others have a single reporting point, but there is no formal integration of the data collected.[68] For example, in Europe, all Statutory Regulators within the European Economic Area receive transaction data from other European Market Authorities, although it is usually restricted to executed trades in instruments that trade primarily on the Trading Venues of an individual member country.[69] This information is shared through the TREM system operated by ESMA, however; there is no formal integration of the data.[70]

---

65 Most Market Authorities state that the data collected for Cross-Market or Cross-Asset surveillance purposes is generally the same as for single asset types traded on a single exchange (e.g., Australia: ASIC; Brazil: CVM; Germany: BaFin; France: AMF; India: SEBI; Mexico: CNBV; Malaysia: SC; U.K.: FSA; U.S.: BATS).

66 See footnote 10, *supra*.

67 For example, Japan: TSE; U.K.: PLUS; U.S. securities sector: SEC.

68 For example, Spain: CNMV; Netherlands: AFM.

69 Thus, by way of example, all transactions (executed trades) in stocks listed on *German exchanges*, no matter where executed in the EU, would be sent to the *German BaFin*. However, the BaFin would not be the repository for transactions in non-German stocks traded on German exchanges. Thus, in that sense, transaction data is not "integrated" in Europe.

70 The Markets in Financial Instruments Directive (MiFID) "establishes that Member States shall require investment firms which execute transactions in any financial instruments admitted to trading on a regulated market to report the details of such transactions to the home competent authority of the firm as quickly as possible." This obligation applies regardless of whether the transaction was executed on a regulated market.

4. Cross-Border Monitoring, Cooperation and Coordination

Many of the instruments traded on domestic exchanges are often listed or traded on other markets or tied to instruments listed on other, foreign markets.[71] In some instances, such trading arrangements may be formalized between participating markets. Nonetheless, most Market Authorities do not conduct Cross-Market or Cross-Asset Surveillance outside of their respective jurisdictions.[72] One exception, however, is the U.S. CFTC (U.S. derivatives sector), which conducts cross-jurisdictional surveillance as a matter of course for certain foreign boards of trade.[73]

It may be difficult (in the absence of a specialized Memorandum of Understanding (MOU)) to obtain cross-market and cross-asset information whenever it is located abroad.[74] The most common difficulties reported by Market Authorities in accessing needed information on a cross-jurisdictional basis are: (1) the length of time it takes to obtain the requested information;[75] and (2) legal restrictions preventing the sharing of some information.

Coordination between Trading Venues and the Statutory Regulator takes place via statutory and other formal arrangements, such as MOUs or protocols that establish regular information sharing through joint working groups. In addition, in order to fulfill their duties, Statutory Regulators have entered into numerous MOUs, both bilateral and multilateral, with various domestic and foreign regulators. Typically, MOUs contain provisions related to consultation, cooperation, and information sharing among signatories.[76]

Historically, many MOUs, including the IOSCO multilateral MOU (IOSCO MMOU), have been aimed at cooperation in securities enforcement matters, rather than surveillance. Recently, however, many Statutory Regulators have been entering into MOUs related to surveillance that facilitate supervisory cooperation in the supervision of financial services firms and the oversight of markets. IOSCO has long supported supervisory cooperation among its members.[77]

In some regions, a common legal and regulatory framework determines the parameters of cross-jurisdictional coordination. In the European Union, for example, member states' Competent Authorities share information with each other on transactions (as set out above) and on suspicious transactions where these relate, directly or indirectly, to cross-border activity.

---

71 E.g., Germany: FSX; Mexico: CNBV; Netherlands: NYX; US securities sector: NASDAQ.

72 E.g., Canada: IIROC and the MX; India: SEBI; Singapore: SMX; U.S. securities sector: BATS, Direct Edge, FINRA, ISE.

73 That is, for those foreign boards of trade that "elect to list for direct access from the U.S. contracts which settle against any price, including the daily or final settlement price, of (1) a contract listed for trading on a DCM (Designated Contract Market), or (2) a contract listed for trading on an ECM (Exempt Commercial Market) that has been determined to be a significant price discovery contract."

74 View of the CFTC (U.S. derivatives sector).

75 These delays can slow Market Authorities' ability to conduct timely surveillance and investigations (e.g., Canada: IIROC). One possible cause of delays may be the "uniqueness" of each particular request. The CFTC (U.S. derivatives sector) observes that "each information-sharing request usually has unique features due to uniqueness of the market event resulting in a unique negotiation even where an MOU exists."

76 See IOSCO *Principles Regarding Cross-Border Supervisory Cooperation*, Final Report, Report of the Technical Committee of IOSCO, May 2010, available at: http://www.iosco.org/library/pubdoc/pdf/IOSCOPD322.pdf

77 *Id.*

Some Market Authorities are limited in their ability to share information via MOUs because of domestic regulations, including so-called *blocking* statutes. Because of such legal restrictions, many Market Authorities find it difficult to obtain information critical to an investigation, e.g., the identity of the beneficial owners of financial products.

Most Market Authorities nonetheless stated in response to the IOSCO Survey that they are able to obtain information on an *ad hoc* (request) basis from other regulators.[78] Provisions of the applicable MOU and/or the ISG Agreement generally govern the confidentiality obligations of a requesting authority. In the absence of an MOU, Market Authorities will often still share non-public information, but impose conditions requiring confidentiality before the information is shared. In Europe, under ESMA's TREM system, data collected from other Market Authorities is sent in encrypted packages that render the information unreadable to anyone other than the receiving member.

Even when information can be and is shared, most Market Authorities express concerns about the format in which the requested information is received.[79] A number of Market Authorities find that because of these differences in the presentation of the data, audit trail data from other Market Authorities often contains less information than audit trail data collected internally.[80] For instance, the information collected from foreign jurisdictions may be in the form of summary reports and not include detailed order and transaction data.[81]

With respect to the issue of differing formats for the presentation of the data, NASDAQ noted in its answer to the survey that requiring the data provided from other jurisdictions to be standardized might affect the way the *liquidity destinations* do business, may impede innovation in the market, and may introduce a translation layer that would have to be closely monitored on an on-going basis. Nevertheless, NASDAQ conceded that the data collected in native formats is less useful and often requires translation or standardization by the market authority making use of the foreign jurisdiction audit trail data.[82]

Coordination amongst Trading Venues may occur through memberships with non-governmental international organizations that coordinate and develop programs and procedures to identify possible fraudulent and manipulative activities across markets and promote information sharing among members. The primary example of this is the ISG.

---

78 For example, Canada: IIROC and MX; U.K.: FSA; Japan: TSE.

79 Canada: IIROC; Netherlands: AFM.

80 Canada: MX; France: AMF; Spain: CNMV.

81 View of the MX (Canada).

82 To address a similar issue, the U.S. CFTC requires data obtained from "linked" foreign markets to be in a form that can be integrated into the CFTC's market surveillance system.

Chapter 3 Challenges to Effective Monitoring of Markets

A. Introduction

In the past decade, Trading Venues have become more automated, trading systems have become ever more sophisticated, and trading volumes have increased significantly. Trading has also become more dispersed across an increasing number of Trading Venues and therefore more difficult to monitor and trace. Advances in technology allow investors to trade cross-market, cross-asset and cross-border in milliseconds. These advances also have substantially increased the vulnerability of markets to inappropriate activity, in that there are opportunities for traders to engage in complex, manipulative activity that is very difficult to uncover. It has also become more challenging for Market Authorities to conduct in due time large-scale market reconstructions and analyses of extraordinary market events, such as the May 2010 *flash crash*.

Current surveillance techniques, including the collection, storage and accessibility of data may be insufficient to capture in a timely manner all of the information necessary to monitor efficiently and effectively trading activity that occurs in the current highly automated and dispersed markets. The absence of cohesive, readily available order and/or transaction information may impact the ability of Market Authorities to perform effectively their respective responsibilities to monitor trading activity by market participants across markets and products. The need of a specific Market Authority for certain kinds of information and the required speed and method by which it should be obtainable, however, depends on the statutory responsibilities of the relevant Market Authority.

There is today generally a clear delineation of responsibilities with regard to surveillance responsibilities and structures. However, these vary significantly between jurisdictions. For instance, in some jurisdictions, each individual Trading Venue is required to undertake real-time surveillance of the activity within its own market to ensure fair and orderly trading, with specific or more serious concerns (e.g., concerns regarding possible market abuse, or egregious breaches of its trading rules) referred to a Statutory Regulator. In other jurisdictions, one central entity – often a SRO – undertakes real-time market surveillance on a consolidated basis for all Trading Venues (at least for given asset classes – e.g., cash equity). In most jurisdictions, Statutory Regulators do not conduct real-time surveillance and rely on Trading Venues and SROs to identify suspicious trading and other issues of concern.

The question for Market Authorities is whether, given the latest technological and market structure developments, existing surveillance tools available to Market Authorities are adequate. The fact finding (responses to the IOSCO survey plus presentations provided by Market Authorities and industry experts) revealed specific challenges and concerns with regard to this question. We set forth immediately below a more detailed description of the challenges identified in response to the survey and during the presentations. In addition, we have identified other challenges related to data collection, resource/technical expertise and cross-border issues. Finally, we discuss the challenges associated with a possible solution suggested by some of establishing (where appropriate and necessary) a Central Reporting Point.

The final recommendations discussed in the next section take account of the challenges identified, and are intended to guide Market Authorities with regard to the capabilities they

should have in order to address these challenges and be able to conduct market surveillance (individually or collectively) more effectively.

B. Issues Relating to Data Collection and Reporting

1. Introduction

There were broadly two distinct categories of concerns expressed by the 42 Market Authorities who responded to the IOSCO Survey and who identified challenges associated with effective market surveillance. The first category relates to the issue of maintaining an effective market-surveillance regime within their jurisdictions. In particular, a large number of respondents, including those from the U.S. and the EU, cited the challenges in monitoring effectively trades occurring on *a cross-market or cross-asset class basis*. They also stated that there was a major challenge in achieving effective cross-border surveillance.

The second category relates to challenges stemming from ongoing technological developments and the way that such developments may make more difficult effective monitoring of markets. The two primary challenges identified were the need to: (1) collect data, including the potential inadequacy of current content and the related collection and storage costs for a vast amount of trade information; and (2) develop a process to use effectively such information for surveillance purposes, particularly for the purpose of identifying customers. One Statutory Regulator also highlighted the increasing amount of *trading noise* produced by the proliferation of fully automated program trading and order execution systems, which has made it a challenge to distinguish *bona fide* orders and trades from manipulative activities.

IOSCO members believe that Market Authorities need to have access to a broad range of data, including transaction and/or order data information, and must be able to manage and use this mass of information, in order to fulfill their market surveillance responsibilities. Survey responses reveal that in some jurisdictions this sort of information is currently (or could be made) accessible to the responsible Market Authority from multiple sources via "request" rather than by direct access. Some believe that such a system works well.

2. Reporting of Data

The survey responses and presenters to IOSCO highlighted the following challenges as being relevant to any jurisdiction with regard to data that must be reported to one or more Market Authorities, whether or not there is a Central Reporting Point.

- Significant disparities in the audit trail requirements among different Trading Venues within a single jurisdiction, especially with respect to the *type of information* captured by each. Disparities might relate, e.g., to data regarding customer identity, quotes (orders), and transactions, etc. Consistency of such information can enhance the ability of a Market Authority to oversee and survey effectively the markets on a timely basis.
- The need to resort in some jurisdictions to the lengthy process of submitting written requests for information to all firms that may be involved in the handling of an order – a process often fraught with delays – in order to narrow down the identity of a customer.

- The lack of synchronized clocks among all of the entities that need to submit data.
- Differences in the format in which data is reported. The lack of format uniformity in (and cross-market compatibility of) audit trails can make detection of illegal or inappropriate trading activity carried out across multiple markets and multiple products more difficult. This was also identified as a major cross-border issue.
- The speed with which Market Authorities are able to access data.
- Possible legal limitations on the time period that information relating to individuals may be retained – i.e., legal provisions relating to data protection.

C. Staffing Skills and Technological Systems

Some respondents to the IOSCO survey expressed the view that some Market Authorities may have inadequate resources to hire the staff necessary to conduct complex technological market surveillance. Market Authorities in general face challenges in recruiting and retaining surveillance staff that possess the requisite level of knowledge and experience and are able to make informed decisions regarding the alerts that are generated. For example, the systems required by a Market Authority fall essentially into two groups: the underlying database that houses reported data, and the analytical systems that are applied to that data. Analytical systems may incorporate alerting functionality, data mining/reporting tools, visualization tools (e.g., the ability to reconstruct an order book on screen) and various other analytical applications. Some respondents to the IOSCO survey noted that they have had problems hiring experienced staff to operate these analytical systems.

Respondents also identified the possible inadequacy of existing computer systems at the disposal of Market Authorities to conduct market surveillance effectively. They believe that Market Authorities responsible for conducting market surveillance need enhanced financial resources to meet the challenges of technological developments. For example, some respondents stated that:

- Manual surveillance may not be adequate for current market conditions. New surveillance approaches to detect anomalous trading cross-venue and cross-asset are needed.

- A Market Authority responsible for surveillance needs systems that can perform the authority's monitoring responsibilities and have the capacity to handle the data they receive/maintain.

- Connectivity arrangements need to be appropriate for the volume and type of data being sent to the given surveillance system, and must be suitably robust.

D. Cross-Border Issues

As noted earlier in this report, many of the instruments traded on domestic Trading Venues are tied to instruments listed on foreign markets. Nonetheless, most Market Authorities do not conduct cross-venue or cross-asset surveillance outside of their respective jurisdictions.

Cross-border coordination among Trading Venues may occur through memberships with non-governmental international organizations, such as the ISG, that coordinate and develop programs

and procedures to identify possible fraudulent and manipulative activities across markets and promote sharing of information among members.

