FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

FINAL NOTICE

To: **Citigroup Global Markets Limited**

FRN: 124384

Address: Citigroup Centre
25 Canada Square
London
E14 5LB
UNITED KINGDOM

Date: 19 August 2022

1. ACTION

1.1. For the reasons given in this Final Notice, the Authority hereby imposes on Citigroup Global Markets Limited (**CGML**) a financial penalty of £12,553,800 pursuant to section 206 of the Act for breaches of Principle 2 of the Authority's Principles for Businesses (**Principle 2**) and Article 16(2) of the Market Abuse Regulation, Regulation (EU) No. 596/2014 (**MAR**).

1.2. CGML agreed to resolve this matter and qualified for a 30% (stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £17,934,030 on CGML.

2. SUMMARY OF REASONS

2.1. The Authority has the operational objective of protecting and enhancing the integrity of the UK financial system. Market abuse, such as insider dealing and market manipulation, undermines the integrity of the UK financial system.

2.2. MAR was published in June 2014 and took effect on 3 July 2016 (**MAR Effective Date**). MAR is a significant piece of legislation that covers the offences of insider

dealing, unlawful disclosure of inside information, and market manipulation. Firms that arrange or execute transactions in financial instruments are required by Article 16(2) of MAR (**Article 16(2)**) to establish and maintain effective arrangements, systems, and procedures to detect and report potential market abuse.

2.3. CGML is headquartered in London and is a wholly-owned indirect subsidiary of Citigroup Inc. (**Citigroup**). As Citigroup's international broker-dealer, CGML professionally arranges and executes transactions and is therefore subject to the requirements of Article 16(2).

2.4. The Compliance function within the EMEA region that serves CGML was responsible for implementing the requirements of MAR, including those of Article 16(2), on behalf of CGML. EMEA Compliance was overseen by a senior leadership team (**EMEA Compliance SLT**), the membership of which has changed since the Relevant Period.

CGML breached Principle 2

2.5. During the period between 2 November 2015 and 18 January 2018 (**Relevant Period**), CGML breached Principle 2 by failing to conduct its business with due skill, care, and diligence in relation to its implementation of the requirements of Article 16(2).

2.6. CGML's breach of Principle 2 comprises the following failures:

a) CGML's implementation of the requirements of Article 16(2) was flawed.

   i. CGML proceeded to implement Article 16(2) without initially considering the secondary legislation that supplemented MAR.

   ii. CGML's initial MAR gap analysis, which was not completed until October 2017, did not provide CGML with the means to prioritise the most serious market abuse risks affecting its business.

   iii. CGML did not begin preparing an Article 16(2) risk assessment until December 2017.

b) The failure to accurately track the implementation of the requirements of Article 16(2).

   i. The MAR Working Group, which was one of the forums involved in the implementation of the requirements of Article 16(2), failed to provide

sufficient oversight of the implementation of the requirements of Article 16(2).

ii. CGML failed to define the scope of the MAR implementation objective in its 2016 EMEA Compliance Plan. As a result compliance with Article 16(2) was not agreed as a prerequisite for the completion of the objective.

iii. CGML's UK Business Risk, Compliance, and Controls committee and the CGML Board were both wrongly informed in late 2016 that MAR implementation was complete.

iv. EMEA Compliance failed to properly evaluate and monitor work relating to Article 16(2) implementation that was conducted as part of a global markets remediation programme undertaken by Citigroup.

CGML breached Article 16(2) of MAR

2.7. Until January 2018, CGML failed to identify significant gaps in its arrangements, systems, and procedures for trade surveillance for the purposes of compliance with Article 16(2).

2.8. CGML notified the Authority in late November 2017 that it had not completed its analysis of the gaps it needed to address to comply with Article 16(2) and that its implementation of the requirements of Article 16(2) was incomplete. At that time, EMEA Compliance had completed a gap analysis that required further work, including the addition of a risk assessment.

2.9. CGML subsequently conducted a *de novo* risk assessment in December 2017 and January 2018, which identified significant gaps in CGML's trade surveillance coverage.

2.10. The identification of the significant gaps in January 2018 marks the end of the Relevant Period (which for the purpose of the Article 16(2) breach commenced on 3 July 2016) in the Authority's investigation. CGML commenced a remediation programme in January 2018, and the most significant gaps were all remediated by the end of that year.

Penalty

2.11. Tackling market abuse is a high priority for the Authority and it views CGML's failings as serious. Furthermore, during the Relevant Period, the Authority

reminded CGML that it was a key market participant and therefore it was particularly important that CGML effectively implemented regulations, like MAR, to ensure market integrity.

2.12. The Authority hereby imposes on CGML a financial penalty in the amount of £12,553,800, pursuant to section 206 of the Act, for breaches of Principle 2 and Article 16(2). This action supports the Authority's statutory objective of protecting and enhancing the integrity of the UK financial system.

3. DEFINITIONS

3.1. The definitions below are used in this Notice:

"the Act" means the Financial Services and Markets Act 2000;

"Article 16(2)" means Article 16(2) of MAR;

"the Authority" means the body corporate previously known as the Financial Services Authority and renamed on 1 April 2013 as the Financial Conduct Authority;

"BRCC" means CGML's UK Business Risk, Compliance, and Control committee;

"BRD" means Business Requirements Document;

"CAP" means Corrective Action Plan;

"CARA" means Citigroup's Compliance Annual Risk Assessment;

"CGML" means Citigroup Global Markets Limited (FRN: 124384);

"Citigroup" means Citigroup Inc. the parent company of CGML;

"DEPP" means the Authority's Decision Procedure and Penalties Manual;

"DR 2016/522" means Commission Delegated Regulation (EU) 2016/522 of 17 December 2015, supplementing MAR, published in the Official Journal of the European Union on 5 April 2016;

"DR 2016/957" means Commission Delegated Regulation (EU) 2016/957 of 9 March 2016, supplementing MAR, published in the Official Journal of the European Union on 17 June 2016;

"EMEA" means the Europe, Middle East, and Africa region;

"EMEA Compliance" means the compliance function within the EMEA region that serves CGML;

"EMEA Compliance SLT" means CGML's EMEA Compliance Senior Leadership Team, the membership of which has changed since the Relevant Period;

"ESMA" means European Securities and Markets Authority;

"ESMA Final Report" means the European Securities and Markets Authority's Final Report, Draft technical standards on Market Abuse Regulation, 28 September 2015, ESMA/2015/1455;

"FX" means Foreign Exchange;

"GSM" means Global Securitised Markets;

"Independent Review" means the report of an independent third-party engaged by Citigroup to review certain business controls within Citigroup;

"MAD" means Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse), published in the Official Journal of the European Union on 12 April 2003;

"MAR" means Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April 2014 on Market Abuse, published in the Official Journal of the European Union on 12 June 2014;

"MAR Effective Date" means 3 July 2016;

"MAR Objective" means the objective relating to MAR in CGML's 2016 EMEA Compliance Plan;

"MAR Observation" means an observation in the Independent Review regarding CGML's compliance with Article 16(2) of MAR;

"MAR Tracker" means the project planner and tracker used by CGML's MAR Working Group;

"MCI" means Citigroup's Markets Conduct Initiative;

"MCRT" means Citigroup's Market Conduct Risk Taxonomy;

"MiFID II" means Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments, published in the Official Journal of the European Union on 12 June 2014;

"PMO" means Citigroup's Project Management Office;

"Principle 2" means Principle 2 of the Authority's Principles for Businesses;

"RAG" means Red, Amber, Green;

"Relevant Period" means the period from 2 November 2015 to 18 January 2018;

"STR" means Suspicious Transaction Report;

"STOR" means Suspicious Transaction and Order Report;

"the Tribunal" means the Upper Tribunal (Tax and Chancery Chamber).

4. FACTS AND MATTERS

Citigroup Global Markets Limited

4.1. Citigroup Global Markets Limited (**CGML**) is a wholly-owned indirect subsidiary of Citigroup Inc. (**Citigroup**). CGML is Citigroup's international broker-dealer and has a major presence in equity, fixed income, and commodity markets. It also provides advisory services to a wide range of corporate, institutional, and government clients.

4.2. CGML is headquartered in London and operates globally, generating the majority of its business from the Europe, Middle East, and Africa region (**EMEA**). During the Relevant Period, CGML earned revenue of approximately £2.6 billion from arranging or executing transactions in the financial instruments that are referred to in Articles 2(1) and 2(2) of MAR.

EMEA Compliance

4.3. EMEA Compliance had a broad remit during the Relevant Period, which included: (i) providing advice and support to the front office; (ii) developing and maintaining policies and procedures; (iii) participating in and managing regulatory change; (iv) conducting trade and communications surveillance; (v) testing & monitoring compliance; (vi) providing training & education; and (vii) contributing to risk management.

4.4. During the Relevant Period, EMEA Compliance had a senior leadership team (**EMEA Compliance SLT**) that oversaw approximately 750 employees in more than 50 countries. The EMEA Compliance SLT consisted of managing directors who were drawn from the following groups: (i) Programme Heads (e.g., Anti-Money Laundering); (ii) Cluster Heads, representing specific countries or regions; and (iii) Product Heads (e.g., Product Compliance, Surveillance, etc.).

4.5. In July 2016, various responsibilities and tasks were formally delegated to members of EMEA Compliance. One of those tasks was the oversight and implementation of systems and controls in respect of market abuse, which was delegated to individuals in Surveillance, Product Compliance, and the Control Room.

Detection and prevention of market abuse

4.6. CGML operates a three lines of defence control framework. The first and second lines of defence have distinct and complementary responsibilities for addressing market conduct risks. The responsibilities for transaction monitoring and surveillance are primarily conducted by the front office (first line) and Compliance (second line), respectively.

Transaction monitoring

4.7. During the Relevant Period, CGML's front office had a transaction monitoring system for the detection of suspicious conduct, including potential market abuse. Transaction monitoring alerts were generated by queries over product and business-specific trade capture systems and then routed to the supervisor of the trader that generated the alert for review and disposition.

EMEA Surveillance

4.8. EMEA Surveillance, which was part of EMEA Compliance, was responsible for trade surveillance (including order surveillance) as well as electronic and voice communications surveillance.

4.9. The EMEA Surveillance team was primarily based in Belfast. During the Relevant Period it consisted of analysts who reviewed alerts generated by CGML's automated trade surveillance system, which had been developed by CGML, with support from a vendor, to create a tailored product that had a suite of tools for each type of financial instrument.

EMEA Product Compliance

4.10. The primary role of EMEA Product Compliance was to provide advice, guidance, and training to sales and trading staff, principally in London. EMEA Product Compliance was also involved in reviewing surveillance alerts that had been escalated by the EMEA Surveillance team.

4.11. EMEA Surveillance relied on EMEA Product Compliance for subject matter expertise regarding products, markets, and their associated risks for the purpose of developing surveillance controls.

Trade Surveillance programme

4.12. During the Relevant Period, CGML had a well-defined process for developing and implementing enhancements for its automated trade surveillance system. CGML used a software development process that had a lead time of approximately 12 months and involved collaboration and coordination between EMEA Surveillance, EMEA Product Compliance, and CGML's Technology team. The process typically involved the following steps:

i. EMEA Surveillance would engage with EMEA Product Compliance to identify new requirements or market abuse scenarios;
ii. Once the new requirements or scenarios were identified, EMEA Surveillance would prepare a Business Requirements Document (**BRD**), which would be approved by EMEA Product Compliance and sent to Technology;
iii. Technology would interpret the BRD and prepare a Functional Requirements Document (**FRD**);
iv. After approval of the FRD, the surveillance enhancement would be developed by Technology;
v. User acceptance testing would take place; and
vi. Following successful user acceptance testing, the surveillance enhancement(s) would be implemented.