In addition, in order to fulfill their duties, statutory regulators have entered into numerous MOUs, both bilateral and multilateral, with various domestic and foreign regulators. MOUs typically contain provisions related to consultation, cooperation, and information sharing obligations. To date, many MOUs have been related to sharing information for enforcement matters. More recently, many statutory regulators entered into MOUs and other arrangements with their foreign counterparts to exchange information for routine market surveillance purposes. Indeed, IOSCO has long supported supervisory cooperation among its members.[83]

Respondent to the survey noted some obstacles to cross-border supervision. For example, in some jurisdictions, it may be necessary to notify a customer before identification information can be obtained from brokers or share registries, which can be both time and resource intensive. Some survey respondents noted that it may be difficult (in the absence of a specialized MOU) to obtain cross-market and cross-asset information whenever it is located abroad. Accordingly, some survey respondents suggested that further consideration be given to possible ways of enhancing cross-border surveillance capabilities.

E. Central Reporting Point

A number of Market Authorities expressed the view that one possible solution to address some of the issues (raised above) is the creation of a single uniform electronic cross-market order and execution-tracking system within a single jurisdiction that includes more information than is captured by the existing audit trails utilized by Trading Venues, and is provided in a uniform format. These respondents took the view that a so-called *consolidated audit trail*, whereby transaction and order data is *consolidated* into a *Central Reporting Point* (CRP), could potentially enhance the ability of Market Authorities to carry out their obligations to oversee the markets and their participants. These respondents further believe that it could in particular aid Market Authorities in their ability to detect the use of manipulative or deceptive devices in the purchase or sale of an instrument, as well as performing market reconstructions in a timely manner. In addition, they take the view that given technological developments, it could be necessary to have this information in order to survey the use of technology in trading, such as high-speed quoting strategies and to assess the impact of market making and other high-frequency quoting behaviors on the quality of the markets. They believe that the enhanced surveillance capabilities of a CRP could outweigh the potential burden and cost of implementing such a system.

However, a number of respondents to the IOSCO survey expressed concerns about establishing such a CRP, and indeed believe its establishment may not be the only solution to enhance market surveillance capabilities. In particular, certain respondents raised concerns about the potential costs related to developing a CRP and the associated costs related to ongoing data storage. These respondents argue that the potential costs could be substantial and accordingly may not be feasible for all jurisdictions. They further argue that the potential benefits may not outweigh the potential costs for all jurisdictions. Additional concerns expressed include the following:

---

[83] See IOSCO *Principles Regarding Cross-Border Supervisory Cooperation*, IOSCO report, May 2010, *supra fn* 76.

- It would require the reconstruction of accurate sequences of events occurring in different trading spaces.
- It would require elimination of the effect of feed latency on alerts.
- Data quality may suffer due to the need to standardize data input.
- Even if there is a single reporting point, individual Trading Venues will still need to keep their own data.
- Including order/quote information would entail a large amount of data and could increase costs.

Chapter 4 High Level Recommendations and Questions for Consultation

A. Introduction

In response to the issues and challenges identified above, IOSCO sets forth below its final recommendations to assist Market Authorities in addressing those challenges, particularly with respect to: (1) improving surveillance capabilities on a cross-market and cross-asset basis; and (2) making more useful to Market Authorities the data collected for surveillance purposes. The final recommendations are unchanged from those set forth in the Consultative Report, but take into account both the survey results and public comments to the Consultative Report.

B. Recommendations

1. Regulatory Capabilities

Market Authorities should have the organizational and technical capabilities to monitor effectively the Trading Venues they supervise, including the ability to identify market abuse and activities that may impact the fairness and orderliness of trading on such venues.

Discussion

A starting point for effective surveillance is a strong legal mandate and regulatory structure to support the surveillance of the market and its participants. IOSCO Core Principle 3 provides that "the Regulator should have adequate powers, proper resources and the capacity to perform its functions and exercise its powers."[84] In this regard, it is important to note that a few commenters to the Consultation Report stated that regulators require greater funding to achieve the necessary organization and technical capabilities.

While legal mandates and regulatory structures will vary across jurisdictions, and IOSCO does not promote any particular approach, jurisdictions need to have the ability to supervise their markets effectively. The ability to supervise and conduct effective surveillance also depends on the structure of a market. For example, a market may have dispersed Trading Venues that necessitate Cross-Market Surveillance; or it may have trading across asset classes that necessitate Cross-Asset Surveillance. Market Authorities, and in particular, Statutory Regulators, need to assess whether they have the organizational and technical capabilities to perform an effective surveillance function in light of their market structure. Of course, the resources available to the Market Authority will determine, in part, the degree to which the Market Authority can develop the capabilities to conduct effective surveillance.

---

[84] See IOSCO *Objectives and Principles of Securities Regulation*, Report of IOSCO, June 2010, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD323.pdf. See also Principle 10, which states: "the Regulator should have comprehensive inspection, investigation and surveillance powers."

Recommendation 1 remains unchanged from the Consultation Report, as the public comments were largely consistent with it. Commenters did, however, express specific views as to what is needed to ensure that Regulators have the organizational and technical capabilities to monitor effectively the Trading Venues they supervise. For example, commenters confirmed that access to trading data (see also Recommendation 3) is the key capability that Market Authorities should have and that cooperation between Trading Venues and regulators plays an essential role of facilitating that capability. They stressed the importance of Market Authorities having access to data from local market participants, remote market participants, other Market Authorities, and domestic and foreign Trading Venues and that effective surveillance requires the ability to reconstruct and analyze order books. Commenters suggested that an effective audit trail system needs identifiers for orders, clients, time, trades and quotes. There was a general consensus that a key improvement that could be made in current systems might be the standardization of data type included in audit trails as to promote cross-jurisdictional compatibility, such as through a consolidated tape that publishes pre- and post-trade data from across all Trading Venues, periodical evaluation of surveillance capabilities by authorities or an audit trail regime similar to SEC's CAT.

2. Review of Surveillance Capabilities

Market Authorities should regularly review and update as appropriate their surveillance capabilities, including systems, tools and surveillance staff skills, particularly with respect to technological advances.

Discussion

Regular review of surveillance capabilities promotes a regulatory framework that supports investor protection, fair, efficient and transparent markets and the reduction of systemic risk.

Surveillance programs are developed by Market Authorities in light of the structure of the market and the legal system that underpins it. As markets evolve, Market Authorities should regularly review whether their existing surveillance programs are sufficient to fulfil their regulatory obligations, including whether they have the necessary resources, in order to ensure the fair and orderly functioning of Trading Venues and to promote market integrity. Such review is key in a market that is complex and continuously evolving.

This recommendation remains unchanged from the Consultation Report, as many commenters acknowledged the impact of technology on Market Authorities' ability to survey markets, along with the corresponding increase in trade volume, the absence of customer identifiers (see Recommendation 4) and the ability of customers to trade in multiple markets across borders (i.e., fragmentation). They noted that technology has led to sophisticated strategies and greater transaction speeds (with a plurality of commenters identifying algorithmic and/or high frequency trading as having the greatest impact on Market Authorities' ability to monitor markets), but that Market Authorities have not always taken advantage of the gains offered through technological developments, such as automated alerts and systems that can capture all information about an order or trade executed on a market. Thus, the public comments generally confirmed the need for Market Authorities to review regularly and update as appropriate their surveillance capabilities remains critically important.

3. Access to Data

Within their jurisdiction, the relevant Market Authority(ies) should individually or collectively have the capability to access data in a way that enables them to conduct effectively their surveillance obligations.

Discussion

The ability to access the data necessary to oversee a market is integral to an effective surveillance system. An effective surveillance system should have, at a minimum, the ability to (1) detect the use of manipulative or deceptive devices in the purchase and sale of securities (equities), futures on commodities and securities markets and other financial products,[85] and (2) perform market reconstructions. Market Authorities that do not have access to necessary surveillance data would not be able to oversee their markets effectively. Moreover, as the use of related OTC derivatives could increase the risk of abuse or manipulation of venue-traded products, regulators may wish to consider putting similar arrangements in place for access to data for such derivatives.[86]

One of the key questions posed underneath this Principle in the Consultation Report was the extent to which commenters believed that a Central Reporting Point (CRP) is necessary within a domestic market in order to conduct surveillance effectively, particularly across markets and/or assets. A review of the public comments to the Consultation Report reveals some support for the development of a CRP as a tool that can enable market authorities to access the data they need to conduct effective surveillance. However, it is equally clear that a number of commenters believe that in light of the costs and other issues associated with the development of a CRP, and in light of specific market structures, alternative tools for organizing effective surveillance may also be appropriate. Consistent across all comments, however, is the idea that relevant Market Authorities should individually or collectively have the capability to access data in a way that enables them to conduct effective surveillance. We believe that these collective comments are wholly consistent with Recommendation 3, as proposed in the Consultation Report. We have therefore not modified the recommendation.

---

85 This recommendation is limited in its application per the IOSCO project specification for this report. In particular, the project specification provides that "the scope of this project will include the trading securities (equities) and futures on commodities and securities markets. It will also include the trading of other financial instruments, such as corporate bonds, municipal bonds, asset-backed securities and other debt instruments. The scope will also include certain types of derivative products, such as credit default and equity swaps and other security based swaps, but only to the extent that the IOSCO OTC Derivatives Task Force (Task Force) and CPSS-IOSCO are not already examining similar issues with regard to such products."

86 See, e.g., CPSS-IOSCO *Principles for Financial Market Infrastructures*, April 2012, available at: http://www.bis.org/publ/cpss101a.pdf. That report notes that trade repositories (TR) have emerged as a new type of financial market infrastructure (FMI) and have recently grown in importance, particularly in the OTC derivatives market. The report notes that "[b]y centralising the collection, storage, and dissemination of data, a well-designed TR that operates with effective risk controls can serve an important role in enhancing the transparency of transaction information to relevant authorities and the public, promoting financial stability, and supporting the detection and prevention of market abuse." It further notes that "[t]he primary public policy benefits of a TR, which stem from the centralisation and quality of the data that a TR maintains, are improved market transparency and the provision of this data to relevant authorities and the public in line with their respective information needs."

4. Customer Identification

Market Authorities (individually or collectively) should have the capability[87] *to associate the customer and market participant with each order and transaction.*

Discussion

As noted at the beginning of this report, all jurisdictions currently use direct market participant (member) identifier codes, which are generally assigned by the Trading Venue. In some jurisdictions with multiple Trading Venues, such as the U.S. and U.K., a single broker-dealer may have multiple market participant identifiers assigned to it by multiple Trading Venues, depending on the securities traded, the markets on which they are traded, and the number and functions of trading desks within the particular broker-dealer. A few, such as Canada and Australia, require the same market participant identifiers to be used across multiple markets. Ultimately, an audit trail/surveillance system is less useful if the customer cannot be identified, particularly when they are coordinating orders across multiple markets. The responsible Market Authority should have the capability to know if a particular customer is sending orders across multiple markets and assets to facilitate an unlawful manipulation. The issue and the challenge remain: what is the optimal system within a given market structure to obtain this information?

The commenters to this recommendation focused on *customer identifiers*. The near unanimous consensus was that customer identifiers should be used. However, a significant number of them also identified confidentiality and legal concerns preventing the use of customer identifiers. Nonetheless, the underlying theme of the public comments was that Market Authorities (individually or collectively) should have the capability to associate the customer and market participant with each order and transaction, but recognizing the practical difficulties in achieving this, particularly in a cross-border situation. The recommendation therefore remains unchanged from the proposal in the Consultation Report.

5. Format

Market Authorities should require that data required for market surveillance be reported to the requisite Market Authority for use and storage in a usable format.

Discussion

Data accessible to Market Authorities from different markets and intermediaries (whether on a systematic or *ad hoc* basis) may be in a myriad of formats (or languages), such as CSV, PDF, XML, TXT, Excel, and *flat file*. This can complicate and delay surveillance efforts, particularly where the responsible Market Authority seeks to compare trade data across markets. Solutions must be found so that the data from all markets within a jurisdiction can be used and compared by Market Authorities in an efficient and effective manner. This could include development of a system that permits the responsible Market Authority to search a relevant database efficiently for certain types/categories of data.

Commenters to the Consultation Report unanimously agreed that Market Authorities should take the steps necessary to standardize data, as this would aid Market Authorities in more effectively monitoring markets. They offered various ideas on how data should be standardized. For

[87] The term is intended to refer both to the technical ability and the legal competence necessary for the Market Authority to request/obtain this information.

example, a number of commenters suggested that Market Authorities work with the industry to establish a common (e.g., international) standard. Moreover, IOSCO shares the concern expressed by most commenters to the Consultation Report relating to the current ability of Market Authorities to reconstruct and analyse order books, including current timestamp granularity and synchronization.

IOSCO believes that the recommendation in the Consultation Report reflects the views of commenters as it also emphasizes that data should be reported to Market Authorities in a usable format, which could significantly enhance the ability of Market Authorities to reconstruct and analyse order books. The recommendation therefore remains unchanged from that proposed in the Consultation Report.

6. Data Protection

Market Authorities should establish and maintain appropriate confidential safeguards to protect surveillance data that is reported to them.

Discussion

It is critical that data provided to Market Authorities for the performance of their surveillance functions is secure and cannot be viewed or amended by unauthorized parties. If this is not the case, Market Authorities cannot be sure that the information they are analyzing is accurate and complete. This may result in illegal and/or inappropriate activity going undetected and may undermine confidence of participants in the markets. In addition, it may lead to sensitive information being leaked, damaging the legitimate interests of the affected parties and undermining their privacy.

In addition, in the context of compliance, investigations and enforcement, Market Authorities may need to share information with other Market Authorities. This may be done under MOUs or other information sharing arrangements. When done, Market Authorities should take steps to ensure the appropriate confidentiality agreements are in place.

Nearly every commenter to the Consultation Report thought that it was important for Market Authorities to be able to obtain the data they need from other Market Authorities (domestic or foreign) in order to conduct effectively securities market surveillance. Most commenters to the Consultation Report impliedly agreed with the recommendation by stating that existing confidentiality provisions are sufficient (no matter where data is currently obtained), while emphasizing that there must be standards both with regard to how data is kept and how data-access networks are maintained. For this reason, the recommendation is unchanged from the proposed recommendation in the Consultation Report.

7. Synchronization of Business Clocks

Market Authorities should consider requiring Trading Venues and their participants within their jurisdiction to synchronize, consistent with industry standards, the business clocks they use to record the date and time of any reportable event.

Discussion

Synchronization of the clocks used by Trading Venues, market participants and Market Authorities can be highly important to ensuring there is a clear audit trail of which market events took place when. This is particularly important in jurisdictions where there are multiple Trading Venues across which trading in a given instrument is dispersed or where markets trade different but related instruments (e.g., a derivative and the associated underlying asset). However, the need for complete clock synchronization between parties and the level of accuracy required (including how granular time-stamps should be) might differ from jurisdiction to jurisdiction, in accordance with local needs, market structures and how surveillance is organized.

Most commenters to the Consultation Report supported the synchronization of business clocks, while recognizing real world challenges, such as seeking to synchronize accurately timestamps within a fragmented market with multiple trading venues and market participants. This is largely consistent with the recommendation proposed in the Consultation Report, which recognized the importance of business clock synchronization, but only suggests that Market Authorities *consider* requiring Trading Venues and other participants within their jurisdiction to synchronize business clocks, consistent with industry standards. This final recommendation, unchanged from the Consultation Report, thus recognizes the practical challenges noted by the commenters.

8. Cross-Border Surveillance Capabilities

Market Authorities should at a minimum map and be aware of the extent of their cross-border surveillance capabilities. Market Authorities should also work collectively and take any steps that would be appropriate to strengthen their cross-border surveillance capabilities.

Discussion

It is important that Market Authorities are clear as to the cross-border surveillance capabilities they have, having regard to the inter-linkages between their domestic markets and those abroad. These inter-linkages will include, but may not be limited to, instances of a single instrument being traded on a domestic and foreign market or related instruments (e.g., a derivative and its underlying asset) being traded in different jurisdictions. Cross-border surveillance capabilities may take many forms, from a Market Authority having an automated audit trail system that gathers information from multiple jurisdictions to MOU arrangements being in place between authorities. By mapping their capabilities, Market Authorities should ensure that they have a clear understanding of where any gaps may lie in their capabilities to help inform their decision-making on how these should be addressed. Market Authorities should work collectively, and where appropriate with international organization(s), to explore initiatives to enhance cross-border cooperation with regard to surveillance capabilities.

Most commenters expressed the view that Market Authorities should encourage and facilitate quick, efficient and flexible cooperation between regulators and market operators regardless of jurisdictional boundaries, and that they should enter into MOUs with regulators in different jurisdictions to establish mechanisms for rapid and efficient exchange of data. This is largely consistent with current practices and the recommendation in the Consultation Report. The recommendation is therefore unchanged in this Final Report.

Appendix A - Principles of the IOSCO Commodities Task Force Report

1. Framework for Undertaking Market Surveillance. Market Authorities should have a clear and robust framework for conducting market surveillance, compliance and enforcement activities and there should be oversight of these activities. A market surveillance program should take account of a trader's related derivatives and physical market positions and transactions. Market surveillance programs should be supported by sufficient resources, access to physical market data and analytical capabilities.

2. Monitoring, Collecting and Analyzing Information. Market Authorities should develop, employ and maintain methods for monitoring of trading activity on the markets they supervise, collecting needed information and analyzing the information they collect that are efficient and suitable for the type of market being supervised. Effective monitoring of orders and electronic transactions requires real-time monitoring capabilities, supported by automated systems that detect trading anomalies. Monitoring, collection and analysis should also focus on intra-day trading.

3. Authority to Access information. Market Authorities should have the authority to access information on a routine and non-routine basis for regulated commodity derivatives markets as well as the power to obtain information on a market participant's positions in related over-the-counter (OTC) commodity derivatives and the underlying physical commodity markets. Market Authorities should review the scope of their authority to obtain such information and if necessary to request such power from the relevant legislature or other appropriate governmental bodies.

4. Collection of Information on On-Exchange Transactions. In respect to on-exchange commodity derivatives transactions, a Market Authority should collect information on a routine and regular basis on: pricing of contracts throughout the trading day in real-time; daily transactional information; daily reports of end-of-day positions held by market intermediaries; and, where appropriate, warehouse stocks or other deliverable supply.

5. Collection of OTC Information. In respect of OTC commodity derivatives transactions and positions, a Market Authority should consider what information it should collect on a routine basis and what it should collect on an *as needed* basis. A Market Authority that has access to a relevant Trade Repository's (TR) data should take such broader access into account, as well as its statutory obligations with respect to the TR, in constructing its data collection policies.

6. Large Positions. Market Authorities should require the reporting of large trader positions for the relevant on-exchange commodity derivatives contracts. The Market Authority should have the ability to aggregate positions owned by, or beneficially controlled on behalf of, a common owner.

Appendix B - Regional Approaches to Surveillance for Equities and Derivatives

(1) Equities Markets

a) Americas

(i) U.S. Securities Sector

In the U.S., FINRA collects a wide range of audit trail data in its capacity as: (1) the SRO for OTC markets for equity and corporate debt securities in the U.S.; and (2) the SRO for all securities firms conducting a public securities business in the U.S. In addition, FINRA performs market surveillance for several U.S. securities exchanges, including the NASDAQ Group, the NYSE Group, Direct Edge and the ISE, pursuant to RSAs.

FINRA collects all order and related information from FINRA members, in relation to NMS (National Market System) securities (including: order receipt, order cancellation, order routing, and order execution) via its Order Audit Trail System (OATS). In addition, FINRA also receives order book information from the exchanges for which it performs market surveillance pursuant to RSAs. FINRA also receives quotation and trade reports for NMS securities from the SIPs (Securities Information Processors) and trade reports from the two trade reporting facilities (TRFs) owned by the two major exchanges, NYSE-Euronext and NASDAQ-OMX. In relation to OTC markets in equity securities, FINRA captures trade reports in unlisted equities through the over-the-counter reporting facility (ORF). By rule, trade reports must be submitted within 30 seconds of the trade's execution.

While SROs focus surveillance on their respective marketplaces, the SEC covers all securities markets in the U.S. The SEC, which is primarily responsible for enforcing federal securities laws and regulations, has dedicated automatic real-time and post-trade systems (including Bloomberg, Reuters, a NASDAQ workstation, feeds from Archipelago, and feeds from all of the newswires) that identify unusual transactions on exchanges and alternative trading systems. In addition, the SEC can at any time obtain: (1) trading information maintained by any SRO, such as audit trails, market maker price movement reports, and equity clearing runs; and (2) transaction data from registered broker-dealers (both customer and proprietary transaction information) through the Electronic Blue Sheets (EBS) system.

The SEC's EBS system, however, lacks two important data elements - the time of execution for the order and a uniform identifier to identify the participant that affected the trade. To enhance its surveillance capabilities, the SEC implemented a large-trade reporting requirement for securities in October 2011, and approved Rule 613, which requires SROs to submit an NMS plan to create, implement, and maintain a consolidated order tracking system, or consolidated audit trail (CAT), in July 2012.

Finally, the SEC also relies upon the National Securities Clearing Corporation's equity cleared report for initial regulatory inquiries. The information provided is searchable by security name and CUSIP number and includes the date, the clearing firm, and the number of transactions cleared by each clearing firm on each SRO.

(ii) Canada

As the securities sector SRO in Canada, IIROC takes in real-time regulatory data feeds from all Canadian equity trading marketplaces (including listing exchanges and alternative trading systems) to undertake real-time market supervision and post-trade surveillance of all Canadian equity markets. IIROC receives trade and order data (including amends and cancels) from all equity marketplaces and creates a consolidated order book across those marketplaces. IIROC also receives other data relating to security status messages (e.g., halted, frozen, etc.), as well as necessary reference data. It also collects Direct Market Access (DMA) client information, including regulatory feed ID numbers and client name, through a separate information source. IIROC only conducts the above described surveillance activity with respect to equity markets, while the Montreal Exchange (MX) monitors all exchange-traded financial derivatives, including equity options; ICE Futures Canada performs surveillance for its commodities market.

The provincial Statutory Regulators in Canada (e.g., the AMF Quebec and the OSC), on the other hand, obtain trade and order data and position information from IIROC, Trading Venues, and market participants to analyse trading patterns and support investigations relating to insider dealings and market manipulation.

(iii) Mexico

In Mexico, the exchanges and the CNBV carry out real-time market surveillance programs in parallel to one another. In order to investigate unusual securities market transactions (equity, debt, and derivatives), the CNBV can request any kind of relevant information from exchanges, securities firms, central depository, and central counterparties. In addition, the CNBV can also conduct on-site investigation visits to any regulated entity to access relevant records and review non-public information. The data collected by the CNBV includes: orders and cancellations; beneficial owners; account statements; contracts (brokerage and bank accounts, financial services, trust accounts, etc.); final settlement; large positions; and the risks taken by each participant.

(iv) Brazil

In Brazil, the CVM is responsible for monitoring the market operating procedures, the disclosure of price sensitive information, and ensuring orderly market conditions, while the BSM (SRO) is responsible for overseeing the BM&FBOVESPA's markets (securities, commodities, and futures). The CVM and the BSM have access to the following audit trail data: order data (entering, amending and canceling) including the replay function (only the BSM); transaction data; client data by T+1 (beneficial owner, identification, economic activity, address, date of creation, active flag, etc.); clearing data; depository data; positions data; and securities lending data.

b) Europe

Trading Venues in Europe are generally responsible for undertaking real-time surveillance and referring suspicious transactions to their regulators for further investigation and enforcement. For the purpose of maintaining fair and orderly trading on European markets, monitoring market abuse and members' compliance with their rulebooks, Trading Venues in Europe generally collect trade and order data (including on cancellations and modifications).

In accordance with MiFID, member states must require investment firms that execute transactions in any financial instrument admitted to trading on a regulated market to report details of such transactions to the competent authority as quickly as possible, and no later than the close of the following working day. This obligation shall apply whether or not such transactions were carried out on a regulated market. The competent authorities shall establish the necessary arrangements in order to ensure that the competent authority of the most relevant market in terms of liquidity for those financial instruments also receives this information. ESMA facilitates this via Europe's Transaction and Exchange Mechanism (TREM) the technical system for exchanging this transaction data. In addition to the audit trail data collected under the MiFID transaction-reporting regime, some Market Authorities in Europe also collect supplementary audit trail information to support their investigation and enforcement activities.[88]

Within the countries of Europe subject to MiFID, there are some country specific approaches:

- In Germany, market surveillance is undertaken at both the federal and state level. At the federal level, the BaFin is responsible for the supervision of insider trading and market manipulation on and off the stock exchange, and is responsible for monitoring compliance with director's dealings and disclosure of material information. At the state level, the stock exchange supervisory authorities of the Federal States, in collaboration with the TSOs (e.g., the FSX), supervise the orderly conduct of trading on the individual exchanges. The main duty of TSOs is to collect, record, and evaluate data regarding exchange trading and the settlement of exchange transactions.

- In the Netherlands, the AFM is responsible for conducting real-time and post-trade market surveillance while European regulators in general (except Switzerland) receive transaction reports from investment firms within their respective jurisdiction no later than the close of the following working day.

- In Switzerland, the SER (SRO) conducts front-line market surveillance activities for all of the three Swiss exchanges and trades in the products admitted to listing on these exchanges, and reports suspicious trades to the FINMA; it also receives and reviews

[88] For example:

- U.K.: The FSA regularly requests and receives data from trading venue operators (generally on an *ad hoc* basis). In addition, the FSA also receives suspicious transaction reports from market participants on possible instances of market abuse.

- Italy: The CONSOB also gets transaction information from Trading Venues and has access to order book data (with detailed information concerning the *history* of each order).

- Netherlands: The AFM also collects real-time transaction and order data (from the NYSE Euronext and the TOM MTF) and theoretical Opening/Closing Prices and Volumes (from the NYSE Euronext). Real-time information is collected by the AFM for the purpose of monitoring price sensitive information and making decisions in relation to trade suspensions.

- Germany: The BaFin routinely collects transaction data on all securities transactions from credit and financial services institutions and receives upon request all order data from the exchanges.

- Spain: The CNMV also receives clearing and settlement data from the Spanish Central Securities Depositary and price sensitive qualitative information from issuers.

- France: The AMF also collects transaction and order data from all regulated markets or MTFs established in France (Euronext Paris, Alternext, Bluenext, Bondmatch) on a routine basis (daily). It also receives clearing and settlement data.

transaction reports. The SER also collects and stores audit trail data for the SIX Swiss Exchange, the Scoach[89] and Eurex. The full life cycle of an order is collected, including: order entry information; order pending status; full match or partial match (execution information); or other delete reasons. In addition, all trade type codes created by the system as well as trade type codes entered by the trader are also collected. Data related to large positions and management transactions are collected separately.

c) Asia

In Singapore, Japan, Malaysia, and India, the Trading Venues are mainly responsible for real-time market surveillance to ensure fair and orderly markets and are responsible for ensuring their market participants' compliance with their respective rules.

The Statutory Regulators, on the other hand, generally play an oversight role, and focus on undertaking more in-depth analysis and investigations for possible trading irregularities and market abuse. In the case of Singapore, the MAS is also responsible for conducting real-time market surveillance of securities issued by the SGX and the derivatives linked to such securities (as the SGX is listed on its own exchange).

In Hong Kong, the SFC being the Statutory Regulator is primarily responsible for real-time market surveillance in detecting market malpractices with statutory implications. The Trading Venues in Hong Kong focus on market participants' compliance with their trading rules and risk management requirements.

Statutory Regulators in Asia generally collect order and trade data to undertake their market surveillance functions. However, some regulators and Trading Venues also collect audit trail information.[90]

d) Australia

ASIC utilizes order (enter, amend, cancellation) and trade (trade and trade cancellation data) data for undertaking real-time surveillance and post-trade surveillance on the ASX and the Chi-X equities markets (including monitoring against manipulation, insider trading, front running or

---

89 Scoach is an exchange for structured products. It is a joint venture of the SIX Group und the Deutsche Börse AG. Scoach runs Trading Venues in Zurich for Switzerland, and in Frankfurt for Germany and other EU countries.