Market Abuse Regulation

4.13. The Market Abuse Regulation (**MAR**) was published in June 2014 and took effect on 3 July 2016 (**MAR Effective Date**). MAR is a significant piece of legislation that repealed the Market Abuse Directive (**MAD**), which came into effect on 12 April 2003 and established a European Union-wide regime for tackling insider dealing and market manipulation. MAD required firms to monitor for potential market

abuse and to notify the Authority of suspicious trading by submitting Suspicious Transaction Reports (**STRs**).

4.14. MAR covers the offences of insider dealing, unlawful disclosure of inside information, and market manipulation. Two of the key changes introduced by MAR were: (i) the requirement to monitor for, identify, and report instances of attempted market abuse; and (ii) the requirement to monitor orders for the purpose of identifying potential market abuse. As a result, under MAR, STRs were replaced by Suspicious Transaction and Order Reports (**STORs**).

4.15. The scope of MAR is broader than MAD. MAD applied only to instruments traded on regulated markets, whereas MAR also applies to instruments traded on other types of venues and over-the-counter trading. By replacing MAD, the goal of MAR was to ensure market integrity and investor protection, most notably by addressing gaps in the regulation of new markets, platforms, and over-the-counter trading in financial instruments as well as in the regulation of commodities and commodity derivatives.

4.16. Article 16(2) of MAR (**Article 16(2)**) sets out the requirements for the detection and reporting of potential market abuse and requires, amongst other things, that:

> *Any person professionally arranging or executing transactions shall establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders and transactions.*

4.17. As Citigroup's international broker-dealer, CGML professionally arranges and executes transactions and is therefore subject to the requirements of Article 16(2).

Delegated Regulations

4.18. MAR was well-publicised and supplemented by delegated regulations prior to the MAR Effective Date.

4.19. On 17 December 2015, the European Commission supplemented MAR with Commission Delegated Regulation 2016/522 (**DR 2016/522**), which sets out a non-exhaustive list of specific indicators of market manipulation. DR 2016/522 was published on 5 April 2016 and is based on technical advice published by the European Securities and Markets Authority (**ESMA**) in February 2015.

4.20. On 9 March 2016, the European Commission supplemented MAR with Delegated Regulation 2016/957 (**DR 2016/957**), which specifies the level of automation that firms should have in place to comply with Article 16(2). DR 2016/957 requires firms to establish and maintain arrangements, systems, and procedures that ensure effective and ongoing monitoring of all orders received and transmitted and all transactions executed. This obligation applies to a firm's full range of trading activities (as defined in Articles 2(1) and 2(2) of MAR).

4.21. DR 2016/957 also requires firms to ensure that their arrangements, systems, and procedures for detecting and reporting potential market abuse are appropriate and proportionate in relation to the scale, size, and nature of their business activity.

4.22. DR 2016/957 was published on 17 June 2016 and is based on draft regulatory technical standards that were published by ESMA and submitted as part of a report to the European Commission in September 2015 (**ESMA Final Report**). With respect to appropriateness and proportionality, the ESMA Final Report noted that, for the "*large majority*" of firms, effective surveillance would require an automated system.

4.23. With respect to the cost of complying with Article 16(2), the ESMA Final Report recognised that "[s]*mall and large investment firms may face significantly different costs with respect to detection. Since larger firms will typically engage in transactions of greater complexity and because interaction between front office and middle/back office staff may be more limited it is likely that these firms will be required to implement automatic monitoring systems in order to comply with the technical standards.*"

4.24. With respect to the range of behaviours that need to be subject to surveillance, DR 2016/957 specifies that a firm's arrangements, systems, and procedures for reporting market abuse must take due account of the elements of insider dealing and market manipulation under Articles 8 and 12 of MAR and of the specific indicators of market manipulation referred to in DR 2016/522.

Advice from the Authority

2014 STR supervisory visit

4.25. In November 2014, the Authority conducted a supervisory visit at CGML's offices to evaluate CGML's approach to surveillance and to the STR regime that existed at that time.

4.26. Following the visit, the Authority sent CGML a letter in January 2015 which noted, amongst other things, that whilst there were "*many aspects of your STR surveillance work that are positive*", CGML's plan for the expansion of its automated surveillance in nonequity markets appeared to be "*unsystematic in terms of the prioritisation of market abuse risk*" and that, in the Authority's experience, "*a strong market abuse risk assessment/gap analysis often lays the foundations for designing and implementing effective surveillance. We believe undertaking such an analysis and using the results to drive the surveillance roadmap would be beneficial.*"

4.27. The Authority's letter asked CGML to either undertake a market abuse risk assessment or, if available, to review an existing assessment, and to incorporate it into CGML's future surveillance development plan. The Authority asked for this action to be taken to provide comfort that CGML was prioritising the areas where it was exposed to the highest market abuse risks.

4.28. In August 2015, CGML provided the Authority with the requested gap analysis. It later advised the Authority that its risk-based methodology was based on risk ratings provided by EMEA Product Compliance and that those risk ratings would be incorporated into CGML's surveillance development plan. CGML, however, did not begin preparing an Article 16(2) risk assessment until December 2017.

"Market Watch" newsletters

4.29. The Authority's *Market Watch* newsletter provides advice on market conduct issues such as market abuse risks and suspicious transaction and order reporting.

4.30. The *Market Watch 48* newsletter, which was published in June 2015, included observations from STR supervisory visits. The newsletter advised firms to consider undertaking a detailed market abuse risk assessment before designing a surveillance programme because, for a number of firms, such an assessment had enabled the design of proportionate and appropriate surveillance.

4.31. The *Market Watch 50* newsletter, which was published on 1 April 2016, noted that it was "*the responsibility of firms to ensure that they understand the new requirements* [of MAR] *and are fully compliant by 3 July 2016.*" Market Watch 50 specifically referred to Article 16 and confirmed that the Authority intended "*to supervise the STOR regime in much the same that* [it] *currently supervise*[s] *the STR regime*".

4.32. The *Market Watch 58* newsletter, which was published after the Relevant Period in December 2018, described the Authority's industry-wide review of MAR

implementation. The Authority's review identified that the most effective compliance was achieved where firms could demonstrate that their risk assessments were calibrated to the markets and asset classes they operate in. The review also identified that there were some areas where firms were encountering difficulties in compliance, including in relation to surveillance. The newsletter also referred to the Authority's flexible approach to supervision in relation to quote surveillance, which was a recognition of the significant technological changes that were required by Article 16(2).

The Authority's supervisory approach

4.33. Prior to the MAR Effective Date, the Authority published an article on its website regarding its supervisory priorities for the new STOR regime. The article stated that the Authority would "*continue to take a risk-based approach, taking into account the position of particular market participants and the markets in which they operate.*" The article also noted that MAR includes a list of indicators of market manipulation that firms "*must be mindful of in ensuring their systems and procedures are effective.*"

4.34. With respect to the challenges in implementing the requirements of Article 16(2), the article acknowledged that MAR "*may require a number of significant technology changes…particularly in relation to surveillance of quotes.*", and, in relation to MAR implementation, "*some notifiers may not be in a position to deploy fully effective surveillance across all types of quotes as required by MAR by 3 July 2016.*" Despite these challenges, the article stated that "[a] *level of surveillance on quotes, which may include manual elements to the process, is expected from* [the MAR Effective Date]." The Authority also emphasised that it expected firms to have in place "*detailed and realistic plans*".

4.35. In July 2017, a year after the MAR Effective Date, the Authority expected firms to be compliant with the requirements of Article 16(2), including the surveillance of quotes. As a result, it updated the article on its website by deleting the section that referred to technological challenges and the Authority's flexible supervisory approach with respect to the surveillance of quotes.

<u>CGML and the requirements of Article 16(2) of MAR</u>

4.36. EMEA Surveillance, in conjunction with EMEA Product Compliance, took steps to address the specific requirements of Article 16(2). Those efforts, which are described in the following sections of this Notice, did not initially consider the

specific indicators of market manipulation in DR 2016/522. In addition, CGML did not begin preparing an Article 16(2) risk assessment until December 2017.

4.37. Consequently, CGML was unable to fully implement effective arrangements, systems, and procedures for detecting and reporting potential market abuse that were appropriate and proportionate in relation to the scale, size, and nature of its business activity during the Relevant Period.

4.38. Furthermore, while CGML's front office did identify and categorise wholesale conduct risks, CGML did not seek to adapt its front office monitoring systems to the specific requirements of Article 16(2).

CGML's approach to implementing MAR prior to the MAR Effective Date

Initial gap analysis

4.39. By September 2014, EMEA Compliance had taken responsibility for implementing the requirements of MAR.

4.40. In early 2015, EMEA Surveillance, which was part of EMEA Compliance, conducted an analysis to identify the differences between MAR and MAD. At the time, EMEA Surveillance intended to use its analysis to identify potential gaps in CGML's surveillance systems and to consult with EMEA Product Compliance to confirm which gaps should be prioritised.

4.41. Almost a year later, in February 2016, EMEA Surveillance informed EMEA Product Compliance that a gap analysis was being prepared and that it would be contacting relevant Product Compliance personnel to collate information regarding CGML's various order management systems.

4.42. EMEA Surveillance subsequently completed an order flow gap analysis, which was an evaluation of the products for which CGML was capable of providing surveillance of orders.

4.43. As noted above, in paragraph 4.12, the first step in developing trade surveillance enhancements at CGML was to identify new surveillance requirements. After completing the order flow gap analysis, EMEA Surveillance began to prepare a further gap analysis to identify the surveillance enhancements that were required by Article 16(2). In March 2016, EMEA Surveillance started that process by requesting assistance from EMEA Product Compliance in developing a MAR gap analysis.

4.44. EMEA Surveillance asked EMEA Product Compliance for information regarding: (i) the individual products that were in scope; (ii) the identity of high-risk products; and (iii) the scenarios where potential market abuse might occur. In its request, EMEA Surveillance emphasised that MAR would come into effect on 3 July 2016 and that it needed to prepare a BRD which, as noted above in paragraph 4.12, was a prerequisite to developing and implementing automated trade surveillance enhancements.

4.45. EMEA Surveillance understood that EMEA Product Compliance would need to approve the MAR gap analysis before a BRD could be prepared. During the Authority's investigation, however, EMEA Product Compliance maintained that its approval was not required and that it had assumed that surveillance enhancements would be developed once gaps were identified even if the MAR gap analysis was not complete. EMEA Product Compliance did acknowledge, however, that it would have been notified if a new technology solution, or an amendment to an existing one, was released to address a surveillance scenario.

4.46. At the end of June 2016, EMEA Surveillance had prepared a MAR gap analysis, with input from EMEA Product Compliance. The gap analysis was a spreadsheet in which each row corresponded to a type of market abuse and each column corresponded to a different product traded by CGML. Each cell therefore represented a specific type of market abuse in relation to a specific product. To identify potential gaps in CGML's surveillance coverage, the MAR gap analysis assigned a colour to each cell using a red/amber/green (**RAG**) system.

4.47. EMEA Surveillance met with EMEA Product Compliance on 29 June 2016 to request approval of the MAR gap analysis.

4.48. The June 2016 MAR gap analysis did not take into account many of the manipulative practices set out in DR 2016/522. The delegated regulations had not yet been considered by EMEA Surveillance, which meant that the gap analysis was created by referring only to the primary legislation that had been published in June 2014. In addition, despite requesting information from EMEA Product Compliance about high-risk products, the gap analysis did not include any assessment of risk.

4.49. EMEA Product Compliance did not approve the MAR gap analysis. Despite being involved in the preparation of the gap analysis, EMEA Product Compliance criticised the accuracy of the RAG status that had been assigned to many of the different market abuse scenarios, particularly in relation to non-equity products.

4.50. At the time of the MAR Effective Date, EMEA Surveillance's consideration of the requirements of Article 16(2) had not taken into account the delegated regulations, the MAR gap analysis was incomplete, and EMEA Product Compliance had not yet attempted to identify the market abuse risks that were most relevant to CGML's business.