90 For example:

- Hong Kong: The SFC also collects short selling flags of stocks (up to brokers' level to monitor short-selling activities on a macro level), net reportable short position data for key index constituent and financial stocks and shareholding data for individual stocks.
- Singapore: The SGX also collects company announcements data from SGXNet and index feeds from Reuters.
- India: The SEBI also collects the holding statements of clients.
- Japan: The SESC also collects:

    1. Information on whether the transaction is a short-selling/margin trading.
    2. Off-exchange transaction data on cash products listed on FIE.
    3. Large shareholding (5 %) reports and the alteration reports on stocks etc., listed on FIEs.
    4. Disclosures of material facts by the issuers listed on FIEs.

other criminal activity). Following the transfer of market supervision to the ASIC on 1 August 2010, the ASX's primary purpose of collecting equities post-trade data is for monitoring compliance by its listed entities with their continuous disclosure obligations. However, for historical reasons, the ASX also receives pre-trade order data done on its equities markets.

(2) Derivatives Markets[91]

a) United States

The CFTC[92] collects clearing member reports for futures (by commodity and by future) and options (by underlying futures contract for options on futures contracts or by underlying physical for options on physicals, and by put, by call, by expiration date, and by strike price). In addition, it also collects order data, cancelled data, transaction data, time and sales data, reference files, and large position data.

Additionally, FINRA (U.S. securities sector) also receives order information from the exchanges for which it performs market surveillance pursuant to RSAs, options execution data from COATS (Consolidated Options Audit Trail system), and options position information from OCC (Options Clearing Corporation).

b) Canada

MX is responsible for the market surveillance of its financial derivatives market. These activities are performed by the Special Regulatory Division of the MX, which is under the authority of the Special Regulatory Committee, a committee of the Board. The Special Regulatory Division of the MX has access to all information related to the orders submitted by its approved participants, trade data and system messages related to options and futures contracts trading activities.

ICE Futures Canada is responsible for the surveillance of its commodities market. The Regulatory Division conducts the surveillance, but is subject to oversight by a *Special Regulatory Committee* appointed by the Exchange's board of directors. The jurisdiction of the Special Regulatory Committee extends to all matters respecting compliance and market surveillance at ICE Futures Canada. It encompasses all of ICE Futures Canada's trading and contract rules, and also delivery, shipping, financial compliance and also compliance by participants with the provisions of applicable legislation and the rules and regulations promulgated thereunder.

c) Europe

LIFFE (U.K.) collects all orders submitted by its members, subsequent trade data, along with all system messages. Similarly, the LME (U.K.) also collates all transaction and order data (including cancelled orders) for the purpose of monitoring its members' futures, options, and warrant positions. In addition to derivatives market data, the LIFFE also collects clearing data (for the London market only; including give-ups/give-ins, settlement instructions, netting,

---

91 This project and the related survey relate *to exchange traded derivatives only*, and *not* OTC.

92 The CFTC's mandate is to regulate commodity futures and option markets in the United States. The Dodd-Frank Wall Street Reform and Consumer Protection Act, however, recently expanded that mandate. As such, the CFTC is the primary regulator of derivatives in the United States.

position adjustments, option exercise, and delivery notifications) and daily position information (for soft commodity products).

d) Asia

In Hong Kong, the SFC collects order and transaction data, large positions data, and position limit data (up to the ultimate client level) in relation to the futures market and the stock option market.

e) Australia

ASIC collects the following information from the market operator: daily ASX 24 Tradelog; daily Beneficial Ownership Reports; Surveillance Reports; Trade Data; and order allocations. The daily Beneficial Ownership Reports provide the total position holdings for the entire ASX 24 market at the end of each day and are largely used by the market operator to identify large position holdings, manage contract expiry and identify any abnormal trading behaviours/patterns.

Appendix C - Audit Trail Data Collected by Regulators (and some SROs) in Various Jurisdictions

Standing Committee Jurisdiction	Respondent (Statutory Regulator, SRO or exchange)	Response
Australia	**ASIC** Statutory Regulator	**Equities** • Order (enter, amend, cancellation) and trade (trade, trade cancellation) data collected from 3 sources: SMARTS, IRESS and Bloomberg. • Electronic data feeds received from the Trading Venue include: order price and volume entries; order amendments; trade price and volume entries; any special trade condition codes; participant number and identifier code; participant operator cross-reference data, where that data is available; and information comprising details of the Financial Products traded through the Trading Platform (incl. name of issuer or publicly available issuer code; tick size; lot size; basis of quotation; time-stamps on all order entries, trades, amendments, cancellations and deletions; and unique order identifier or, if this is not available, unique order series identifier). **Futures** • Audit trail data collected includes the daily ASX 24 Tradelog, Daily Beneficial Ownership Reports, Surveillance Reports, Trade Data and order allocations.
Brazil	**Comissão de Valores Mobiliários** Statutory Regulator	• Orders (entering, amending and canceling), including the replay function (only BSM); Transaction; Client by T+1 (beneficial owner, id, economic activity, address, date of creation, active flag, others); Clearing data; Depository data; Positions; and Securities Lending.
Canada	**Investment Industry Regulatory Organization of Canada (IIROC)** SRO	• IIROC collects regulatory data in real-time from Canadian equity Trading Venues via a FIX-based feed. The primary data received includes trades and orders (incl. amends and cancels) from all Trading Venues, and quote data from visible markets only. • Other regulatory feed data includes certain security status messages, (e.g. halted, frozen, etc.), as well as necessary reference data including stock name, CUSIP, dividend and reorganization information, currency, dealer identification, trader identification (feed id#, name and telephone number), etc.

Standing Committee Jurisdiction	Respondent (Statutory Regulator, SRO or exchange)	Response
		• IIROC also collects Direct Market Access (DMA) client information including regulatory feed ID numbers and client name through a separate information source.
Canada	**Montreal Exchange, MX**	• With respect to trading data, the audit trail data collected is complete from the time an order is entered into the electronic trading system up to final allocation of trades for clearing purposes. Audit trail also includes all order cancellations or modifications as well as trade cancellations. • For all derivative instruments traded on MX, approved participants are required to file position reports when gross positions held by an AP or by a customer in a given instrument exceed thresholds that are set in the rules. • Position reports are used to identify and monitor concentration situations (an account owner holding a significant proportion of the open interest in a given derivative instrument) as well as situations where an account owner is about to reach or has reached the permitted position limits that are set in the MX rules. • APs are also required to file, on a bi-weekly basis, reports of all OTC transactions made in derivative instruments having underlying interests identical to those of derivative instruments traded on MX. This allows MX to identify situations where an exchange-listed derivative instrument is also traded on the OTC market, a practice that is prohibited by MX rules.
Switzerland	**Swiss Financial Market Supervisory Authority, FINMA** Statutory Regulator	• The full order history/life cycle of an order is collected and kept in storage, incl. order entry, order pending status, full match or partial match (execution information) or other delete reasons. • In addition, all trade type codes created by the system as well as trade type codes entered by the trader are collected. • Data related to large positions and management transactions are separately available.

Standing Committee Jurisdiction	Respondent (Statutory Regulator, SRO or exchange)	Response
Europe (incl. Germany, Spain, Netherlands, France, Italy and the U.K.)	Statutory Regulator	According to MiFID, member states shall require investment firms which execute transactions in any financial instrument admitted to trading on a regulated market to report details of such transactions to the competent authority as quickly as possible, and no later than the close of the following working day. This obligation shall apply whether or not such transactions were carried out on a regulated market. The competent authorities shall establish the necessary arrangements in order to ensure that the competent authority of the most relevant market in terms of liquidity for those financial instruments also receives this information. ESMA facilitates this via Europe's Transaction and Exchange Mechanism ("TREM") the technical system for exchanging this transaction data. The regulators in Europe generally collect the following audit trail data: • Time and date of the day the transaction was concluded. • Identification of the companies involved in the transaction (including client IDs in most European jurisdictions as part of transaction reports). • Name of the stock exchange, if the transaction was conducted on one. • Designation of the security or the derivative, with their ISIN or national identification number. • The market price of the security or derivative traded. • The traded amount. • Purchase or sale. • A recognition code specifying whether the transaction involved was concluded for the reporting party's own account or not.
Hong Kong	**Securities and Futures Commission (SFC)** Statutory Regulator	• All orders and trades data (up to brokers' level), including cancelled, amended and revoked orders, is collected for the purposes of detection of trading malpractices. • Data for short selling flags of stocks (up to brokers' level) and short position data (up to ultimate client level) for key index constituent and financial stocks. • Large positions data and position limit data (up to ultimate client level) in relation to the futures market and the

Standing Committee Jurisdiction	Respondent (Statutory Regulator, SRO or exchange)	Response
		stock option market. • Shareholding data for individual stocks is collected. (Currently SFC only relies on the shareholding information at participant level posted on the website of HKEx).
India	**Securities and Exchange Board of India (SEBI)** Statutory Regulator	• Data received from national RSEs includes order data (order entered, cancelled and modified), trade data, position-level of clients etc. Data received from depositories includes holding statements of clients.
Japan	**Securities and Exchange Surveillance Commission (SESC)** Statutory Regulator	• Transaction data on cash and derivatives products traded in Financial Instruments Exchanges -FIEs- (each data includes information on execution time, counterparties' names, and whether the transaction is a principal trade or an agency trade). 1) Order data (including order cancellations, order corrections) • Transaction data (execution price, quantity). • For a cash equity trade, information on whether the transaction is a short-selling/margin trading. • Long/short positions, resales/redemptions for derivatives trades. 2) Off-exchange transaction data on cash products listed on FIEs. 3) Large shareholding (5%) reports and the alteration reports on stocks etc., listed on FIEs. 4) Disclosures of material facts by the issuers listed on FIEs.
Mexico	**Comisión Nacional Bancaria y de Valores (CNBV)** Statutory Regulator	• CNBV can request any kind of information relevant to exchanges, securities firms, central depository and central counterparties. The collected data includes orders and cancellations, beneficial owners, account statements, contracts (brokerage and bank accounts, financial services, trust accounts, etc.), final settlement, large positions and the risks taken by each participant. • In addition, the CNBV can conduct investigation visits to any regulated entity, incl. on-site interviews, access to relevant records and review of non-public information.
Malaysia	**Securities Commission of Malaysia (SC)** Statutory Regulator	• Daily feed from the Exchange to SC comprises orders, trades and positions data.

Standing Committee Jurisdiction	Respondent (Statutory Regulator, SRO or exchange)	Response
Singapore	**Monetary Authority of Singapore (MAS)** Statutory Regulator	The available data includes (but is not limited to): • date and time of orders entered, traded, amended or deleted; • price and quantity of orders and trades; • the identity of the broker-dealer, along with account numbers of the orders and trades; and • market depth data, etc.
U.S.	**FINRA** SRO	• Certain types of equity-related market activity collected directly from FINRA members, including orders and related information. • OTC trade reports in exchange-listed and non-listed equity securities through either of 2 exchange-owned TRFs and the ORF, respectively. • Also obtains equities market audit trail data from industry utilities, called Securities Information Processors ("SIPs"), which collect and publicly disseminate quotations and trade reports. • FINRA also receives order book information from each RSA-client exchange. • With respect to U.S. options trading data, systems used by FINRA to conduct market surveillance incorporate exchange specific order information obtained directly from FINRA's client exchanges. Additionally, these surveillance systems incorporate 100% of options execution data (via the Consolidated Options Audit Trails System ("COATS") file) and options position information via the OCC (Options Clearing Corporation) position files. These systems also obtain inter-market quote data from OPRA, the SIP for options quote data. • With respect to fixed income instruments, FINRA collects from FINRA member firms all trade reports in TRACE-eligible instruments that are reportable to FINRA's TRACE system. • FINRA also receives transaction reports for corporate debt securities executed on the NYSE and transaction reports in municipal securities that are reported to the Municipal Securities Rulemaking Board's ("MSRB") Real Time Transaction Reporting System.
U.S.	**U.S. Securities and Exchange**	On July 11, 2012, the U.S. SEC approved Rule 613 that requires U.S. exchanges and FINRA to jointly submit a

Standing Committee Jurisdiction	Respondent (Statutory Regulator, SRO or exchange)	Response
	Commission (SEC) Statutory Regulator	comprehensive plan detailing how they would create, implement, and maintain a consolidated audit trail that must collect and accurately identify every order, cancellation, modification, and trade execution for all exchange-listed equities and equity options across all U.S. markets.[93] The SEC has dedicated automatic real-time and after fact systems that identify unusual transactions on securities exchanges and alternative trading systems. • The SEC has full authority to use information from SRO's in enforcing the federal securities laws, such as audit trails, Market Maker price movement reports, and Equity Clearing runs to investigate possible violations of the federal securities laws. • SEC MarketWatch has a variety of monitoring systems including Bloomberg, Reuters, a NASDAQ workstation, feeds from Archipelago, and feeds from all of the newswires. • Currently, to support its regulatory and enforcement activities, the Commission collects transaction data from registered broker-dealers through the Electronic Blue Sheets (EBS) system. o For a proprietary transaction, Rule 17a-25 requires a broker-dealer to provide the following information electronically upon request: 1) clearing house number or alpha symbol used by the broker-dealer submitting the information; 2) clearing house number(s) or alpha symbol(s) of the broker-dealer(s) on the opposite side to the trade; 3) security identifier; 4) execution date; 5) quantity executed; 6) transaction price; 7) account number; 8) identity of the exchange or market where the transaction was executed; 9) prime broker identifier; 10) average price account identifier; and 11) the identifier assigned to the account by a depository institution. o For customer transactions, the broker-dealer is also

[93] See footnote 10, *supra*.

Standing Committee Jurisdiction	Respondent (Statutory Regulator, SRO or exchange)	Response
		required to include the customer's name, customer's address, the customer's tax identification number, and other related account information. • Effective October 3, 2011, the SEC adopted Rule 13h-1 and Form 13H under Section 13(h) of the Exchange Act to assist in both identifying, and obtaining trading information on, market participants that conduct a substantial amount of trading activity, as measured by volume or market value, in the U.S. securities markets. Rule 13h-1 requires a "large trader," defined as a person whose transactions in NMS securities equal or exceed 2 million shares or $20 million during any calendar day, or 20 million shares or $200 million during any calendar month, to identify itself to the SEC and make certain disclosures to the SEC on Form 13H. Upon receipt of Form 13H, the Commission will assign to each large trader an identification number that will uniquely and uniformly identify the trader, which the large trader must then provide to its registered broker-dealers. Such registered broker-dealers will then be required to maintain records of two additional data elements in connection with transactions effected through accounts of such large traders (the large trader identification number, and the time transactions in the account are executed). In addition, the SEC requires that such broker-dealers report large trader transaction information to the SEC upon request through the Electronic Blue Sheets systems currently used by broker-dealers for reporting trade information. Finally, certain registered broker-dealers subject to the Rule will be required to perform limited monitoring of their customers' accounts for activity that may trigger the large trader identification requirements of Rule 13h-1. • The SEC also relies upon the National Securities Clearing Corporation's (NSCC) equity cleared report for initial regulatory inquiries. This report is generated on a daily basis by the SROs and is provided to the NSCC, in a database accessible by the Commission, and shows the number of trades and daily volume of all equity securities in which transactions took place, sorted by clearing member. The information provided is end of day data and is searchable by security name and CUSIP number.

Standing Committee Jurisdiction	Respondent (Statutory Regulator, SRO or exchange)	Response
		Since the information made available on the report is limited to the date, the clearing firm, and the number of transactions cleared by each clearing firm on each SRO, it basically serves as a starting point for an investigation, providing a tool the Commission can use to narrow down which clearing firms to contact concerning a transaction in a certain security.
U.S.	**Commodity Futures Trading Commission (CFTC)** Statutory Regulator	• Clearing Member Reports: for futures by commodity and by future, and, for options, by underlying futures contract for options on futures contracts or by underlying physical for options on physicals, and by put, by call, by expiration date and by strike price: 1. The total of all long open contracts and the total of all short open contracts carried at the end of the day covered by the report, excluding from open futures contracts the number of contracts against which delivery notices have been stopped or against which delivery notices have been issued by the clearing organization of the reporting market; 2. The quantity of contracts bought and the quantity of contracts sold during the day covered by the report; 3. The quantity of purchases of futures for commodities or for derivatives positions and the quantity of sales of futures for commodities or for derivatives positions which are included in the total quantity of contracts bought and sold during the day covered by the report, and the names of the clearing members who made the purchases or sales; and 4. For futures, the quantity of the commodity for which delivery notices have been issued by the clearing organization of the reporting market and the quantity for which notices have been stopped during the day covered by the report. • Daily Trade and Supporting Reports: include transaction-level trade data and related order information for each futures or options contract. Also time and sales data, reference files and other information as the Commission or its designee may require. • Order Data, Cancelled Data and Transaction Data. • Large Position Data: collects information on beneficial ownership of reportable positions.

Appendix D - Typical audit trail data fields that are collected by Statutory Regulators (and some SROs)

A. Equities: Audit Trail Data for Orders

The following data is typically collected for market surveillance purposes:

- Order history, including entries, amendments, cancellations and deletions.
- Timestamp (date and time of orders entered, traded, amended or deleted).
- Security ID.
- Quantity.
- Price.
- Special handling or routing instructions.
- Action (purchase or sell).
- Participant identifier.
- Order ID.
- Order pending status.
- Delete reason.

Some respondents also indicated that they collected the following:

- Market data: Quotes, BBO, market depth.
- Direct Market Access (DMA) client identifier.
- Rejected orders (incl. message timestamp, participant ID, stock identifier, side, price, reject reason).

B. Equities: Audit Trail Data for Trades

The following data is typically collected for market surveillance purposes:

- Timestamps (time and date of the day the transaction was concluded).
- Identification of the companies involved in the transaction (incl. participant identifier).
- Name of the stock exchange, if the transaction was conducted on one.
- Designation of the security, with their ISIN or national identification number.
- The market price of the security traded.
- The traded volume.
- Purchase or sale.
- A recognition code specifying whether the transaction involved was concluded for the reporting party's own account or not.
- Trade ID.
- Trade type code.
- Special trade condition codes.
- Execution information (e.g., full match or partial match).
- Trade cancellations.

Some respondents also indicated that they collected the following:

- Client identifier (e.g., tax id, beneficial owner id).
- Other client reference data (e.g., customer name, economic activity, address, date of creation, active flag, others).
- Off-exchange transaction data.
- Clearing and settlement data (e.g., clearing house number, clearing member number).
- Account number.
- Direct Market Access (DMA) client information (including identifier).
- Data for short selling flags of stocks (up to brokers' level).
- Large positions data and position limit data (up to ultimate client level) in relation to the stock option market.
- Information on whether the transaction is a short selling or margin trading.
- Aggregated data (e.g., number of entries, updates, cancels, and trades per trading member and stock).

C. Equities: Other Market Data/Information

Some respondents also indicated that they obtained the following market data/information for market surveillance analysis purposes:

- Security status messages (e.g., halted, frozen).
- Feeds from Reuters, Bloomberg, and other newswires.
- Securities lending.
- Settlement data (incl. fails).
- Shareholding data for individual stocks.
- Large shareholding report.
- Connection/session information.
- Trading interruption events.
- Company announcements / price sensitive information.
- Depository data (e.g., holding statements of clients).
- Contracts (e.g., brokerage and bank accounts, financial services, trust accounts).
- Long/short positions.
- Buy-back activity.
- Market marker data.
- Opening prices and end of day closing prices.
- Master data of participants/traders/issuers and reference market data (incl. stock name, issuer name, issuer code, CUSIP, dividend and reorganization information, currency, tick size, lot size, basis of quotation).

D. Derivatives: Audit Trail Data

The following data is typically collected for market surveillance purposes:

- Order history, including entries, amendments, cancellations and deletions, order routing and order execution.
- Timestamp (date and time orders entered, traded, amended or deleted).
- Quantity.
- Security ID.

- Designation of the security or the derivative, with their ISIN or national identification number.
- Action (purchase or sell).
- Subsequent trade execution details (e.g., trade ID, the market price of the derivative traded).
- Identification of the companies involved in the transaction (incl. participant identifier).
- Name of the stock exchange, if the transaction was conducted on one.
- A recognition code specifying whether the transaction involved was concluded for the reporting party's own account or not.
- Large positions data and position limit data (up to ultimate client level).
- Resales/redemptions for derivatives trades.
- Clearing information: settlement instructions, netting position adjustments, option exercise and delivery notifications.

Some respondents also indicated that they collected the following:

- Quote data.
- Beneficial ownership data.
- Clients' futures, options, warrants positions.
- Total long/short open positions.
- Total quantity of contracts bought and sold.
- Name of clearing members who bought or sold.

Appendix E - Mechanisms and Sources for Clock Synchronization by Jurisdiction

- Australia:
  - The ASIC Market Integrity Rules oblige Trading Venues to maintain their system clocks to a standard of UTC (AUS) +/- 20 milliseconds with timestamp precision of 1 millisecond. The Australian Government National Measurement Institute is the source reference point for UTC (AUS).

- Canada:
  - The Marketplace Rules implemented by the Statutory Regulators and the UMIR require all equity dealers and marketplaces to synchronize their various systems' time clocks "to the clock used by the Market Regulator." Guidance provided by the IIROC provides that each marketplace and participant shall synchronize their clocks with the Cesium Clock operated by the National Research Council of Canada or other atomic clock utilized for determining the International Atomic Time.
  - All data held by the MX is also time-stamped with an accuracy of $1/1{,}000^{th}$ of one second (e.g., to one millisecond). Time-stamps are synchronized with the Canadian official time source, the National Research Center atomic clock.

- U.S. securities sector:
  - NASDAQ: Systems are synchronized to the US Naval Observatory Master Clocks in Colorado Springs, CO.
  - Direct Edge: Time-stamps are synchronized against the National Institute of Standards and Technology (NIST) clock.
  - ISE: The Network Time Protocol (NTP) is used as time source and to maintain consistency in the clocks.

- U.K.:
  - LSE: The trading system is synchronized with the atomic clock.
  - BATS Europe: Utilizes a precision time protocol (PTP) and synchronizes its systems to this to ensure the accuracy of timestamps across multiple systems.
  - LIFFE: There is a system clock maintained within the overall trading architecture, which is synchronized with an atomic clock.
  - PLUS: Timestamps are synchronized across servers using NTP "daemons" pointed at www.uk.pool.ntp.org.

- Netherlands:
  - Overall trading architecture is synchronized with an atomic clock.

- Germany:
  - The TSOs of the Eurex and the FSX: Timestamps are originated within the trading engines of Deutsche Börse Group, which use a cluster of three Meinberg clocks (one per data center location) and are synchronized by GPS and DCF77 as backup; these serve the time via NTP protocol to all backend servers resulting in an overall time precision of better than one millisecond.

Appendix F - Recommendations and Principles of FSB Legal Entity Identifier Expert Group Contained in its May 2012 Report to the FSB Steering Committee

A Global Legal Entity Identifier for financial markets

Annex 2: Recommendations for the Development and Implementation of the Global LEI System

The following 35 recommendations are proposed by the FSB LEI Expert Group in order to develop and implement the global LEI system. They also include steps to be addressed by the recommended FSB LEI Implementation Group in the implementation phase of the global LEI initiative.

Recommendation 1

SETTING UP A GLOBAL LEI SYSTEM The Expert Group strongly supports the development and implementation of a global LEI system that uniquely identifies participants to financial transactions.

Recommendation 2

GLOBAL REGULATORY COMMUNITY REQUIREMENTS The LEI system should meet the requirements of the global regulatory community (including supranational organizations). The potential benefits of the LEI include: to support authorities in fulfilling their mandates to assess systemic risk and maintain financial stability; conduct market surveillance and enforcement; supervise market participants; conduct resolution activities; prepare high quality financial data and undertake other regulatory functions.

Recommendation 3

GLOBAL LEI SYSTEM GOVERNING DOCUMENTS Global LEI system High Level Principles set out the principles and commitments that specify and define the governance and structure of the global LEI system. A global LEI Regulatory Oversight Committee Charter should specify the mission, role and responsibilities of the Committee as well as the process for its establishment. Support for the High Level Principles agreement and Charter will indicate a desire to participate in the global LEI system.

Recommendation 4

SUPPORT OF FINANCIAL MARKET PARTICIPANTS The LEI system should be designed in a manner that provides benefits to financial market participants.

Recommendation 5

SYSTEM FLEXIBILITY Flexibility must be built into the global LEI system to provide the capability for the system to expand, evolve and adapt to accommodate innovations in financial markets. It must also allow the seamless introduction of new participants. To these ends, critical software and other relevant elements must be defined and made publicly available without any licensing, intellectual property or similar restrictions under open source principles. The LEI should be portable[94] within the global LEI system.

Recommendation 6

COMPETITION AND ANTI-TRUST CONSIDERATIONS The LEI system should be designed to ensure that it is not "locked-in" with a particular service provider for any key system functions or processes, and that the principles of competition are ensured on both global and local levels where appropriate. The governance framework should provide safeguards to ensure that competition principles and anti-trust considerations are upheld. The local implementation of the global LEI system should meet local anti-trust requirements.

Recommendation 7

FEDERATED NATURE OF THE LEI SYSTEM The global LEI system should support a high degree of federation and local implementation under agreed and implemented common standards.

Recommendation 8

SCOPE OF COVERAGE Eligibility of 'legal entities' to apply for an LEI should be broadly defined, in order to identify the legal entities relevant to any financial transaction. No more than one LEI shall be assigned to any legal entity.

Recommendation 9

LEI REFERENCE DATA AT SYSTEM LAUNCH The official name of the legal entity, the address of the headquarters of the legal entity, the address of legal formation, the date of the first LEI assignment, the date of last update of the LEI, the date of expiry, business registry information (if applicable), alongside a 20 digit alphanumeric code should form the basis for the global system at the launch of the global LEI initiative. For entities with a date of expiry, the reason for the expiry should be recorded and, if applicable, the LEI of the entity or entities that acquired the expired entity.

94 In this context a portable LEI means that the code could be transferred from one LOU to another LOU. This may be necessary, for example, in case of the LEI being obtained originally from a foreign LOU before a local LOU was established or if an entity changed its legal address or headquarters, etc.

Recommendation 10

REVIEW OF SCOPE OF COVERAGE AND REFERENCE DATA The Regulatory Oversight Committee should undertake regular reviews of the scope and extent of coverage of the LEI to reflect emerging regulatory and market requirements for the LEI use according to an agreed schedule. The Regulatory Oversight Committee should undertake regular reviews of the LEI reference data according to a set schedule to monitor the required changes, additions, retirements and modifications.

Recommendation 11

STANDARDS FOR THE LEI SYSTEM The LEI system should meet to the degree possible, evolving requirements of both the regulatory community and industry participants in terms of information content, scope, timeliness and availability. The Regulatory Oversight Committee is responsible for the final determination for any standards for the LEI to be utilized in the global LEI system. When proposing areas for the development of new standards, the Regulatory Oversight Committee should strongly consider utilizing existing standard setting organizations to develop such standards, provided that such organizations incorporate the requirements for the standards as determined and communicated by the Regulatory Oversight Committee.

Recommendation 12

LEI REFERENCE DATA ON OWNERSHIP The FSB LEI Implementation Group should as soon as possible develop proposals for additional reference data on direct and ultimate parent(s) of legal entities and relationship or ownership data more generally and to prepare recommendations by the end of 2012. The group should work closely with private sector experts in developing the proposals.

Recommendation 13

LEI OPERATIONAL AND HISTORICAL DATA The LEI system should maintain high quality records that retain relevant information on amendments (query, add, modify or delete of any data element) to data items as well as additional data to facilitate the surveillance and control of the system by the COU where appropriate.

Recommendation 14

CENTRAL OPERATING UNIT The mission and role of the Central Operating Unit should be to ensure the application of uniform global operational standards and protocols that deliver global uniqueness of the LEI, seamless access to the global LEI and to high quality reference data for users with depth of access controlled by appropriate access rights, as well as protocols and methods for how local systems can connect to the Central Operating Unit.

Recommendation 15

FORMATION OF THE CENTRAL OPERATING UNIT The LEI Implementation Group should develop a detailed plan for the formation of the Central Operating Unit via the establishment of a not-for-profit LEI foundation[95] by interested industry participants under the oversight of the formed LEI Regulatory Oversight Committee. The foundation would rely on industry participants, their expertise and knowledge to identify and develop the most technologically, financially and legally sound methods to implement the global LEI system in line with the standards and framework defined by the Regulatory Oversight Committee. Representatives from all geographic areas and industry sectors would be invited to participate in the preparatory work underpinning the formation of the LEI foundation as the Central Operating Unit in a manner defined by the Implementation Group.