4.51. As described in the later sections of this Notice, EMEA Surveillance continued to develop the MAR gap analysis during 2016 and early 2017 with input from EMEA Product Compliance.

MAR Working Group

4.52. In November 2015, EMEA Compliance created a MAR Working Group to coordinate various MAR implementation projects. Each of the implementation projects was assigned an owner who was responsible for its completion. A Project Planner and Tracker (**MAR Tracker**) was used to record the progress of the different tasks that comprised each of the implementation projects. Although the MAR Tracker was made available to members of the EMEA Compliance SLT, there was a lack of clarity regarding who, if anyone, had oversight of the MAR Working Group.

4.53. One of the projects listed in the MAR Tracker was designated "*STORs/Surveillance*", which was owned by EMEA Surveillance. The STORs/Surveillance project was divided into several implementation tasks that each had a line item in the MAR Tracker with a target date, a RAG status, and a place to record status updates.

4.54. Although the MAR Tracker had a line item for the order flow gap analysis, it did not have a line item for the MAR gap analysis that would identify the market abuse risks that CGML needed to address to comply with Article 16(2).

4.55. Consequently, the MAR Tracker did not provide an accurate account of the work that was needed to achieve compliance with Article 16(2). By 5 May 2016, the MAR Tracker showed that the order flow gap analysis was complete and that delivery planning and the BRD for the STORs/Surveillance project were in progress, which was incorrect because the MAR gap analysis was not complete and therefore work had not yet begun on the BRD.

4.56. Shortly after the MAR Effective Date, the MAR Working Group's coordinator, who maintained the MAR Tracker, asked EMEA Surveillance for an update on the status of the user acceptance testing and production tasks for the STORs/Surveillance project. The MAR Tracker showed that these tasks had not been started and were labelled red. EMEA Surveillance responded ambiguously, stating that: "*the* [user

acceptance testing] *and Production are amber in the sense that the analysis is under way, and it will be the results of this that will design the requirements for delivery into packages of* [user acceptance testing] *and Production*".

4.57. The MAR Working Group's coordinator requested further updates in December 2016 and January 2017, but no further information was provided by EMEA Surveillance except to say that the "*MAR analysis*" was still being discussed with EMEA Product Compliance. The coordinator told the Authority that they did not know who else to contact regarding the STORs/Surveillance project. They did not request an update from EMEA Product Compliance because they understood that EMEA Surveillance, as the owner of the project, was responsible for its completion.

EMEA Compliance MAR Objective

4.58. In addition to the MAR Working Group, CGML's implementation of MAR was tracked by the EMEA Compliance SLT through monthly reports that were used to monitor the work being done in relation to CGML's annual Compliance objectives.

4.59. EMEA Compliance Objectives were principally used by the EMEA Compliance SLT as a way to track regional workstreams that were often derived from Citigroup's Compliance Annual Risk Assessment (**CARA**), which was a global process that identified the areas of highest risk across the business.

4.60. The final version of CGML's 2016 EMEA Compliance Plan, which was the output from the CARA process, was approved on 12 April 2016. The plan included a number of EMEA Compliance Objectives, including one for MAR (**MAR Objective**). The description of the MAR Objective stated that it was to "[d]*evelop and implement training, policies and procedures to give effect to new MAR across EMEA Region.*" The MAR Objective had a target date of June 2016.

4.61. The MAR Objective was owned by EMEA Product Compliance. During the Authority's investigation, EMEA Product Compliance claimed that responsibility for the MAR Objective was shared with other areas of EMEA Compliance. However, CGML confirmed that EMEA Product Compliance was solely responsible for the completion of the MAR Objective.

4.62. The MAR Objective did not have milestones. According to CGML, milestone dates were considered unnecessary because of the short time period between the creation of the objective and the target date.

4.63. There is conflicting evidence regarding the scope of the MAR Objective. For example, one of the individual owners of the MAR Objective told the Authority that the objective related to "*MAR in all the components*", which included surveillance. In contrast, one of the other individual owners of the MAR Objective stated that it pertained only to those areas for which EMEA Product Compliance would ordinarily be responsible, which did not include surveillance.

4.64. EMEA Surveillance considered that EMEA Product Compliance was responsible for achieving compliance with Article 16(2) partly because EMEA Product Compliance owned the MAR Objective.

4.65. On 6 July 2016, only a week after refusing to approve the MAR gap analysis, EMEA Product Compliance approved the closure of the MAR Objective as complete. As a result, the subsequent monthly reports prepared for the EMEA Compliance SLT noted that the MAR Objective was complete.

Communication with the Authority

4.66. Around the time of the MAR Effective Date, CGML requested a call with the Authority to discuss the firm's approach to the investment recommendations requirements in MAR. The call took place on 6 July 2016 and EMEA Product Compliance was one of the participants.

4.67. During the call, CGML informed the Authority that, broadly speaking, it considered that it was in compliance with MAR.

4.68. With respect to surveillance, CGML advised the Authority that it continued to face challenges with order surveillance because of the increased volume of data handling and the different ways in which orders were received, which according to CGML was more challenging for certain products.

CGML's approach to addressing Article 16(2) after the MAR Effective Date

Continued development of the MAR gap analysis

4.69. After the MAR Effective Date, EMEA Surveillance continued to develop the MAR gap analysis with input from EMEA Product Compliance.

4.70. Despite the continuing work on the MAR gap analysis, the CGML Board was informed on 26 October 2016 that MAR implementation was complete. Also, on 23 November 2016, The UK Business Risk, Compliance, and Control (**BRCC**)

committee, which was the management committee that oversaw operational risk, was informed that MAR implementation was complete.

4.71. As with other firms, CGML faced technological challenges with respect to the requirements of Article 16(2) and consequently EMEA Product Compliance was unconcerned that work on the MAR gap analysis was continuing after the MAR Effective Date. In addition, EMEA Product Compliance considered the development of the gap analysis to be an iterative process between Surveillance and Product Compliance that was not expected to have a definitive end date. EMEA Product Compliance also considered that there was already good surveillance coverage of Equities.

4.72. On 2 February 2017, the CGML Board considered the Authority's annual evaluation of the firm, which had been summarised in a letter that the Authority had sent to CGML on 12 January 2017. The Authority's letter identified certain key risks and issues, including regulatory change implementation. The letter noted that CGML did not have a "*seamless implementation*" of an earlier piece of legislation and that:

> "*There are a number of incoming EU regulations, such as Market Abuse Regulation (MAR) and MiFID II, that firms are required to implement and comply with, notwithstanding the UK's withdrawal from the EU. Given the breadth and volume of* [CGML's] *business in EMEA, the implementation of MAR has generated practical and technological challenges for the firm.…As a key market participant, it is particularly important that* [CGML] *is effectively implementing regulations that impact the functionality of the markets in which it operates, in order maintain* [sic] *the integrity of the market.*"

4.73. CGML regarded the Authority's letter to be forward-looking and therefore inapplicable to regulations like MAR that were already in effect. Also, at an institutional level, CGML understood that any changes required by MAR had already been implemented prior to January 2017.

4.74. CGML's understanding was reflected in the 2017 EMEA Compliance Plan, which took MAR into account only in relation to training and investment recommendations monitoring, even though the plan specifically referred to the Authority's January 2017 letter and noted that CGML would continue to focus on managing and improving its regulatory change implementation.

4.75. In late March 2017, EMEA Surveillance planned to have the MAR gap analysis completed and signed off by EMEA Product Compliance by the end of April 2017. In late April 2017, however, the MAR gap analysis was not yet complete. EMEA Surveillance rescheduled the sign-off meeting with EMEA Product Compliance to take place in June 2017.

MAR/MiFID II gap analysis

4.76. On 9 May 2017, although work on the MAR gap analysis was still ongoing, the EMEA Compliance SLT agreed to incorporate the requirements of MiFID II into the gap analysis. As a result, EMEA Surveillance began to work with EMEA Product Compliance to identify any additional surveillance requirements that would be introduced by MiFID II, which was due to come into effect in January 2018. Consequently, the MAR gap analysis became the MAR/MiFID II gap analysis.

4.77. MiFID II incorporates the requirements of MAR, which means that compliance with MiFID II, in relation to certain types of trading, requires compliance with MAR.

Further input from EMEA Product Compliance

4.78. In June 2017, EMEA Product Compliance participated in a meeting attended by the Authority and members of an industry group representing participants in Europe's wholesale financial markets. The purpose of the meeting was to discuss the implementation of MAR, including STORs, surveillance, and investment recommendations. EMEA Product Compliance provided an update from the meeting to Citigroup's Global Equities Governance and Controls forum in July 2017, which noted that there were "[n]*o issues or comments indicating a need to modify Citi procedures*".

4.79. On 8 August 2017, EMEA Surveillance and Product Compliance met for an hour to discuss various surveillance matters, including the MAR/MiFID II gap analysis. The gap analysis was, by that time, a substantial multi-tab spreadsheet that indicated the presence of several hundred surveillance gaps. The gap analysis took into account the manipulative practices set out in DR 2016/522, but did not include any assessment of risk, which meant that the most serious risks had not been identified and could not be prioritised.

4.80. EMEA Product Compliance did not provide sign-off for the MAR/MiFID II gap analysis. During the Authority's investigation, none of the meeting attendees could recall why the gap analysis had not been approved. Following the meeting, EMEA

Surveillance again requested input from EMEA Product Compliance to further develop the MAR/MiFID II gap analysis.

Markets Conduct Initiative

4.81. Whilst EMEA Surveillance and EMEA Product Compliance continued to develop the MAR gap analysis in late 2016 and early 2017, Citigroup was taking steps at a global level to design and implement trade surveillance enhancements as part of a remediation programme known as the Markets Conduct Initiative (**MCI**).

4.82. The MCI was a business-owned global remediation programme that Citigroup initiated in response to foreign regulators' findings in relation to Citigroup's FX business.

4.83. The goal of the MCI was to address identified risks through globally consistent standards and to create baseline surveillance standards across all markets and products, including those in EMEA.

2016 Independent Review

4.84. In 2016, Citigroup engaged an independent third-party to review Citigroup's internal controls (**Independent Review**). The Independent Review set out numerous observations regarding Citigroup's internal controls, including CGML's EMEA surveillance processes and procedures for communications, trade, and personal account trading.

4.85. The Independent Review included an observation (**MAR Observation**) that "*EMEA trade surveillance scenarios currently do not cover all FCA specified risks or upcoming Market Abuse Regulation requirements across all asset classes*". The Independent Review recommended that, to "*make further enhancements, the global Compliance Surveillance team should perform a gap analysis against upcoming regulations and other risks to mitigate these as required.*"

4.86. On 22 August 2016, Citigroup's Project Management Office (**PMO**), which was responsible for running large projects, like the MCI, informed EMEA Surveillance that Trade Surveillance would be added to the scope of the MCI as part of a pre-existing Corrective Action Plan.

Corrective Action Plans

4.87. Corrective Action Plans (**CAPs**) were used by CGML to log issues that required remediation and to track the progress of remediation work against specific

deadlines. The use of a CAP usually resulted in additional oversight and monitoring of an affected issue.

4.88. Following an assessment of the Independent Review, CGML decided that the MAR Observation was one that required a new CAP. Ownership of the MAR Observation was assigned to the Global Surveillance team in New York.

4.89. In September 2016, EMEA Surveillance considered that a trade surveillance CAP should be opened that was specific to Article 16(2). By that time, Surveillance had begun to transition from a regional management structure to a global structure. As a result, EMEA Surveillance needed approval from Global Surveillance before it could open a MAR-specific trade surveillance CAP.

4.90. Global Surveillance decided that a MAR-specific CAP was not needed and that the MAR Observation should initially be addressed via a pre-existing CAP known as CAP 36B.