Recommendation 16

BALANCED REPRESENTATION IN THE CENTRAL OPERATING UNIT The Regulatory Oversight Committee and LEI Implementation Group should ensure that the global LEI foundation takes account of the interests of financial and non-financial industry participants from different geographic areas and economic sectors.

Recommendation 17

LOCAL OPERATING UNITS The LEI system should allow the local provision of all LEI functions, which the Regulatory Oversight Committee determines, do not need to be centralized. The LEI system should enable the use of local languages, organization types and relationship structures as required. Procedures to integrate local systems into the global LEI system should be developed by the LEI Implementation Group in consultation with local jurisdictions and potential Local Operational Units (when available) in a way and manner that meets the global LEI system High Level Principles. The Central Operating Unit of the LEI system should be able to provide support to Local Operating Unit operations when necessary according to criteria and requirements established by the Regulatory Oversight Committee and administered by the Central Operating Unit.

Recommendation 18

LEI DATA VALIDATION The LEI system should promote the provision of accurate LEI reference data at the local level from LEI registrants. Responsibility for the accuracy of reference data should rest with the LEI registrant, but Local Operating Units have responsibility to exercise due diligence in guarding against errors, as consistent with Regulatory Oversight Committee standards, and to encourage necessary updating. The Central Operating Unit has responsibility to check registrations for global uniqueness and to coordinate reconciliation by Local Operating Units where necessary. Accuracy should be ensured at the local level by the registered entities. Self-registration should be encouraged as a best practice for the global LEI system.

[95] Or body of equivalent legal form.

Recommendation 19

LEI ISSUANCE WHEN NO LOCAL REGISTRAR AVAILABLE Whenever possible the LEI registration should take place with the relevant Local Operating Unit. When a Local Operating Unit is not available, the Regulatory Oversight Committee and a local jurisdiction (when willing to engage) should agree on approaches for local entities to obtain LEIs. The Implementation Group should develop proposals for such mechanisms via: (1) establishing a mechanism of obtaining LEIs through other Local Operating Units; (2) establishing a mechanism of obtaining LEIs from a registration facility in the Central Operating Unit; and (3) any other mechanisms that are appropriate.

Recommendation 20

SUSTAINABLE FUNDING The steady state funding of the global LEI system should be self-sustainable and reliable. The funding system should be based on an efficient non-profit cost-recovery model. The system should have two components: a local discretionary charge, and a common fee based on the number of registrations in each LOU to pay for the centralized operations in the Central Operating Unit, alongside any costs of implementing and sustaining the governance framework. Fees should be sufficiently modest not to act as a barrier to acquiring a LEI.

Recommendation 21

GLOBAL REGULATORY OVERSIGHT COMMITTEE CHARTER The governance framework of the global LEI system should be developed at the international level in an open and transparent manner that supports collective governance of the global system. A global LEI Regulatory Oversight Committee Charter should set out the formation and operations of the Regulatory Oversight Committee. The global LEI Regulatory Oversight Committee Charter should be prepared by the FSB LEI Implementation Group for endorsement by the G-20 at the Finance Ministers and Central Bank Governors meeting in November 2012 or by the FSB Plenary in October.

Recommendation 22

REGULATORY OVERSIGHT COMMITTEE A Regulatory Oversight Committee, as specified in the Charter, should have the responsibility of upholding the governance principles and oversight of the global LEI system functioning to serve the public interest. The Regulatory Oversight Committee should be a body representing regulators and other government or supranational entities engaged in regulating or monitoring the financial system or markets. The Charter would establish membership and decision-making processes. Wherever possible, decisions would be reached by consensus.

Recommendation 23

POWER AND AUTHORITY OF THE REGULATORY OVERSIGHT COMMITTEE The Regulatory Oversight Committee has the ultimate power and authority over the global LEI system. Any power delegated to the Central Operating Unit, Local Operating Units and other entities can be reversed by the Regulatory Oversight Committee.[96] The Regulatory Oversight Committee should establish a formal oversight plan to ensure that its directives to the Central Operating Unit or other parts of the system are enforced and that the governance principles are upheld.

Recommendation 24

PARTICIPATION IN THE REGULATORY OVERSIGHT COMMITTEE To participate in the LEI Regulatory Oversight Committee, an authority should indicate support for the global LEI High Level Principles and Charter for the Regulatory Oversight Committee. Authorities may elect to be a full member of the Regulatory Oversight Committee or an observer. The rights and responsibilities of members and observer status participants should be defined in the Charter.

Recommendation 25

LEVERAGING INFRASTRUCTURE OF AN INTERNATIONAL FINANCIAL ORGANISATION In developing proposals to establish the Regulatory Oversight Committee following agreement on the Charter, the Implementation Group should if possible and, subject to agreement, leverage on the existing infrastructure of an international financial organization to initiate and stand-up the global LEI governance structure in a timely manner, utilizing the experience of the international organization in executing international initiatives.

Recommendation 26

GOVERNING DOCUMENTS FOR THE CENTRAL OPERATIONAL UNIT Alongside the development of the global Charter, the Implementation Group should develop legal documents governing the mandate the Regulatory Oversight Committee to the Central Operating Unit as well as other legal documents needed to specify the full governance framework for the global LEI system.

Recommendation 27

BOARD OF DIRECTORS OF THE CENTRAL OPERATIONAL UNIT The Central Operations Unit shall have a Board of Directors. The Regulatory Oversight Committee has the right to veto membership of the BOD, as well as to remove members. The ROC has the right to appoint independent members.[97]

---

96 Local authorities may also reserve rights to be engaged in decisions on local registration operations to the extent that they act in accordance with the high-level principles of the LEI system.

97 In this context independent members mean non-industry representatives.

Recommendation 28

FORMATION OF THE INITIAL BOARD OF DIRECTORS OF THE CENTRAL OPERATIONAL UNIT The Central Operating Unit's initial Board of Directors should be appointed by the Regulatory Oversight Committee, taking into account the need for geographic and sectoral diversity. The Implementation Group should develop the fitness criteria, size, role etc. for the BOD that should be reviewed in two years by the Regulatory Oversight Committee.

Recommendation 29

POWERS AND FUNCTIONS OF THE BOD OF THE CENTRAL OPERATING UNIT The Board of Directors of the Central Operating Unit should be granted powers to direct the management and operations of the Central Operating Unit in line with the overall standards set by the Regulatory Oversight Committee.

Recommendation 30

CONTINGENCY ARRANGEMENTS The Regulatory Oversight Committee is responsible for setting and overseeing the application of business continuity standards for the global LEI system in line with best practices for key financial infrastructure. Rules and procedures should be defined that the Central Operating Unit and Local Operating Units must follow in case of insolvency, bankruptcy, etc. in order to ensure continuity of the global LEI system. A protocol should also be developed for maintenance of secure parallel copies of the LEI, in a manner that respects local laws.

Recommendation 31

LEI INTELLECTUAL PROPERTY The LEI Implementation Group should conduct analysis and provide recommendations on the treatment of the "LEI" intellectual property (such as the LEI code, software, reference data, any other LEI data, operational protocols, etc.) according to the principles of open access and the nature of the LEI system as a public good. The objective of this analysis shall be to ensure a regime that assures the availability in the public domain, without limit on use or redistribution, of LEI data, reference data, and processes. Any intellectual property rights should be held by, or licensed to the global LEI foundation unless defined otherwise by the Regulatory Oversight Committee. Copyright should be used to the extent possible to promote the free flow or combination of information from disparate sources.

Recommendation 32

FSB LEI IMPLEMENTATION GROUP Subject to the G-20 supporting further work to launch the global LEI, and entrusting implementation planning to the FSB, an FSB LEI Implementation Group should be established with a clear mandate to launch the global LEI system on a self- standing basis. The LEI Implementation Group should cease to exist upon formation of the Regulatory Oversight Committee, which should be by 31 March 2013 at the latest.

Recommendation 33

STRUCTURE OF THE FSB LEI IMPLEMENTATION GROUP A time-limited FSB LEI Implementation Group (IG) of interested and willing experts (legal, IT, and other) from the global regulatory community that includes interested parties from the FSB LEI Expert Group should be formed to take the global LEI initiative forward into the global implementation phase until the Regulatory Oversight Committee is established. The IG should be led by a chair and two vice-chairs or three co-chairs from different geographic areas to reflect the global nature of the LEI initiative and will be supported by the FSB Secretariat. The IG should develop proposals for the global LEI system stand-up as defined in the mandate below for review and endorsement by the FSB Plenary in October 2012 and [final review and endorsement by G-20 Finance Ministers and Central Bank Governors and Deputies in November 2012].

Recommendation 34

RESPONSIBILITIES OF THE FSB LEI IMPLEMENTATION GROUP The mandate of the FSB LEI Implementation Group should be to prepare a draft global LEI Regulatory Oversight Committee Charter, proposals for the establishment of the LEI Regulatory Oversight Committee and related structures, develop all necessary legal documents for Regulatory Oversight Committee operations, develop necessary intellectual property agreements and contracts, conduct research and provide recommendations on LEI related information sharing arrangements; set up the process and any necessary legal documentation necessary for establishment of the Central Operational Unit and its Board of Directors; and set up the process for establishment of the necessary standards, protocols, rules and procedures and organizational design for the Central Operating Unit.

Recommendation 35

ESTABLISHMENT OF THE GLOBAL LEI SYSTEM The global LEI system will be established by the endorsement of the high level Charter for the Regulatory Oversight Committee [by the G-20 Finance Ministers and Governors in November]/[FSB Plenary in October]

Annex 3 to the Expert Group's Report: Global LEI System High Level Principles

The global LEI System High Level Principles have been prepared by the FSB LEI Expert Group to guide the development of the global LEI system, in line with the G-20 mandate of developing a governance framework that represents the public interest. The recommendations for the development and implementation of the global LEI system in Annex 2 draw on the proposed High Level Principles.

1. The Global LEI system should uniquely identify participants to financial transactions.

2. The LEI system should meet the requirements of the global regulatory community for accurate, consistent and unique entity identification.

3. The LEI system should be designed in a manner that provides benefits to financial market participants.

4. Flexibility must be built into the global LEI system to provide the capability for the system to expand, evolve, and adapt to accommodate innovations in financial markets.

5. The LEI system should not be “locked-in” with a particular service provider for any key system functions or processes. The principles of competition should be ensured on both global and local levels where appropriate.

6. The global LEI system should support a high degree of federation and local implementation under agreed and implemented common standards.

7. The LEI system should meet evolving requirements of both the regulatory community and industry participants in terms of information content, scope of coverage, timeliness and availability.

8. The LEI Regulatory Oversight Committee should have the responsibility of upholding the governance principles and oversight of the global LEI system functioning to serve the public interest. The Committee has the ultimate power and authority over the global LEI system.

9. The mission, role and responsibilities of the ROC shall be specified by the global LEI Regulatory Oversight Committee Charter, which shall establish the Committee.

10. Participation in the global LEI Regulatory Oversight Committee shall be open to all authorities subscribing to the High Level Principles and to the objectives and commitments in the Charter.

11. The LEI Central Operating Unit should have the mission and role to ensure the application of uniform global operational standards and protocols set by the ROC and act as the operational arm of the global LEI system. It shall be established as a foundation or legal equivalent.

12. The LEI Central Operating Unit should have a balanced representation of industry participants from different geographic areas and sectors of economy. Its Board of Directors should be selected from industry representatives, plus independent participants.

13. The LEI system should allow the local provision by Local Operating Units of all LEI functions, which the ROC determines, are not required to be centralized.

14. The LEI system should promote the provision of accurate LEI reference data at the local level from LEI registrants and ensure global uniqueness of the registrants.

15. Any global universal intellectual property rights should belong to the global LEI system.

Appendix G - Feedback Statement to Comments Received on Consultation Report

I. Under Recommendation I (questions 1-3)

A. Questions

> ***Question 1)*** *What regulatory capabilities are, in general, needed in order for Market Authorities to survey for and detect market abuse that occurs on a cross-asset and cross-market basis? How can such abuse be best detected and combated?*

commenters support standardizing data, which is explored in greater depth below (Question 11).[98]

Three commenters noted that Market Authorities require greater funding.[99] Two of the three commenters arguing for greater funding also argued for a strongly worded regulatory mandate conferring Market Authorities with strengthened enforcement and settlement powers.[100]

One commenter suggested market surveillance authority should be enshrined in national legislation that clearly delineates the scope of violations, financial instruments and trading venues that are subject to the mandate, that provides for rulemaking powers to the authority as to adapt to changes in the market and that specifies investigative and enforcement powers.[101]

> ***Question 2:*** *Do you think existing systems (e.g., audit trail systems) in your jurisdiction monitor effectively electronic trading (both cross-market and cross-asset), i.e., are they able to ensure the fair and orderly functioning of Trading Venues and to promote market integrity? Please explain and describe any enhancements that you believe are necessary. Are the necessary resources for effective systems available?*

Commenters provided a plethora of elements necessary for an effective audit trail system. The most common suggestions were that an effective audit trail system needs identifiers for orders, clients, time, trades and quotes.[102]

Of the limited amount of commenters addressing Question 2, two commenters found that audit trail systems could be improved through a more efficient mechanism for transferring order books from other jurisdictions.[103] Additional suggestions for improvements include standardization of data type included in audit trails as to promote cross-jurisdictional

---

98 Avenues; Crispin; FSB; Amafi; Hessian, Eurex and Frankfurt Exchanges; FIA; Central Bank of Ireland; FIX; FESE.

99 Avenues; Crispin; ICI.

100 Avenues; Crispin.

101 FINRA.

102 Hessian, Eurex and Frankfurt Exchanges (argued for automated way to exchange data between regulators and for identifiers for orders, trades, and quotes); FSB (supports being able to identify trading down to client level and to identify time of transaction); BATS (real time supervision, complete records of orders and trades); FESE.

103 Hessian, Eurex and Frankfurt Exchanges; Central Bank of Ireland.

compatibility,[104] a consolidated tape that publishes pre and post trade data from across all Trading Venues,[105] periodical evaluation of surveillance capabilities by authorities[106] and an audit trail regime similar to SEC's CAT.[107]

> ***Question 3:*** *To be able to perform effectively market surveillance, to what extent should Market Authorities have the ability to reconstruct and analyse order books? Why or why not?*

Commenters answering this question unanimously agreed that effective surveillance requires the ability to reconstruct and analyze order books.[108] Reconstructing and analyzing books is necessary to detect abusive behaviors (price manipulation, misleading impression by placing orders without trading intention)[109] and to have full overview of trading strategies employed.[110]

Two commenters pointed out impracticalities that may be associated with reconstructing and analyzing order books, namely costs of reconstructing books across multiple venues and asset classes, storage costs and administrative costs.[111]

B. Feedback to comments on Recommendation 1

Recommendation 1 remains unchanged from the Consultation Report, as the public comments were largely consistent with it. Commenters did, however, express specific views as to what is needed to ensure that Regulators have the organizational and technical capabilities to monitor effectively the Trading Venues they supervise. For example, commenters confirmed that access to trading data (*see also* Recommendation 3) is the key capability that Market Authorities should have and that cooperation between Trading Venues and regulators plays an essential role of facilitating that capability. They stressed the importance of Market Authorities having access to data from local market participants, remote market participants, other Market Authorities, and domestic and foreign Trading Venues and that effective surveillance requires the ability to reconstruct and analyze order books. Commenters suggested that an effective audit trail system needs identifiers for orders, clients, time, trades and quotes. There was a general consensus that a key improvement that could be made in current systems might be the standardization of data type included in audit trails as to promote cross-jurisdictional compatibility, such as through a consolidated tape that publishes pre- and post trade data from across all Trading Venues, periodical evaluation of surveillance capabilities by authorities or an audit trail regime similar to SEC's CAT.

II. Under Recommendation 2 (questions 4 - 7)

---

104 FIA; Crispin.

105 BATS.

106 FINRA.

107 ICI.

108 Avenues, Hessian, Eurex and Frankfurt Exchanges, Crispin, Amafi, FSB, FIA, NASDAQ, Central Bank of Ireland, FIX, FESE, ICI, SEC Pakistan.

109 Avenues; Crispin; Hessian, Eurex and Frankfurt Exchanges.

110 Central Bank of Ireland.

111 FIA; Central Bank of Ireland.

A. Questions

Question 4: *Do you think that developments in technology have impacted Market Authorities' ability to monitor markets? If so, how?*

All commenters who addressed this question acknowledged the impact of technology on Market Authorities' ability to monitor markets.[112] Technology has led to sophisticated strategies and greater transaction speeds, but Market Authorities have failed to fully utilize the gains associated with developments in technology and are playing catch up.[113] Some argue that the negative impact of technology is not the speed associated with technology. Instead, the corresponding increase in volume and missing identifiers has made it more difficult for Market Authorities to monitor markets.[114]

Potential positive impacts of technology on Market Authorities' ability to monitor markets include the ability to monitor through the use of automated alerts and the ability to capture all information about an order or trade executed on a market.[115]

Question 5: *Are there specific developments that have impacted this ability more than others? If so, which ones?*

A plurality of commenters identified algorithmic and/or high frequency trading as having the greatest impact on Market Authorities' ability to monitor.[116] One commenter noted that the current regulatory framework may not be properly designed to address changes in applied technology. It further stated the idea of a registered trader who actually executes a trade is dated. Today, in their view, it is more likely a "responsible person" overseeing running algorithms. Moreover, in many firms, there is no single contact person who knows in depth the applied algorithm and could explain a concrete decision underlying a trading strategy. This makes it difficult to conduct a criminal investigation insofar as there is a need to prove human intent to commit an act.[117]

Two commenters identified the ability to trade in multiple markets across borders as a development that has had the largest impact on Market Authorities' ability to monitor because trading across borders and in multiple markets has made it easier for market participants to disguise market abuses.[118]

---

112 Hessian, Eurex and Frankfurt Exchanges; FIA; FSB Crispin; Central Bank of Ireland; FESE; AMAFI; BATS; Avenue.

113 BATS; Avenues; FESE; Crispin.

114 Hessian, Eurex and Frankfurt Exchanges; NASDAQ.

115 FIA; FSB; Avenue.

116 Avenues; Crispin; Central Bank of Ireland; BATS.

117 Hessian, Eurex and Frankfurt Exchanges.

118 BATS; SEC Pakistan.

Two commenters spoke specifically on the European experience, *i.e.*, MIFID's impact on the markets. MIFID has caused greater fragmentation of liquidity, which has had the largest impact on Market Authorities' ability to monitor markets.[119]

> ***Question 6:*** *To what extent have you identified instances of market abuse or possible market abuse, including inappropriate activity that could (or has) lead to disorderly markets, which you feel is directly related to the misuse of automated trading technology? Please provide details.*

For example: Do you believe your jurisdiction has experienced market infrastructure disruptions caused by automated trading, including HFT/algorithm use, that have caused network traffic or processing to exceed the capacity of Trading Venues, key market information providers or large market participants? If so, please describe.

No commenter identified deliberate misuse of automated trading technology.[120] Commenters, however, noted that malfunctions in technology have created disorderly trading.[121]

> ***Question 7****: Have there been any developments other than technology that have impacted Market Authorities' ability to monitor the markets? Please provide details.*

Commenters offered a variety of other developments that have impacted Market Authorities' ability to monitor the markets: fragmentation of trading venues and markets,[122] increasing complexity of financial products,[123] a greater variety of domestic and foreign market participants,[124] the lack of readily available accurate data,[125] under-regulated and unregulated markets,[126] the introduction of DMA[127] and increased trade volumes- though this seems to be a

---

119 FESE; Amafi; see also NASDAQ (NASDAQ points to fragmentation, increasing number of smaller traders and high numbers of order per trade).

120 Avenues; Hessian, Eurex and Frankfurt Exchanges; Amafi; FSB; NASDAQ; BATS; Central Bank of Ireland; SEC Pakistan.

121 NASDAQ ("European surveillance has never encountered such deliberate abuse that aims at disrupting a trading system or information flow. We have however encountered different situations where malfunctions in technology have created disorderly trading"); ICI ("There have been a number of recent instances of market infrastructure disruptions in the financial markets that have been related in one way or another to the use of technology in trading. ICI and ICI Global therefore have supported the establishment of robust pre- and post-trade risk controls to prevent systems from generating and sending orders to the market that may be erroneous or not compliant with applicable regulatory requirements. One issue that we believe should be examined by Market Authorities is the increasing number of order cancellations in the markets, particularly those that are cancelled shortly after submission").

122 NASDAQ; BATS; FESE; ICI; Crispin; FIA.

123 Avenues; Crispin.

124 Crispin; SEC Pakistan.

125 Central Bank of Ireland.

126 Crispin (referring to dark pools and OTC products).

127 Hessian, Eurex and Frankfurt Exchanges ("The introduction of DMA (or from a German perspective order-routing) eroded basic regulatory exchange set-up. During investigations this may lead to long loops (long chains of order submitters). And in general there is limited scope with respect to the market places rules and regulations and whether these are applicable to DMA clients (no direct jurisdiction)"); NASDAQ.

byproduct of technology instead of a separate development.[128] markets,[129] the introduction of DMA[130] and increased trade volumes- though this seems to be a byproduct of technology instead of a separate development.[131]

B. Feedback to comments on Recommendation 2

This recommendation remains unchanged from the Consultation Report, as many commenters acknowledged the impact of technology on Market Authorities' ability to survey markets, along with the corresponding increase in trade volume, the absence of customer identifiers (*see* Recommendation 4) and the ability of customers to trade in multiple markets across borders (*i.e.*, fragmentation). They noted that technology has led to sophisticated strategies and greater transaction speeds (with a plurality of commenters identifying algorithmic and/or high frequency trading as having the greatest impact on Market Authorities' ability to monitor), but that Market Authorities have not always taken advantage of the gains offered through technological developments, such as automated alerts and systems that can capture all information about an order or trade executed on a market. Thus, the public comments generally confirmed the need for Market Authorities to review regularly and update as appropriate their surveillance capabilities remains critically important.

III. Under Recommendation 3 (questions 8-9)

A. Questions

> ***Question 8:*** *To what extent do you think that a Central Reporting Point is necessary within a domestic market in order to conduct surveillance effectively, particularly across markets and/or assets? In other words, to what extent would the development of audit trail systems that are able to consolidate pre- and post-trade data across Trading Venues within a domestic market be beneficial? Please explain your answer.*
> *a. To the degree that you advocate a Central Reporting Point, what kind of data would be needed for your respective surveillance tasks, e.g., order data/transactions data, both? What are the impediments to introducing these systems? What are the benefits?*
> *b. What are the potential costs associated with the establishment of a Central Reporting Point?*

Six commenters clearly supported the creation of a CRP.[132] However, one of them suggested as an alternative that there could "be enhanced pre-trade transparency and pre-trade risk

---

FIA; ICI ("While arguably related to technology, we believe that the fragmentation of the financial markets and the submission of large numbers of orders and trades across multiple venues have contributed to the difficulties for Market Authorities to effectively monitor the markets").

129 Crispin (referring to dark pools and OTC products).

130 Hessian, Eurex and Frankfurt Exchanges ("The introduction of DMA (or from a German perspective order-routing) eroded basic regulatory exchange set-up. During investigations this may lead to long loops (long chains of order submitters). And in general there is limited scope with respect to the market places rules and regulations and whether these are applicable to DMA clients (no direct jurisdiction)"); NASDAQ.

131 FIA; ICI ("While arguably related to technology, we believe that the fragmentation of the financial markets and the submission of large numbers of orders and trades across multiple venues have contributed to the difficulties for Market Authorities to effectively monitor the markets").

132 Avenues; Amafi; Crispin; NASDAQ; ICI; SEC Pakistan.

management at the point of the broker-dealer" (*e.g*, where broker-dealers would "exercise more due diligence into investigating if a client should be granted DEA" or by taking other "post-trade risk management initiatives)."[133] In addition, among those that supported the creation of a CRP, many noted that fragmentation of markets and the possible need for several CRPs (*e.g.*, in the "European trading space") would be an obstacle to overcome.[134]

Three commenters[135] impliedly expressed some support for a CRP, but also stated that the concept merits further investigation and should be subject to a cost-benefit analysis. They argued that a CRP in itself is not a functional necessity, and that it may not make sense for all market structures. Several of these commenters suggested alternatives to a CPR, such as the development of standardized machine readable surveillance language to address automatically cross-market and cross-asset investigations[136] or the enhancement of existing audit trails by collecting consistent types of data to facilitate aggregation in more targeted surveillance investigations.[137]

Three commenters clearly did not support the creation of a CRP[138] and offered alternative solutions, such as the establishment of a consolidated tape for the trade data of a particular security[139] or enhancement of the current ability to obtain data during an investigation as required by the relevant market authority.[140]

Data Necessary, Impediments and Costs:

CRP supporters suggest that the data necessary for a CRP includes order data and transaction data,[141] while some want all order book activities.[142] The impediments to access to such data are primarily related to client confidentiality,[143] competitive sensitivity,[144] possible commercial

---

133 Crispin

134 Avenues; FESE ("Any model for market surveillance that imposes a Central Reporting Point (CRP) would still need to overcome the obstacle of having several CRP's in the European Trading Landscape that would need standard harmonized interfaces to exchange data, automate surveillance requests and to enable collaborative joint investigations across multiple venues and strict legislation to ensure that requests for information are adhered to and that no request goes unanswered"); Amafi.

135 Hessian, Eurex and Frankfurt Exchanges ("A CRP is more a design issue than a functional necessity. It is more a question whether the ability to conduct a cross/market and asset investigation does exist...Many stylized facts of abusive behavior are detectable within a sub-set of data, thus not for all abusive schemes centralizing in terms of aggregating is necessary"); North Rhine-Westphalia ("The Exchange Supervisory Authority does not support the idea of installing a CPR that is not authorized to administrate market surveillance at the same time"); FIA ("…the cost and complexity of collecting and storing audit trail data in a CPR across multiple asset classes and jurisdictional boundaries is tremendously expensive").

136 Hessian, Eurex and Frankfurt Exchanges.

137 FIA.

138 London Stock Exchange; BATS; Central Bank of Ireland.

139 BATS.

140 Central Bank of Ireland.

141 FSB; Central Bank of Ireland.

142 Avenues.

143 Avenues.

144 Avenues.

conflicts of interest,[145] and non-standardized information (especially a problem for integrating multiple systems into a single CRP).[146]

Commenters' projection on potential costs range from as low as 100mm Euros[147] to as high as $4 billion to establish and $1.7 billion annually to maintain a CRP.[148] Most commenters simply stated that the cost of establishing a CRP would be high, but economies of scale will mitigate some costs.[149] A key cost of establishing a CRP is the transfer/storage of data.[150]

Commenters Not in Support of Establishing a CRP:

Two commenters point to the cost and complexity of establishing and maintaining a CRP across multiple assets and jurisdiction boundaries and noted that a CRP is not necessarily cost effective.[151] Instead, a commenter suggested Market Authorities consider ways to collect data in a consistent manner with sufficient identifiers to facilitate cost-effective, tailored investigations.[152] Another commenter suggested Market Authorities use transaction reporting, which would enable Market Authorities to perform ex-post investigations on market abuses.[153]

Only one commenter believes that the current mechanisms are adequate and no CRP is necessary.[154]

> ***Question 9:*** *Are there alternatives to a Central Reporting Point that can achieve the same end? Please explain.*

"Standardization" is a central theme among comments for alternatives to a CRP.[155] Commenters proposed standardization of surveillance language to facilitate automated cross-market and cross-border investigations. The idea: "Let surveillance systems interact with each other given a common framework of 'how' and 'what.'"[156]

---

145 Avenues.

146 Central Bank of Ireland; Amafi.

147 Avenues.

148 Crispin.

149 North Rhine-Westphalia; Amafi ("There is no doubt that Central Reporting Points are less costly than multiple systems…also economies of scale of a single system largely compensate the transfers of multiple systems towards one single").