CAP 36B

4.91. CAP 36B was an MCI CAP that was intended to define the controls that were needed to mitigate key market conduct risks in every country in which each of Citigroup's eight Markets Sales and Trading businesses had a physical presence, which included the UK. In the event that deficiencies were identified, the purpose of CAP 36B was to develop a risk-based plan to provide effective controls.

4.92. CAP 36B resulted in the establishment of a target state framework known as the Markets Conduct Control Framework, which consisted of:

i. a catalogue of conduct risks, known as the Market Conduct Risk Taxonomy (**MCRT**), which was used to assess CGML's Markets Sales and Trading businesses;

ii. a Risk Appetite Statement that explained the risk tolerance levels for each conduct risk in the MCRT, which was used to determine whether a conduct risk had been sufficiently mitigated; and

iii. the necessary internal controls to mitigate the different market conduct risks.

Application to Article 16(2)

4.93. Because CAP 36B was only intended to identify market conduct risks and controls, CGML recognised that the MAR Observation would ultimately be addressed by successor CAPs.

4.94. On 15 October 2016, a member of the Global Surveillance team, which was responsible for the MAR Observation, contacted EMEA Surveillance to ask what behaviours constitute "*upcoming Market Abuse Regulation requirements across all asset classes*". In response, EMEA Surveillance provided a list of behaviours that corresponded to Articles 8 and 12 of MAR as well as the specific indicators of market manipulation referred to in DR 2016/522.

4.95. On 16 October 2016, Global Surveillance provided the PMO with the proposed language for the CAP that would address the MAR Observation. The proposed language simply stated that: "*Successor CAP for existing MCI CAP 36B will address observation*". At that time, Global Surveillance did not believe that the MCI would effectively address the requirements of Article 16(2). A member of the Global Surveillance team advised the PMO that they could "*almost guarantee that our work on the MCRT to fill the Hub and Large gaps coupled with our QA review of transaction monitoring alerts is not going to be extensive enough to cover this gap.*"

4.96. Work relating to CAP 36B was completed on 15 December 2016 and 47 successor CAPs were created to address, on a global scale, the key market conduct risks that had been identified via CAP 36B. Of the 47 successor CAPs, 30 related to trade surveillance and were owned by Global Surveillance.

<u>CAP 36B successor CAPs</u>

4.97. The MAR Observation was mapped to several of the CAP 36B successor CAPs that were owned by Global Surveillance. In early 2017, Global Surveillance asked EMEA Surveillance to confirm whether the MCI would be sufficient to address some or most of the requirements of Article 16(2). EMEA Compliance understood that Global Surveillance had decided that compliance with Article 16(2) would be achieved as part of the MCI and, in particular, CAP 36B and its successor CAPs. However, it was never intended that CAP 36B and its successor CAPs would fully address the Article 16(2) requirements. There was also no formal decision to incorporate all MAR requirements into the MCI trade surveillance programme, or to expressly track work relating to Article 16(2) in the context of the MCI..

4.98. Ultimately, the CAP 36B successor CAPs were not specifically designed to address the requirements of Article 16(2) because they were not linked to any specific regulatory requirements. Instead, the MCI used a holistic approach to create baseline global surveillance standards across all markets and asset classes and, as a consequence, it addressed only some of the requirements in Article 16(2).

Meetings with the Authority

4.99. On 26 April 2017, a meeting took place between the Authority and CGML regarding CGML's implementation of MAR. The Authority had requested the meeting to discuss CGML's experience of implementing the requirements of MAR. Surveillance was one of four key topics the Authority wanted to discuss. The Authority had asked to "*meet with the individuals responsible for implementing MAR…which may include project managers, accountable directors or members of the compliance department.*"

4.100. During the meeting, CGML informed the Authority that prior to MAR implementation it had conducted an assessment of conduct risks in relation to the MCI. CGML considered that those risk assessments covered MAR and therefore CGML did not complete an additional risk assessment as part of its MAR implementation. In addition, CGML informed the Authority that it had sought to implement MAR in combination with other projects, such as the MCI.

4.101. At that time, however, CGML had not completed its MAR gap analysis to identify how the requirements of Article 16(2) applied to CGML's business.

Outcome of the work relating to the MAR Observation

4.102. In late 2017, EMEA Surveillance recognised that it should have escalated its request in 2016 for a MAR-specific CAP by taking steps to overrule the decision by Global Surveillance to rely on the MCI CAPs. Similarly, CGML's Internal Audit function concluded, in 2018, that the MAR Observation should not have been mapped to CAP 36B and its successor CAPs because those CAPs were not specifically designed to address MAR. Also, during the Authority's investigation, a member of the EMEA Surveillance team noted that the overlap between the MCI and MAR was "[v]*ery insignificant*".

Escalations to EMEA and Global Compliance management

4.103. Between 9 October and 11 November 2017, at least four formal escalations were made to either EMEA or Global Compliance management regarding concerns about the delayed completion of the MAR/MiFID II gap analysis or MAR implementation in general.

4.104. The first escalation, which was made by EMEA Surveillance to Global Surveillance on 9 October 2017, highlighted concerns "*that the requirements for enhancements to the existing EMEA Trade Surveillance program in prep for MiFID 2 have not been fully identified or documented and nor had this been escalated to you by the EMEA team.*"

4.105. After raising its concerns, a member of the EMEA Surveillance team noted, in internal discussions, that the MAR gap analysis had not yet been approved by EMEA Product Compliance and that CGML's schedule of technology releases had been fully utilised by the MCI, which meant there was no capacity for addressing MAR in 2017.

4.106. In addition, on 12 October 2017, the recipient of the 9 October escalation received an email from another member of Global Surveillance regarding items for the 2018 budget, which noted that "*MAR/MIFID is a regulatory requirement and I am not comfortable living with that risk until 2019…*".

4.107. Further escalations took place in early November 2017. However, despite raising concerns about MAR, the escalations between 9 October and 11 November focused primarily on the trade surveillance requirements in MiFID II, which was due to come into effect in January 2018.

4.108. Ultimately, on 17 November 2017, EMEA Compliance management emailed Senior Global Compliance management to escalate concerns regarding MAR and MiFID II. EMEA Compliance management informed Senior Global Compliance management that "*MAR came into force on July 3, 2016 across EU member states. Initial work, including impact analysis, on both of these regulations commenced in 2016 and was not completed or actioned further given MCI program priorities. There were no and are no CAPs raised and we are just learning of these details. We are likely covering limited elements of both regulatory requirements within our existing trade surveillance program and hope to know the proportion of coverage by the end of next week. We are in a current state of non-compliance with MAR and will continue to be…well into 2018.*"

4.109. CGML subsequently notified the Authority on 23 November 2017 that its MAR gap analysis for surveillance was incomplete and that its deployment of surveillance requirements was also incomplete. The Authority asked CGML if it had an understanding of the main impacted areas. CGML advised the Authority that it was still working to complete its gap analysis and that it was difficult to provide the Authority with a definitive answer until that work was near completion.

October 2017 MAR/MiFID II gap analysis

Approval of the MAR gap analysis by EMEA Product Compliance

4.110. On 11 October 2017, shortly after the first escalation, EMEA Surveillance emailed the MAR gap analysis to EMEA Product Compliance for "*one final look*". EMEA Surveillance suggested in its email that an "*overly cautious approach*" had been taken when deciding whether a gap existed or not. EMEA Surveillance advised EMEA Product Compliance that following approval of the gap analysis the next step would be to "*undertake the massive challenge of figuring out how we cover every gap in this document*".

4.111. By 26 October 2017, EMEA Product Compliance had approved the MAR aspect of the MAR/MiFID II gap analysis. The gap analysis did not include any assessment of risk.

Review by Global Surveillance and the PMO

4.112. Global Surveillance and the PMO reviewed the MAR/MiFID II gap analysis in early November 2017. On 10 November 2017, the PMO informed EMEA Surveillance that the gap analysis required more work. In particular, the PMO noted that: "*there is no indication of the size of the 'gap' identified in this document. So, if we just count the number of reds or ambers, it is a tremendous amount that could take us years to remediate.*" The PMO also noted that Global Surveillance had "*raised several questions re: whether some of the perceived gaps are even applicable to the products...this needs to be revisited to make sure the gaps are accurate.*" Finally, the PMO indicated that it had started to consider the appropriate methodology for measuring the level of risk, which it identified as one of the key elements of the gap analysis that had to be completed before a remediation plan could be designed.

4.113. Global Surveillance subsequently met with EMEA Surveillance and EMEA Product Compliance to discuss the October 2017 gap analysis and to analyse whether the specific risks identified in the 900+ gaps originally identified genuinely applied to

the particular products. Following that meeting, the number of gaps was reduced from 900+ to approximately 220.

4.114. On 22 November 2017, the PMO requested further input from EMEA Product Compliance. The PMO advised EMEA Product Compliance that almost all of the MAR conduct risks could be addressed through the implementation of trade surveillance enhancements and that input from EMEA Product Compliance was needed to confirm that the updated gap analysis was accurate. The PMO also asked EMEA Product Compliance to help prioritise the gaps using a risk-based approach because "*we can't remediate all gaps at the same time. So we would like to agree on which ones to focus on first and which ones can be deferred to a later time*".

4.115. The MAR/MiFID II gap analysis was updated by EMEA Surveillance, EMEA Product Compliance, and Global Surveillance during the week commencing 27 November 2017. At the end of that week, on 1 December 2017, a member of the Global Surveillance team advised the other teams that although "*we still have a few open items within each product grouping we need to get started on the gap prioritization*".

4.116. EMEA Compliance prioritised the gaps by assigning them into different risk tiers based on the level of seriousness, which was calculated for each risk using the likelihood of occurrence and significance of impact.

Completion of the MAR/MiFID II gap analysis

4.117. In January 2018, CGML completed its MAR/MiFID II gap analysis. The gap analysis was conducted across 23 behaviours and 39 products, which were divided into six asset classes (Equities, FX, Futures & Options, Rates, Credit/GSM, and Commodities). The gap analysis assessed: (i) the applicability of each behaviour to each product; (ii) CGML's current surveillance coverage of the applicable behaviours; and (iii) the risk ratings for each applicable scenario. After January 2018, CGML continued to update the MAR/MiFID II gap analysis, which resulted in the identification of additional market abuse risks and surveillance gaps.

Surveillance coverage

4.118. The completed MAR/MiFID II gap analysis assessed CGML's existing level of surveillance coverage based only on the surveillance controls CGML had in place at the time. Supplemental controls such as policies and training were also in place at this time but were not considered for the purpose of determining the level of surveillance coverage. During the Authority's investigation, EMEA Surveillance

acknowledged that manual surveillance would not be suitable for a firm the size and complexity of CGML because MAR requires monitoring of all orders received and transmitted and all transactions executed.

4.119. If the coverage sufficiently addressed an applicable behaviour, that behaviour was deemed to have full surveillance coverage. If the surveillance coverage partially addressed the behaviour, or covered a subset of the trading activity for that product, there was deemed to be partial coverage. The remaining applicable behaviours were deemed to be gaps.

4.120. CGML had the following surveillance coverage of its trade and communication surveillance risks across the different risk tiers:

Tier	Risks	Full coverage	Partial coverage	Gaps	% coverage (full or partial)
1	20	20	0	0	100%
2	74	28	11	35	52.7%
3	148	49	12	87	41.2%
4	298	38	17	243	18.5%
Tail	77	32	15	30	61%

Distribution of trade surveillance gaps

4.121. The 35 Tier 2 gaps and 87 Tier 3 gaps were distributed across the different asset classes in the following way:

Asset class	Daily vol.	% vol.	Tier 2 risks	Tier 2 gaps	% Tier 2 coverage (full or partial)	Tier 3 risks	Tier 3 gaps	% Tier 3 coverage (full or partial)
Equities	651,842	72.9	1	1	0%	33	16	51.5%
FX (excl. Spot FX)	107,575	12	2	0	100%	0	0	N/A
Futures & Options	97,324	10.8	38	16	57.9%	52	19	63.5%
Rates	22,475	2.5	5	5	0%	30	22	26.7%
Credit/GSM	8,962	1	18	8	55.6%	13	10	23.1%
Commodities	6,033	0.7	10	5	50%	20	20	0%

4.122. The 30 Tail Risk gaps were distributed across the different asset classes in the following way:

Asset class	Daily vol.	% vol.	Tail Risks	Tail Risk gaps	% Tail Risk coverage (full or partial)
Equities	651,842	72.9	0	0	N/A
FX (excl. Spot FX)	107,575	12	16	4	75%
Futures & Options	97,324	10.8	26	2	92.3%
Rates	22,475	2.5	21	13	38.1%
Credit/GSM	8,962	1	2	0	100%
Commodities	6,033	0.7	12	11	8.3%

Remediation programme

4.123. CGML considered the January 2018 gap analysis to be confirmation of its non-compliance with Article 16(2). On 7 February 2018, EMEA Compliance provided the CGML Board with an update on MAR. The update noted that CGML was "*not in compliance with the EU Market Abuse Regulation (MAR) surveillance requirements*". The update referred to the behaviours in the January 2018 gap analysis and stated that EMEA Compliance had "*failed to implement the required MAR surveillance routines….*" The update also acknowledged that "[i]*t does not appear that there was appropriate governance, regulatory change management oversight, or appropriate escalation to management about this issue within* [CGML]."

4.124. CGML used the January 2018 gap analysis as the basis for a remediation programme. On 3 August 2018, CGML advised the Authority that it expected to "*achieve effective MAR risk mitigation by the end of June 30, 2019.*"

4.125. CGML also informed the Authority in August 2018 that it had carried out an exercise whereby it mapped its existing control framework to its Tier 4 gaps and that the existing controls provided sufficient mitigation of these lower risk Tier 4 surveillance gaps. The Tier 4 risks were mitigated by CGML's policies, training, communications surveillance, supervisory framework, algorithmic trading controls framework, and benchmark controls framework.

4.126. On 24 October 2018, the CGML Board was provided with a further update on MAR. The update again noted that CGML was not in compliance with the MAR surveillance requirements. EMEA Compliance confirmed that it had prepared an accelerated remediation plan and that "[t]*he implementation of the surveillance program will be appropriate and proportionate to the Firm's trading activity in order to effectively*

mitigate the MAR related risks through the use of 'effective arrangements, systems and procedures to detect and report suspicious orders and transactions (MAR Art 16 (2))'."

4.127. During 2018, CGML successfully remediated all Tier 2 trade surveillance gaps and more than half of its Tier 3 trade surveillance gaps. The remediation programme continued until the end of June 2019.

4.128. In 2016, CGML allocated a budget of approximately $230,000 for the identification and implementation of trade surveillance enhancements to comply with Article 16(2). Because the gap analysis was not completed in 2016, that budget was never utilised. For 2017, $600,000 was allocated to MAR in the trade surveillance budget. Again, that money was not needed because the gap analysis was not completed until January 2018. In late 2017, when the 2018 trade surveillance budget was being prepared, $1 million was allocated to MAR. Ultimately, in 2018, CGML spent approximately $14.5 million and 181,914 staff-hours implementing the requirements of Article 16(2).

5. FAILINGS

5.1. The statutory and regulatory provisions relevant to this Notice are referred to in Annex A.

CGML breached Principle 2

5.2. CGML breached Principle 2 by failing to conduct its business with due skill, care, and diligence during the Relevant Period. The failures comprising CGML's breach of Principle 2 are described below.

<u>CGML's implementation of the requirements of Article 16(2) was flawed</u>

5.3. CGML's approach to assessing the requirements of Article 16(2) during the Relevant Period did not enable it to implement effective arrangements, systems, and procedures for detecting and reporting potential market abuse.

5.4. CGML did not properly take into account the delegated regulations as part of its implementation of Article 16(2) until after the MAR Effective Date. Consequently, when EMEA Surveillance presented the MAR gap analysis to EMEA Product Compliance in late June 2016, the gap analysis did not include many of the manipulative practices set out in DR 2016/522.

5.5. The MAR gap analysis that was ultimately approved by EMEA Product Compliance in October 2017 did not include a risk assessment of the more than 900 identified surveillance gaps. As a result, it did not provide CGML with the means to prioritise the most serious market abuse risks affecting its business.

5.6. By November 2017 the PMO and Global Trade Surveillance had reconsidered the number of gaps and following this the number of gaps was reduced to 220.

5.7. CGML began preparing an Article 16(2) risk assessment in December 2017. With the completion of the MAR/MiFID II gap analysis on 19 January 2018, the risk assessment was substantially complete. The preparation of the January 2018 gap analysis marks the end of the Relevant Period.

CGML failed to accurately track its implementation of Article 16(2)

MAR Working Group

5.8. The purpose of the MAR Working Group was to coordinate CGML's various MAR implementation projects. However, the group did not have a designated owner who was responsible for overseeing and confirming the completion of all the projects.

5.9. Also, the MAR Tracker that was used by the MAR Working Group did not provide the means to monitor the development of the MAR gap analysis because it did not contain a line item for that task.

5.10. Consequently, when the coordinator for the MAR Working Group had concerns about the STORs/Surveillance project, they did not have the necessary information to properly scrutinise the updates that were provided by EMEA Surveillance. Also, because EMEA Surveillance owned the STORs/Surveillance project, the coordinator did not know who else to contact regarding the project.

5.11. The creation of the MAR Working Group in November 2015 marks the start of the Relevant Period.

MAR Objective

5.12. EMEA Compliance did not take steps to clearly define the scope of the MAR Objective. As a result, the EMEA Compliance SLT did not have an agreed understanding of what the MAR Objective required. One of the owners of the MAR Objective informed the Authority that it related to MAR in its entirety. Another owner, however, believed that the MAR Objective related only to work that would

ordinarily be carried out by EMEA Product Compliance, which did not include surveillance.

5.13. When the MAR Objective was closed in July 2016, EMEA Product Compliance did not consider compliance with Article 16(2) to be a prerequisite for the completion of the MAR Objective.

5.14. After the MAR Objective was recorded as complete in July 2016, the monthly reports produced for the EMEA Compliance SLT indicated that MAR implementation was complete, which implied that the requirements of Article 16(2) had been implemented.

CGML Board and UK BRCC

5.15. The CGML Board and the UK BRCC were wrongly advised in late 2016 that MAR implementation was complete.

CGML failed to properly evaluate and monitor the work relating to Article 16(2) implementation that was conducted as part of the MCI

5.16. EMEA Compliance understood that compliance with Article 16(2) would be achieved as part of the MCI. That understanding was incorrect and lacked a reasonable basis because such a determination could not be made without first determining how the requirements of Article 16(2) applied to CGML's business.

5.17. CGML's Internal Audit function concluded, in 2018, that the MAR Observation should not have been mapped to CAP 36B and its successor CAPs because those CAPs were not designed to address Article 16(2).

5.18. The MCI was based on the MCRT, which was not specific to any particular regulation. Therefore, even though the MCI used a risk-based approach, it did not include steps to ensure that CGML's arrangements, systems, and procedures took due account of the elements of insider dealing and market manipulation in Articles 8 and 12 of MAR and the specific indicators of market manipulation referred to in DR 2016/522.

5.19. Global Surveillance declined the request from EMEA Surveillance for a CAP that was specific to Article 16(2) and EMEA Surveillance did not escalate its request or attempt to overrule that decision.

5.20. Ultimately, there was an insignificant degree of overlap between the MCI and Article 16(2).

Consequences of failing to accurately track the implementation of Article 16(2)

5.21. Although CGML's senior management took steps to oversee the implementation of MAR, the EMEA Compliance SLT members who were responsible for ensuring that CGML implemented the requirements of Article 16(2) did not properly communicate with each other or their colleagues regarding the status of CGML's compliance with Article 16(2) during the Relevant Period.

5.22. When the CGML Board reviewed the Authority's firm evaluation letter in early 2017, it did not give sufficient weight to the Authority's guidance regarding MAR implementation because it considered the Authority's guidance to be inapplicable to MAR, which was already in effect, and because it believed that MAR implementation was complete.

5.23. CGML's 2017 EMEA Compliance Plan included MAR training and investment recommendations monitoring, but it did not include any arrangements for MAR implementation, even though the plan referred to the Authority's concerns about CGML's ability to implement new regulatory requirements.

5.24. When the Authority met with CGML in April 2017, CGML incorrectly advised the Authority that the MCI risk assessment covered MAR and therefore CGML had not completed an additional risk assessment as part of its MAR implementation. CGML also informed the Authority that it had sought to implement MAR in combination with other projects, such as the MCI. CGML failed to mention, however, that the MCI did not expressly track work done pursuant to Article 16(2).

CGML breached Article 16(2) of MAR

5.25. CGML failed to comply with Article 16(2) during the period between the MAR Effective Date and the end of the Relevant Period.

<u>CGML did not properly consider how Article 16(2) applied to its business during the Relevant Period</u>

5.26. Article 16(2) required CGML to establish and maintain effective arrangements, systems, and procedures to detect and report potential market abuse. DR 2016/957 required CGML to ensure that those controls were capable of monitoring all orders received and transmitted and all transactions executed across CGML's full range of trading activities (as defined in Articles 2(1) and 2(2) of MAR).

5.27. In terms of the behaviours that CGML needed to detect and report, DR 2016/957 specifies that a firm's arrangements, systems, and procedures for reporting market abuse must take due account of the elements of insider dealing and market manipulation in Articles 8 and 12 of MAR and the specific indicators of market manipulation referred to in DR 2016/522.

5.28. When MAR came into effect, EMEA Surveillance had not properly considered the delegated regulations insofar as they related to Article 16(2), which meant that it had not considered how the delegated regulations affected the applicability of Article 16(2) to CGML's business.

5.29. With respect to the required level of automation, DR 2016/957 required CGML to ensure that its arrangements, systems, and procedures for detecting and reporting potential market abuse were appropriate and proportionate in relation to the scale, size, and nature of its business activity. The Authority acknowledges that there were difficulties in implementing quote surveillance before July 2017 due to a lack of technological solutions before that time, but notes that firms were still expected to have a level of surveillance on quotes from the MAR Effective Date, that could include manual elements, and to have in place detailed and realistic plans.

5.30. As noted in paragraph 4.12, the first step in CGML's process for developing and implementing automated surveillance enhancements was the identification of new requirements. CGML initiated this first step prior to the MAR Effective Date, but it was not completed until it prepared the January 2018 gap analysis.

5.31. CGML also identified additional market abuse risks and surveillance gaps in July 2018.

5.32. CGML notified the Authority in November 2017 that it had not completed an Article 16(2) risk assessment, the MAR gap analysis that had been signed-off the previous month was unsuitable for implementing the requirements of Article 16(2) because it did not provide the means for implementing effective arrangements, systems, and procedures that were appropriate and proportionate in relation to the scale, size, and nature of CGML's business activity.

CGML failed to implement effective arrangements, systems, and procedures that were appropriate and proportionate for the scale, size, and nature of its business activity

Surveillance gaps

5.33. The completed gap analysis still identified many significant trade surveillance gaps. CGML had only 52.7% coverage (either full or partial surveillance) of its 74 Tier 2 trade and communication surveillance risks. Furthermore, only 37.8% of CGML's Tier 2 risks were subject to full surveillance coverage.

5.34. CGML had only 41.2% coverage (either full or partial surveillance) of its 148 Tier 3 risks. Furthermore, only 33.1% of CGML's Tier 3 risks were subject to full surveillance coverage.