150 Central Bank of Ireland; Crispin.

151 FIA; London Stock Exchange Group.

152 FIA.

153 London Stock Exchange Group.

154 BATS ("The current model, whereby Trading venues supervise activity on their own markets, supplemented by the enhanced ability to monitor cross market that a consolidated tape would provide and the receipt of Transaction Reports by Statutory Regulators together provide an effective framework for surveillance across markets and asset classes").

155 Hessian, Eurex and Frankfurt Exchanges; FIA; FIX; Central Bank of Ireland ("In our case a workable solution would be to obtain the data during an investigation as required from the relevant market authority and therefore if there is a seamless and efficient integration, our objectives could be met").

156 Hessian, Eurex and Frankfurt Exchanges.

Other alternatives include: consolidated tape capturing pre and post trade for the trading of particular security,[157] customer identification,[158] transaction report,[159] readily available audit trail[160] and enhanced pre-trade transparency and risk management by broker-dealers.[161]

See also summary to Question 8.

B. Feedback to comments on Recommendation 3

One of the key questions posed underneath this Principle in the Consultation Report was the extent to which commenters believed that a Central Reporting Point (CRP) is necessary within a domestic market in order to conduct surveillance effectively, particularly across markets and/or assets. A review of the public comments to the Consultation Report reveals some support for the development of a CRP as a tool that can enable market authorities to access the data they need to conduct effective surveillance. However, it is equally clear that a number of commenters believe that in light of the costs and other issues associated with the development of a CRP, and in light of specific market structures, alternative tools for organizing effective surveillance may also be appropriate. Consistent across all comments, however, is the idea that relevant Market Authorities should individually or collectively have the capability to access data in a way that enables them to conduct effective surveillance. We believe that these collective comments are wholly consistent with Recommendation 3, as proposed in the Consultation Report. We have therefore not modified the recommendation.

IV. Under Recommendation 4 (question 10)

A. Questions

> ***Question 10:*** *To what extent should market surveillance systems or audit trails require the provision of customer identifiers? What are the impediments to providing customer identifiers in audit trail data?*

The near unanimous consensus is that customer identifiers should be used.[162] However, a significant number of commenters identified confidentiality and legal concerns preventing the use of customer identifiers.[163] These commenters proposed alternative identifiers, based on trading venue or market[164] or internal client identifiers on transaction reports submitted to Statutory Regulators.[165] Other commenters did not note the legal and confidentiality issues or

---

157 BATS.

158 FESE, Central Bank of Ireland.

159 London Stock Exchange Group.

160 SEC Pakistan.

161 Crispin ("There can be enhanced pre-trade transparency and pre-trade risk management at the point of the broker-dealer. Brokers should exercise more due diligence into investigating if a client should be grated DEA. There are also examples of firms that have undertaken post-trade risk management initiatives").

162 Avenues; Hessian, Eurex and Frankfurt Exchanges; Crispin; Amafi; FSB; FIA; NASDAQ; Central Bank of Ireland; ICI; SEC Pakistan; BATS; FINRA.

163 Avenues; Hessian, Eurex and Frankfurt Exchanges; Amafi; BATS.

164 Eurex and Frankfurt Exchanges.

165 BATS.

found that issues could be overcome and support the development of a global legal entity identifier ("LEI").[166]

B. Feedback to comments on Recommendation 4

The commenters to this recommendation focused on "customer identifiers." The near unanimous consensus was that customer identifiers should be used. However, a significant number of them also identified confidentiality and legal concerns preventing the use of customer identifiers. Nonetheless, the underlying theme of the public comments was that Market Authorities (individually or collectively) should have the capability to associate the customer and market participant with each order and transaction, recognizing the practical difficulties in achieving this, particularly in a cross-border situation. The recommendation therefore remains unchanged from the proposal in the Consultation Report.

V. Under Recommendation 5 (questions 11-12)

A. Questions

> ***Question 11:*** *What regulatory steps, if any, should Market Authorities take in order to help ensure that any data reported to them for use and storage is in a usable format?*

Commenters addressing this question came to the unanimous consensus that standardization of data would aid Market Authorities in monitoring markets.[167] Commenters, however, offered varied steps on how data should be standardized. A number of commenters suggested that Market Authorities work with the industry to establish a common standard.[168] A small number of commenters argued that IOSCO should lead by recommending a usable format.[169]

As to the reach of standardization, commenters support an international standard.[170]

> ***Question 12:*** *To what extent are you concerned about the ability of Market Authorities to reconstruct and analyze order book(s) in the correct sequence? What tools are necessary to do so?*

Most commenters are concerned about Market Authorities' ability to reconstruct and analyze order books and point to a host of necessary tools to reconstruct and analyze order books.[171] Most commenters point to mapping correct sequencing of order books as a major concern and a

---

166 ICI; Crispin; Avenues; FIA.

167 Avenues; Hessian, Eurex and Frankfurt Exchanges; Crispin; Amafi; FIA; NASDAQ; Central Bank of Ireland; BATS; SEC Pakistan; FIX (argues for the use of non-proprietary, free and open industry standards); FINRA.

168 Hessian, Eurex and Frankfurt Exchanges; Amafi ("In the EU[,] the current situation is not satisfactory because of the lack of harmonization of reference and format data. The Market Authorities should develop in liaison with the industries common standards").

169 Crispin; Avenues.

170 BATS; Central Bank of Ireland.

171 NASDAQ believes Market Authorities are able to reconstruct order books.

hurdle for Market Authorities. Mapping sequences correctly requires the finest timestamp granularity and time stamp synchronization.[172]

B. Feedback to comments on Recommendation 5

Commenters to the Consultation Report unanimously agreed that Market Authorities should take the steps necessary to standardize data, as this would aid Market Authorities in more effectively monitoring markets. They offered various ideas on how data should be standardized. For example, a number of commenters suggested that Market Authorities work with the industry to establish a common (*e.g.*, international) standard.

IOSCO believes that the recommendation in the Consultation Report reflects the views of commenters as it also emphasizes that data should be reported to Market Authorities in a usable format, which could significantly enhance the ability of Market Authorities to reconstruct and analyze order books. The recommendation therefore remains unchanged from that proposed in the Consultation Report.

VI. Under Recommendation 6 (questions 13-14)

A. Questions

Question 13: *To what extent are current confidentiality provisions sufficient? If not, how can they be strengthened?*

Significant shares of commenters believe the current confidentiality provisions are sufficient,[173] but standards need to be applied to how data is kept and how the networks in which the data is accessed are maintained.[174] Additionally, some commenters raised concerns about the use of data to prosecute other illegal conduct outside of market manipulation and abuse, such as tax fraud.[175]

One commenter argued for legislation to strengthen and enshrine confidentially of data.[176] Similar to legislation enshrining confidentiality, a commenter suggested a written code of

---

172 Avenues (Market Authorities need the ability to map correct sequences); SEC Pakistan (Market Authorities need to be able to reconstruct order book in correct sequence); FIA (need to be able to accurately sequence); Hessian, Eurex and Frankfurt Exchanges (need finest timestamp granularity); BATS (Trading venues must use a standardized time source for time stamps. If time stamps are consistent then Statutory Regulators can request order book reconstructions from Trading Venues when required and, depending on the capabilities of their systems, create a consolidated view"); NASDAQ (Market Authorities must "have the right structure in place (synchronized timestamps, [stop orders, 'how volume adjustments are handled with orders that have partially hidden volume'] and data sourced from trading venues)"); Central Bank of Ireland (need more accurate timestamps); FIX (need sequential identification); FSB (concerned with ability to reconstruct order books but not in its jurisdiction).

173 Hessian, Eurex and Frankfurt Exchanges; FSB; FESE (current safeguards among trading venues has proved to work well, but "confidentially of data must be enshrined in legislation to create confidence between trading venues and Regulators"); SEC Pakistan (only looking at its jurisdiction).

174 Hessian, Eurex and Frankfurt Exchanges; FSB; FIA; Central Bank of Ireland (speaks only of its jurisdiction); SEC Pakistan (speaks only of its jurisdiction).

175 Hessian, Eurex and Frankfurt Exchanges; NASDAQ (confidentiality of information is essential and such information should only be used for surveillance purposes); ICI.

176 FESE.

conduct that sets forth fundamental requirements for employees to protect sensitive and non-public disclosures.[177] Another commenter raised a whistle blower issue associated with disclosure of suspicious transaction to authorities and suggested steps be taken to ensure that whistle blower's identity is not revealed by a Market Authority.[178]

One commenter distinguished confidentiality needs between Statutory Regulators and non-Statutory Regulators, noting that, "If the Market Authority is not a Statutory Regulator, then extra safeguards should be put in place to ensure that there is no leakage of sensitive or commercially confidential information."[179]

> ***Question 14:*** *To what extent should Market Authorities be able to obtain surveillance data from other Market Authorities, whether inside or outside their jurisdiction, relating to securities trading, including the identity of customers? What issues are raised? Please explain your answer.*

Nearly every commenter supported Market Authorities' ability to obtain surveillance necessary data from other Market Authorities.[180]

Issues raised include differing regulatory requirements,[181] safeguarding proprietary surveillance methodology and data,[182] differing surveillance technology platforms,[183] non-standardized data format[184] and deciding cost-sharing mechanisms.[185]

B. Feedback to comments on Recommendation 6

Nearly every commenter to the Consultation Report thought that it was important for Market Authorities to be able to obtain the data they need from other Market Authorities (domestic or foreign) in order to conduct effectively securities market surveillance. Most commenters to the Consultation Report impliedly agreed with the recommendation by stating that existing confidentiality provisions are sufficient (no matter where data is currently obtained), while emphasizing that there must be standards both with regard to how data is kept and how data-access networks are maintained. For this reason, the recommendation is unchanged from the proposed recommendation in the Consultation Report.

VII. Under Recommendation 7 (question 15)

---

177 FINRA.

178 Amafi.

179 BATS.

180 Avenues; Hessian, Eurex and Frankfurt Exchanges; Crispin; FSB; NASDAQ; Central Bank of Ireland; ICI; SEC Pakistan. In contrast, BATS believes that trading venues, even where they are a "market authority," should not be permitted to directly request data from other venues.

181 Crispin.

182 Central Bank of Ireland (issues that might be raised include differences in terms of data protection rules); SEC Pakistan; Crispin.

183 Crispin.

184 Central Bank of Ireland.

185 Crispin.

A. Questions

Question 15: *To what extent do you think there would be value in requiring Trading Venues and market participants to attach a synchronized time-stamp to their orders reflecting when that order was sent?*

Most commenters support synchronized clocks[186] but one commenter noted the physical limits ("no perfect time synchronization exists"),[187] while another noted the practical limits, such as accurately synchronizing timestamps within a fragmented market with multiple trading venues and market participants.[188]

One commenter was skeptical about synchronization of business clocks and calls for further cost-benefit analysis.[189]

B. Feedback to comments on Recommendation 7

Most commenters to the Consultation Report supported the synchronization of business clocks, while recognizing real world challenges, such as seeking to synchronize accurately timestamps within a fragmented market with multiple trading venues and market participants. This is largely consistent with the recommendation proposed in the Consultation Report, which recognized the importance of business clock synchronization, but only suggests that Market Authorities *consider* requiring Trading Venues and other participants within their jurisdiction to synchronize business clocks, consistent with industry standards. Thus, the recommendation is not changed in the Final Report as it already recognizes the practical challenges noted by the commenters.

VIII. Under Recommendation 8 (questions 16-17)

A. Questions

Question 16: *What steps, if any, should Market Authorities take to facilitate cross-border surveillance? Are the current processes sufficient?*

Most commenters believe Market Authorities should encourage and facilitate quick, efficient and flexible cooperation between regulators and market operators regardless of jurisdictional boundaries.[190] Market Authorities should enter into MOUs with regulators in different jurisdictions to establish mechanisms for rapid and efficient exchange of data.[191] Additionally,

---

186 SEC Pakistan; Central Bank of Ireland; FIX; BATS; Avenues; FSB; Crispin; Hessian, Eurex and Frankfurt Exchanges; ICI; NASDAQ; FINRA.

187 Hessian, Eurex and Frankfurt Exchanges.

188 ICI.

189 London Stock Exchange Group.

190 NASDAQ; FIA; Hessian, Eurex and Frankfurt Exchanges.

191 FSB; SEC Pakistan; Central Bank of Ireland; BATS.

cross-border surveillance can be facilitated through harmonization of data[192] and a consistent approach to surveillance across different jurisdictions.[193]

One commenter favors the creation of a European consolidated tape to facilitate cross-border surveillance.[194]

> ***Question 17:*** *What regulatory capabilities are, in general, needed in order for Market Authorities to survey for and detect market abuse that occurs on a cross-border basis? How can such abuse be best detected and combated?*

One commenter suggested, "there needs to be a governance structure that combines the priorities of the various national regulators and to oversee the implementation of regulations… [which] can take shape in many forms such as bilateral or multilateral agreements and memorandum of understanding. Otherwise, an overarching supervising body funded by the various jurisdictions with authority through an agreed mechanism can exercise oversight."[195]

Because of fragmentation of markets, one commenter suggested that one venue should be assigned the overall view for shares traded across multiple venues.[196] Additional capabilities include consistent software tools that are "fed" with consistent data,[197] experienced and well-trained staff[198] and mechanisms to easily share data on a cross-jurisdiction basis without authorization from government bodies.[199]

B. Feedback to comments on Recommendation 8

No commenter to the Consultation Report disagreed with this recommendation. The recommendation is therefore unchanged in the Final Report. It is worth noting that most commenters expressed the view that Market Authorities should encourage and facilitate quick, efficient and flexible cooperation between regulators and market operators regardless of jurisdictional boundaries, and that they should enter into MOUs with regulators in different jurisdictions to establish mechanisms for rapid and efficient exchange of data. This is largely consistent with current practices.

---

192 NASDAQ.

193 ICI.

194 BATS.

195 Crispin; Central Bank of Ireland (supports the use of MOU relating to identification of market authorities responsible for individual stock).

196 NASDAQ.

197 FIA.

198 FIA.

199 SEC Pakistan.