5.35. CGML had only 61% coverage (either full or partial surveillance) of its 77 Tail Risks. Furthermore, only 41.6% of CGML's Tail Risks were subject to full surveillance coverage. The Tail Risks were those risks with a low likelihood of occurrence and a "significant" significance of impact.

Asset class coverage

5.36. Equities and Rates each had 0% surveillance coverage of Tier 2 risks, of which there were 6 in total. Commodities had only 50% coverage (either full or partial surveillance) of its 10 Tier 2 risks and Futures and Options had 57.9% coverage (either full or partial surveillance), but with the greatest number of Tier 2 gaps (16 out of 38 risks). Credit/GSM had 55.6% coverage (full surveillance) of its 18 Tier 2 risks.

5.37. Commodities had 0% surveillance coverage of Tier 3 risks, of which there were 20 in total. There was 23.1% and 26.7% full surveillance coverage of the Tier 3 risks in Credit/GSM and Rates, respectively, of which there were 43 risks in total. Equities had 51.5% coverage (full surveillance) of its 33 Tier 3 risks. Futures and Options had 63.5% coverage (either full or partial surveillance) of its 52 Tier 3 risks.

5.38. Finally, with respect to Tail Risks, Commodities had coverage of only 1 of its 12 risks (8.3%, full coverage). Rates had 38.1% coverage (full surveillance) of its 13 risks. FX (excluding Spot FX) had 75% coverage (full or partial surveillance) of its 16 risks and Futures and Options had 92.3% coverage (full or partial surveillance)

of its 24 risks. There was 100% full surveillance coverage of the 2 Tail Risks in Credit/GSM.

Low-volume asset classes

5.39. Article 16(2) applies to the full range of CGML's trading activities (as defined in Articles 2(1) and 2(2) of MAR). Therefore, although Equities accounted for 72.9% of CGML's average daily trading volume during the Relevant Period, and Rates, Credit/GSM, and Commodities collectively accounted for less than 5%, the Authority considers the surveillance gaps associated with CGML's low-volume asset classes to be significant, particularly because of the scale, size, and complexity of CGML's business, which meant that even a small proportion of CGML's business could represent a significant volume.

5.40. As noted in the Authority's January 2017 firm evaluation letter, CGML is a key market participant. Therefore, it is particularly important that CGML effectively implements regulatory requirements that impact the functionality of the markets in which it operates, to ensure the integrity of those markets. Also, even its lowest volume asset class (Commodities) had an average daily trading volume in excess of 6,000 trades.

5.41. The ESMA Final Report noted that, in replacing MAD, the goal of MAR was to ensure market integrity and investor protection, most notably by addressing gaps in the regulation of new markets, platforms, and over-the-counter trading in financial instruments as well as in the regulation of commodities and commodity derivatives.

5.42. With respect to CGML's low-volume asset classes, the Authority notified CGML in January 2015 of the concerns it had regarding CGML's plan for the expansion of its automated surveillance in non-equity markets. The Authority described the plan as "*unsystematic in terms of the prioritisation of market abuse risk*" and advised CGML of the benefits of a robust market abuse risk assessment/gap analysis that could lay the foundation for designing and implementing effective surveillance. However, CGML's Article 16(2) risk assessment was not substantially complete until January 2018, more than 18 months after the MAR Effective Date.

5.43. During the Relevant Period, CGML recognised the importance of effective surveillance of non-equity products. EMEA Product Compliance was split into two main areas: (i) Equities and (ii) Fixed Income, Commodities, and Currencies. EMEA Product Compliance did not approve the MAR gap analysis until October 2017 partly

because it was not satisfied that the gap analysis accurately addressed CGML's non-equities market conduct risks.

Remediation programme

5.44. CGML's remediation programme demonstrated that, assisted by the availability of post-MiFID II order data, effective arrangements, systems, and procedures for detecting potential market abuse could be implemented in approximately 12-18 months. Using the January 2018 gap analysis as the basis for its programme, CGML successfully remediated all of its Tier 2 trade surveillance gaps and more than half of its Tier 3 trade surveillance gaps by the end of 2018. The remediation programme then continued for a further 6 months.

5.45. The ESMA Final Report, which was published in September 2015, had advised firms that the primary cost of complying with Article 16(2) would likely be the detection of potential market abuse and that the cost would be partly dependent on the size of the firm.

5.46. Given the complexity of CGML's business, and the long lead time for the development of trade surveillance enhancements, CGML should have identified the applicable risks and required enhancements at an earlier stage to ensure that it could achieve compliance with Article 16(2) in a timely manner.

5.47. Pursuant to section 206 of the Act, the Authority may therefore impose on CGML a penalty of such amount as it considers appropriate.

6. SANCTION

6.1. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

6.2. The total financial penalty which the Authority hereby imposes on CGML is £12,553,800. In summary, this penalty is calculated as follows.

Step 1: Disgorgement

6.3. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breaches where it is practicable to quantify this.

6.4. The Authority has not identified any financial benefit that CGML derived directly from its breaches.

6.5. The Step 1 figure is therefore £0.

Step 2: Seriousness of the breaches

6.6. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breaches. The Authority considers that revenue is an appropriate indicator of the harm or potential harm that CGML's breaches may cause. The Authority has therefore determined a Step 2 figure based on a percentage of CGML's "relevant revenue".

6.7. CGML's relevant revenue has been calculated using the revenue derived by CGML from the arrangement or execution of transactions in the financial instruments that fall within the scope of MAR. The Authority considers that CGML's relevant revenue should be indicative of the risk that market abuse could occur undetected because of a lack of effective arrangements, systems, and procedures for the detection of potential market abuse.

6.8. The Authority has measured the risk created by the absence of effective controls by calculating a residual risk multiplier. Residual risk is the risk that remains after controls have been taken into account. In this case, residual risk is the risk that certain types of market abuse could not be detected and reported by CGML because of a lack of effective arrangements, systems, and procedures.

6.9. CGML's relevant revenue has been calculated by applying the residual risk multiplier to the total revenue that CGML generated during the Relevant Period from the arrangement or execution of transactions in the financial instruments that fall within the scope of MAR (£2,575,148,623).

6.10. The Authority therefore considers CGML's relevant revenue to be £986,632,387.

6.11. In deciding on the percentage of the relevant revenue that forms the basis of the Step 2 figure, the Authority considers the seriousness of the breaches and chooses a percentage between 0% and 20%. This range is divided into five fixed levels that represent, on a sliding scale, the seriousness of the breaches; the more serious the breaches, the higher the level. For penalties imposed on firms there are the following five levels:

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

6.12. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breaches, and whether they were committed deliberately or recklessly. DEPP 6.5A.2G(11) lists factors likely to be considered 'level 4 or 5 factors'. The Authority considers that none of those factors are relevant.

6.13. DEPP 6.5A.2G(12) lists factors likely to be considered 'level 1, 2 or 3 factors'. Of these, the Authority considers the following factors to be relevant:

a) Little, or no, profits were made or losses avoided as a result of the breaches, either directly or indirectly.

6.14. The Authority also considers that the following factors are relevant:

a) MAR is a significant and well-publicised piece of legislation for which the Authority issued clear advice, particularly in relation to Article 16. (DEPP 6.5A.2G(7)(a)).

b) The breach of Article 16(2) had an adverse effect on markets that was serious because CGML is a globally significant broker-dealer and failed to have effective arrangements, systems and procedures to detect and report potential market abuse for an extended period of time. (DEPP 6.5A.2G(6)(f)).

6.15. Taking all of these factors into account, the Authority considers the seriousness of the breaches to be level 3 and so the Step 2 figure is 10% of £986,632,387.

6.16. The Step 2 figure is therefore £98,663,239.

6.17. DEPP 6.5.3G(3) provides that the Authority may decrease the level of penalty arrived at after applying Step 2 of the framework if it considers that the penalty is disproportionately high for the breach concerned. The Authority considers that the level of penalty is disproportionate, taking into account the non-deliberate nature of the breaches and the lack of any financial benefit arising from them.

6.18. To achieve a penalty that (at Step 2) is proportionate to the breaches, and having taken into account previous cases, the Step 2 figure is reduced to £16,303,664.

Step 3: Mitigating and aggravating factors

6.19. Pursuant to DEPP 6.5A.4G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2 (not including any amount to be disgorged as set out in Step 1) to take into account factors that aggravate or mitigate the breaches

6.20. The Authority considers that the following factor aggravates the breaches:

a) The Authority informed CGML in 2015 that it had concerns about the unsystematic approach to the prioritisation of risk in the firm's expansion of its automated surveillance in nonequity markets. To address those concerns, the Authority advised CGML to incorporate a risk assessment into its future surveillance development plan. Ultimately, however, CGML did not begin preparing an Article 16(2) risk assessment until December 2017.

6.21. The Authority considers that there are no factors that mitigate the breaches.

6.22. Having taken into account the aggravating factors, the Authority considers that the Step 2 figure should be increased by 10%.

6.23. The Step 3 figure is therefore £17,934,030.

Step 4: Adjustment for deterrence

6.24. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm that committed the breaches, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.25. The Authority considers that the Step 3 figure of £17,934,030 represents a sufficient deterrent to CGML and others, and so has not increased the penalty at Step 4.

6.26. The Step 4 figure is therefore £17,934,030.

Step 5: Settlement discount

6.27. Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7

provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement. The settlement discount does not apply to the disgorgement of any benefit calculated at Step 1.

6.28. The Authority and CGML reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure.

6.29. The Step 5 figure is therefore £12,553,800.

Penalty

6.30. The Authority hereby imposes a total financial penalty of £12,553,800 on CGML for breaching Principle 2 and Article 16(2) during the Relevant Period.

7. PROCEDURAL MATTERS

7.1. This Notice is given to CGML under and in accordance with section 390 of the Act. The following statutory rights are important.

Decision maker

7.2. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

Manner and time for payment

7.3. The financial penalty must be paid in full by CGML to the Authority no later than 5 September 2022.

If the financial penalty is not paid

7.4. If all or any of the financial penalty is outstanding on 6 September 2022, the Authority may recover the outstanding amount as a debt owed by CGML and due to the Authority.

Publicity

7.5. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority

may not publish information if such publication would, in the opinion of the Authority, be unfair to CGML or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

7.6. The Authority intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

Authority contacts

7.7. For more information concerning this matter generally, contact Gavin Carrucan at the Authority (direct line: 020 7066 9272/ Email: gavin.carrucan@fca.org.uk).

Sadaf Hussain
Head of Department
Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A - RELEVANT STATUTORY AND REGULATORY PROVISIONS

FINANCIAL SERVICES AND MARKETS ACT 2000

1B The FCA's general duties

1. In discharging its general functions the FCA must, so far as is reasonably possible, act in a way which –

    (a) is compatible with its strategic objective, and

    (b) advances one or more of its operational objectives.

2. The FCA's strategic objective is: ensuring that the relevant markets (see section 1F) function well.

3. The FCA's operational objectives are –

    (a) […];

    (b) the integrity objective (see section 1D);

    (c) […]

1D The integrity objective

1. The integrity objective is: protecting and enhancing the integrity of the UK financial system.

2. The "integrity" of the UK financial system includes –

    (a) its soundness, stability and resilience,

    (b) its not being used for a purpose connected with financial crime,

    (c) its not being affected by contraventions by persons of Article 14 (prohibition of insider dealing and of unlawful disclosure of inside information) or Article 15 (prohibition of market manipulation) of the market abuse regulation,

    (d) the orderly operation of the financial markets, and

    (e) the transparency of the price formation process in those markets.

206 – Financial penalties

1. If the Authority considers that an authorised person has contravened a relevant requirement imposed on the person, it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate.

MARKET ABUSE REGULATION, (EU) NO. 596/2014

Article 2 Scope

1. This Regulation applies to the following:

(a) financial instruments admitted to trading on a regulated market or for which a request for admission to trading on a regulated market has been made;

(b) financial instruments traded on an MTF, admitted to trading on an MTF or for which a request for admission to trading on an MTF has been made;

(c) financial instruments traded on an OTF;

(d) financial instruments not covered by point (a), (b) or (c), the price or value of which depends on or has an effect on the price or value of a financial instrument referred to in those points, including, but not limited to, credit default swaps and contracts for difference.

This Regulation also applies to behaviour or transactions, including bids, relating to the auctioning on an auction platform authorised as a regulated market of emission allowances or other auctioned products based thereon, including when auctioned products are not financial instruments, pursuant to Regulation (EU) No 1031/2010. Without prejudice to any specific provisions referring to bids submitted in the context of an auction, any requirements and prohibitions in this Regulation referring to orders to trade shall apply to such bids.

2. Articles 12 and 15 also apply to:

(a) spot commodity contracts, which are not wholesale energy products, where the transaction, order or behaviour has or is likely or intended to have an effect on the price or value of a financial instrument referred to in paragraph 1;

(b) types of financial instruments, including derivative contracts or derivative instruments for the transfer of credit risk, where the transaction, order, bid or behaviour has or is

likely to have an effect on the price or value of a spot commodity contract where the price or value depends on the price or value of those financial instruments; and

(c) behaviour in relation to benchmarks.

3. This Regulation applies to any transaction, order or behaviour concerning any financial instrument as referred to in paragraphs 1 and 2, irrespective of whether or not such transaction, order or behaviour takes place on a trading venue.

4. The prohibitions and requirements in this Regulation shall apply to actions and omissions, in the Union and in a third country, concerning the instruments referred to in paragraphs 1 and 2.

Article 16 Prevention and detection of market abuse

1. […]

2. Any person professionally arranging or executing transactions shall establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders and transactions. Where such a person has a reasonable suspicion that an order or transaction in any financial instrument, whether placed or executed on or outside a trading venue, could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, the person shall notify the competent authority as referred to in paragraph 3 without delay.

3. Without prejudice to Article 22, persons professionally arranging or executing transactions shall be subject to the rules of notification of the Member State in which they are registered or have their head office, or, in the case of a branch, the Member State where the branch is situated. The notification shall be addressed to the competent authority of that Member State.

COMMISSION DELEGATED REGULATION (EU) 2016/522 of 17 DECEMBER 2015

[Recitals]

Whereas:

1. Regulation (EU) No 596/2014 confers on the Commission the power to adopt delegated acts in a number of closely related matters pertaining the exemption of certain third countries public bodies and central banks from the scope of application of that Regulation, the indicators of market manipulation, the thresholds for the disclosure by emission allowance market participants of inside information, the specification of the

competent authority for the notification of delays in the public disclosure of inside information, the circumstances under which trading during closed period can be permitted by the issuer and the types of notifiable managers' transactions.

[…]

5. It is essential to specify the indicators of manipulative behaviour relating to false or misleading signals and to price securing laid down in Annex I to Regulation (EU) No 596/2014, in order to clarify their elements and to take into account technical developments on financial markets. Therefore, a non-exhaustive list of such indicators including examples of practices should be provided.

6. For some practices, additional indicators should be identified as they can respectively clarify and illustrate such practices. Those indicators should neither be deemed exhaustive nor determinative and their relations to one or more examples of practices should not be deemed limitative. The examples of practices should not be considered to constitute market manipulation per se, but should be taken into account where transactions or orders to trade are examined by market participants and competent authorities.

7. A proportionate approach should be followed, taking into consideration the nature and specific characteristics of the financial instruments and markets concerned. The examples may be linked to and illustrate one or more indicators of market manipulation as provided in Annex I to Regulation (EU) No 596/2014. As a result, a specific practice may involve more than one indicator of market manipulation laid down in Annex I to Regulation (EU) No 596/2014 depending on how it is used, and there can be some overlap. Similarly, although not specifically referenced in this Regulation, certain other practices may illustrate each of the indicators set out in this Regulation. Therefore, market participants and competent authorities should take into account other unspecified circumstances that could be considered to be potential market manipulation in accordance with the definition set out in Regulation (EU) No 596/2014.

8. Certain examples of practices set out in this Regulation describe cases that are included in the notion of market manipulation or that, in some respects, refer to manipulative conduct. On the other hand, certain examples of practices may be considered legitimate if, for instance, a person who enters into transactions or issues orders to trade which may be deemed to constitute market manipulation may be able to establish that his reasons for entering into such transactions or issuing orders to trade were legitimate and in conformity with an accepted practice on the market concerned.

9. For the purposes of listing examples of practices referring to indicators of market manipulation as provided in Annex I to Regulation (EU) No 596/2014, cross-referencing in Annex II to this Regulation includes both the relevant example of practice and the additional indicator associated with that example.

10. For the purpose of indicators of manipulative behaviour set out in this Regulation, any reference to 'order to trade' encompasses all types of orders, including initial orders, modifications, updates and cancellations, irrespective of whether or not they have been executed, of the means used to access the trading venue or to carry out a transaction or to enter an order to trade and of whether or not the order has been entered into the trading venue's order-book.

[…]

31. The relevant provisions and empowerments set out in Regulation (EU) No 596/2014 only begin to apply from 3 July 2016. Therefore, it is important that the rules laid down in this Regulation also apply from the same date.

[…]

Article 1 – Subject-matter and scope

This Regulation lays down detailed rules with regard to:

[…]

2. the indicators of market manipulation laid down in Annex I to Regulation (EU) No 596/2014.

[…]

Annex II – Indicators of manipulative behaviour

[Numerous indicators of manipulative behaviour are provided in Annex II of the delegated regulation.]

COMMISSION DELEGATED REGULATION (EU) 2016/957 of 9 MARCH 2016

[Recitals]

Whereas:

1. It is necessary to specify appropriate requirements for the arrangements, procedures and systems that market operators and investment firms operating a trading venue and any person professionally arranging or executing transactions should have in place for the reporting of orders and transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation under Regulation (EU) No 596/2014. Such requirements should assist the prevention and detection of market abuse. They should also assist in ensuring that notifications submitted to competent authorities are meaningful, comprehensive and useful. In order to ensure that detection of market abuse is effective, appropriate systems should be in place to monitor orders and transactions. Such systems should provide for human analysis carried out by appropriately trained staff. The systems for monitoring market abuse should be capable of producing alerts in line with predefined parameters in order to allow for further anaysis [sic] to be conducted on potential insider dealing, market manipulation or attempted insider dealing or market manipulation. The whole process is likely to require some level of automation.

2. In order to facilitate and promote a consistent approach and practices across the Union in relation to prevention and detection of market abuse, it is appropriate to lay down detailed provisions harmonising the content of, the template for and the timing of the reporting of suspicious orders and transactions.

[…]

4. Persons that are professionally engaged in arranging or executing transactions should be able to delegate the monitoring, detection and identification of suspicious orders and transactions within a group or to delegate the data analysis and the generation of alerts, subject to appropriate conditions. Such delegation should make it possible to share resources, to centrally develop and maintain monitoring systems and to build expertise in the context of monitoring orders and transactions. Such delegationg [sic] should not prevent the competent authorities from assessing, at any time, whether the systems, arrangements and procedures of the person to whom the functions are delegated are effective to comply with the obligation to monitor and detect market abuse. The obligation to report as well as the responsibility to comply with this

Regulation and with Article 16 of Regulation (EU) No 596/2014 should remain with the delegating person.

[…]

16. In order to ensure the smooth functioning of the financial markets, it is necessary that this Regulation enters into force as a matter of urgency and that the provisions laid down in this Regulation apply from the same date as those laid down in Regulation (EU) No 596/2014,

[…]

Article 2 – General requirements

1. Persons professionally arranging or executing transactions shall establish and maintain arrangements, systems and procedures that ensure:

    (a) effective and ongoing monitoring, for the purposes of detecting and identifying orders and transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, of all orders received and transmitted and all transactions executed;

    (b) the transmission of STORs to competent authorities in accordance with the requirements set out in this Regulation and using the template set out in the Annex.

2. The obligations referred to in paragraph 1 shall apply to orders and transactions relating to any financial instrument and shall apply irrespective of:

    (a) the capacity in which the order is placed or the transaction is executed;

    (b) the types of clients concerned;

    (c) whether the orders were placed or transactions executed on or outside a trading venue.

3. Market operators and investment firms operating a trading venue shall establish and maintain arrangements, systems and procedures that ensure:

    (a) effective and ongoing monitoring, for the purposes of preventing, detecting and identifying insider dealing, market manipulation and attempted insider dealing and market manipulation, of all orders received and all transactions executed;

(b) the transmission of STORs to competent authorities in accordance with the requirements set out in this Regulation and using the template set out in the Annex.

4. The obligations referred to in paragraph 3 shall apply to orders and transactions relating to any financial instrument and shall apply irrespective of:

   (a) the capacity in which the order is placed or the transaction is executed;

   (b) the types of clients concerned.

5. Persons professionally arranging or executing transactions, market operators and investment firms operating a trading venue shall ensure that the arrangements, systems and procedures referred to in paragraphs 1 and 3:

   (a) are appropriate and proportionate in relation to the scale, size and nature of their business activity;

   (b) are regularly assessed, at least through an annually conducted audit and internal review, and updated when necessary;

   (c) are clearly documented in writing, including any changes or updates to them, for the purposes of complying with this Regulation, and that the documented information is maintained for a period of five years.

The persons referred to in the first subparagraph shall, upon request, provide the competent authority with the information referred to in point (b) and (c) of that subparagraph.

Article 3 – Prevention, monitoring and detection

1. The arrangements, systems and procedures referred to in Article 2(1) and (3) shall:

   (a) allow for the analysis, individually and comparatively, of each and every transaction executed and order placed, modified, cancelled or rejected in the systems of the trading venue and, in the case of persons professionally arranging or executing transactions, also outside a trading venue;

   (b) produce alerts indicating activities requiring further analysis for the purposes of detecting potential insider dealing or market manipulation or attempted insider dealing or market manipulation

(c) cover the full range of trading activities undertaken by the persons concerned.

2. Persons professionally executing or arranging transactions and market operators and investment firms operating trading venues shall, upon request, provide the competent authority with the information to demonstrate the appropriateness and proportionality of their systems in relation to the scale, size and nature of their business activity, including the information on the level of automation put in place in such systems.

3. Market operators and investment firms operating trading venues shall, to a degree which is appropriate and proportionate in relation to the scale, size and nature of their business activity, employ software systems and have in place procedures which assist the prevention and detection of insider dealing, market manipulation or attempted insider dealing or market manipulation.

   The systems and procedures referred to in the first subparagraph shall include software capable of deferred automated reading, replaying and analysis of order book data, and such software shall have sufficient capacity to operate in an algorithmic trading environment.

4. Persons professionally arranging or executing transactions and market operators and investment firms operating a trading venue shall put in place and maintain arrangements and procedures that ensure an appropriate level of human analysis in the monitoring, detection and identification of transactions and orders that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation.

5. Market operators and investment firms operating a trading venue shall put in place and maintain arrangements and procedures that ensure an appropriate level of human analysis also in the prevention of insider dealing, market manipulation or attempted insider dealing or market manipulation.

6. A person professionally arranging or executing transactions shall have the right, by a written agreement, to delegate to a legal person forming part of the same group the performance of the functions of monitoring, detection and identification of orders and transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation. The person delegating those functions shall remain fully responsible for discharging all of its obligations under this Regulation and Article 16 of Regulation (EU) No 596/2014 and shall ensure the arrangement is clearly

documented and the tasks and responsibilities are assigned and agreed, including the duration of the delegation.

7. A person professionally arranging or executing transactions may, by written agreement, delegate the performance of data analysis, including order and transaction data, and the generation of alerts necessary for such person to conduct monitoring, detection and identification of orders and transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation to a third party ('provider'). The person delegating those functions shall remain fully responsible for discharging all of its obligations under this Regulation and Article 16 of Regulation (EU) No 596/2014 and shall comply at all times with the following conditions:

   (a) it shall retain the expertise and resources necessary for evaluating the quality of the services provided and the organisational adequacy of the providers, for supervising the delegated services and for the management of the risks associated with the delegation of those functions on an ongoing basis;

   (b) it shall have direct access to all the relevant information regarding the data analysis and the generation of alerts.

   The written agreement shall contain the description of the rights and obligations of the person delegating the functions referred to in the first subparagraph and those of the provider. It shall also set out the grounds that allow the person delegating the functions to terminate such agreement.

8. As part of the arrangements and procedures referred to in Article 2(1) and (3), persons professionally arranging or executing transactions and market operators and investment firms operating a trading venue shall maintain for a period of five years the information documenting the analysis carried out with regard to orders and transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation which have been examined and the reasons for submitting or not submitting a STOR. That information shall be provided to the competent authority upon request.

   The persons referred to in the first subparagraph shall ensure that the arrangements and procedures referred to in Article 2(1) and (3) guarantee and maintain the confidentiality of the information referred to in the first subparagraph.

Article 5 – Reporting obligations

1. Persons professionally arranging or executing transactions and market operators and investment firms operating a trading venue shall establish and maintain effective arrangements, systems and procedures that enable them to assess, for the purpose of submitting a STOR, whether an order or transaction could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation. Those arrangements, systems and procedures shall take due account of the elements constituting the actual or attempted insider dealing or market manipulation under Articles 8 and 12 of Regulation (EU) No 596/2014 and of the non-exhaustive indicators of market manipulation referred to in Annex I to that Regulation, as further specified in the Commission Delegated Regulation (EU) 2016/522….

[…]

PRINCIPLES FOR BUSINESSES

The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority's Handbook. They derive their authority from the Authority's rule-making powers set out in the Act. The relevant Principles are as follows:

Principle 2

A firm must conduct its business with due skill, care and diligence.

DECISION PROCEDURE AND PENALTIES MANUAL ("DEPP")

Chapter 6 of DEPP, which forms part of the Authority's Handbook, sets out the Authority's statement of policy with respect to the imposition and amount of financial penalties under the Act.

DEPP 6.5A THE FIVE STEPS FOR PENALTIES IMPOSED ON FIRMS

Step 1 – disgorgement

1. The FCA will seek to deprive a firm of the financial benefit derived directly from the breach (which may include the profit made or loss avoided) where it is practicable to quantify this. The FCA will ordinarily also charge interest on the benefit.

2. Where the success of a firm's entire business model is dependent on breaching FCA rules or other requirements of the regulatory system and the breach is at the core of

the firm's regulated activities, the FCA will seek to deprive the firm of all the financial benefit derived from such activities. Where a firm agrees to carry out a redress programme to compensate those who have suffered loss as a result of the breach, or where the FCA decides to impose a redress programme, the FCA will take this into consideration. In such cases the final penalty might not include a disgorgement element, or the disgorgement element might be reduced.

Step 2 – the seriousness of the breach

1. The FCA will determine a figure that reflects the seriousness of the breach. In many cases, the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, and in such cases the FCA will determine a figure which will be based on a percentage of the firm's revenue from the relevant products or business areas. The FCA also believes that the amount of revenue generated by a firm from a particular product or business area is relevant in terms of the size of the financial penalty necessary to act as a credible deterrent. However, the FCA recognises that there may be cases where revenue is not an appropriate indicator of the harm or potential harm that a firm's breach may cause, and in those cases the FCA will use an appropriate alternative.

2. In those cases where the FCA considers that revenue is an appropriate indicator of the harm or potential harm that a firm's breach may cause, the FCA will determine a figure which will be based on a percentage of the firm's "relevant revenue". "Relevant revenue" will be the revenue derived by the firm during the period of the breach from the products or business areas to which the breach relates. Where the breach lasted less than 12 months, or was a one-off event, the relevant revenue will be that derived by the firm in the 12 months preceding the end of the breach. Where the firm was in existence for less than 12 months, its relevant revenue will be calculated on a pro rata basis to the equivalent of 12 months' relevant revenue.

3. Having determined the relevant revenue, the FCA will then decide on the percentage of that revenue which will form the basis of the penalty. In making this determination the FCA will consider the seriousness of the breach and choose a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach. The more serious the breach, the higher the level. For penalties imposed on firms there are the following five levels:

(a) level 1 - 0%;

(b) level 2 - 5%;

(c) level 3 - 10%;

(d) level 4 - 15%; and

(e) level 5 - 20%.

4. The FCA will assess the seriousness of a breach to determine which level is most appropriate to the case.

5. In deciding which level is most appropriate to a case involving a firm, the FCA will take into account various factors, which will usually fall into the following four categories:

(a) factors relating to the impact of the breach;

(b) factors relating to the nature of the breach;

(c) factors tending to show whether the breach was deliberate; and

(d) factors tending to show whether the breach was reckless.

6. Factors relating to the impact of a breach committed by a firm include:

(a) the level of benefit gained or loss avoided, or intended to be gained or avoided, by the firm from the breach, either directly or indirectly;

(b) the loss or risk of loss, as a whole, caused to consumers, investors or other market users in general;

(c) the loss or risk of loss caused to individual consumers, investors or other market users;

(d) whether the breach had an effect on particularly vulnerable people, whether intentionally or otherwise;

(e) the inconvenience or distress caused to consumers; and

(f) whether the breach had an adverse effect on markets and, if so, how serious that effect was. This may include having regard to whether the orderliness of, or confidence in, the markets in question has been damaged or put at risk.

7. Factors relating to the nature of a breach by a firm include:

(a) the nature of the rules, requirements or provisions breached;

(b) the frequency of the breach;

(c) whether the breach revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business;

(d) whether the firm's senior management were aware of the breach;

(e) the nature and extent of any financial crime facilitated, occasioned or otherwise attributable to the breach;

(f) the scope for any potential financial crime to be facilitated, occasioned or otherwise occur as a result of the breach;

(g) whether the firm failed to conduct its business with integrity;

(h) whether the firm, in committing the breach, took any steps to comply with FSA rules, and the adequacy of those steps; and

(i) in the context of contraventions of Part VI of the Act, the extent to which the behaviour which constitutes the contravention departs from current market practice.

8. Factors tending to show the breach was deliberate include:

(a) the breach was intentional, in that the firm's senior management, or a responsible individual, intended or foresaw that the likely or actual consequences of their actions or inaction would result in a breach;

(b) the firm's senior management, or a responsible individual, knew that their actions were not in accordance with the firm's internal procedures;

(c) the firm's senior management, or a responsible individual, sought to conceal their misconduct;

(d) the firm's senior management, or a responsible individual, committed the breach in such a way as to avoid or reduce the risk that the breach would be discovered;

(e) the firm's senior management, or a responsible individual, were influenced to commit the breach by the belief that it would be difficult to detect;

(f) the breach was repeated; and

(g) in the context of a contravention of any rule or requirement imposed by or under Part VI of the Act, the firm obtained reasonable professional advice before the contravention

occurred and failed to follow that advice. Obtaining professional advice does not remove a person's responsibility for compliance with applicable rules and requirements.

9. Factors tending to show the breach was reckless include:

(a) the firm's senior management, or a responsible individual, appreciated there was a risk that their actions or inaction could result in a breach and failed adequately to mitigate that risk; and

(b) the firm's senior management, or a responsible individual, were aware there was a risk that their actions or inaction could result in a breach but failed to check if they were acting in accordance with the firm's internal procedures.

10. Additional factors to which the FCA will have regard when determining the appropriate level of financial penalty to be imposed under regulation 34 of the RCB Regulations are set out in RCB 4.2.5 G.

11. In following this approach factors which are likely to be considered 'level 4 factors' or 'level 5 factors' include:

(a) the breach caused a significant loss or risk of loss to individual consumers, investors or other market users;

(b) the breach revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business;

(c) financial crime was facilitated, occasioned or otherwise attributable to the breach;

(d) the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur;

(e) the firm failed to conduct its business with integrity; and

(f) the breach was committed deliberately or recklessly.

12. Factors which are likely to be considered 'level 1 factors', 'level 2 factors' or 'level 3 factors' include:

(a) little, or no, profits were made or losses avoided as a result of the breach, either directly or indirectly;

(b) there was no or little loss or risk of loss to consumers, investors or other market users individually and in general;

(c) there was no, or limited, actual or potential effect on the orderliness of, or confidence in, markets as a result of the breach;

(d) there is no evidence that the breach indicates a widespread problem or weakness at the firm; and

(e) the breach was committed negligently or inadvertently.

13. In those cases where revenue is not an appropriate indicator of the harm or potential harm that a firm's breach may cause, the FCA will adopt a similar approach, and so will determine the appropriate Step 2 amount for a particular breach by taking into account relevant factors, including those listed above. In these cases the FCA may not use the percentage levels that are applied in those cases in which revenue is an appropriate indicator of the harm or potential harm that a firm's breach may cause.

Step 3 – mitigating and aggravating factors

1. The FCA may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach. Any such adjustments will be made by way of a percentage adjustment to the figure determined at Step 2.

2. The following list of factors may have the effect of aggravating or mitigating the breach:

(a) the conduct of the firm in bringing (or failing to bring) quickly, effectively and completely the breach to the FCA's attention (or the attention of other regulatory authorities, where relevant);

(b) the degree of cooperation the firm showed during the investigation of the breach by the FCA, or any other regulatory authority allowed to share information with the FCA;

(c) where the firm's senior management were aware of the breach or of the potential for a breach, whether they took any steps to stop the breach, and when these steps were taken;

(d) any remedial steps taken since the breach was identified, including whether these were taken on the firm's own initiative or that of the FCA or another regulatory authority; for example, identifying whether consumers or investors or other market users suffered loss and compensating them where they have; correcting any misleading statement or impression; taking disciplinary action against staff involved (if appropriate); and taking

steps to ensure that similar problems cannot arise in the future. The size and resources of the firm may be relevant to assessing the reasonableness of the steps taken;

(e) whether the firm has arranged its resources in such a way as to allow or avoid disgorgement and/or payment of a financial penalty;

(f) whether the firm had previously been told about the FCA's concerns in relation to the issue, either by means of a private warning or in supervisory correspondence;

(g) whether the firm had previously undertaken not to perform a particular act or engage in particular behaviour;

(h) whether the firm concerned has complied with any requirements or rulings of another regulatory authority relating to the breach;

(i) the previous disciplinary record and general compliance history of the firm;

(j) action taken against the firm by other domestic or international regulatory authorities that is relevant to the breach in question;

(k) whether FCA guidance or other published materials had already raised relevant concerns, and the nature and accessibility of such materials; and

(l) whether the FCA publicly called for an improvement in standards in relation to the behaviour constituting the breach or similar behaviour before or during the occurrence of the breach.

Step 4 – adjustment for deterrence

1. If the FCA considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches then the FCA may increase the penalty. Circumstances where the FCA may do this include:

(a) where the FCA considers the absolute value of the penalty too small in relation to the breach to meet its objective of credible deterrence;

(b) where previous FCA action in respect of similar breaches has failed to improve industry standards. This may include similar breaches relating to different products (for example, action for mis-selling or claims handling failures in respect of 'x' product may be relevant to a case for mis-selling or claims handling failures in respect of 'y' product);

(c) where the FCA considers it is likely that similar breaches will be committed by the firm or by other firms in the future in the absence of such an increase to the penalty; and

(d) where the FCA considers that the likelihood of the detection of such a breach is low.

Step 5 – settlement discount

The FCA and the firm on whom a penalty is to be imposed may seek to agree the amount of any financial penalty and other terms. In recognition of the benefits of such agreements, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the FCA and the firm concerned reached an agreement. The settlement discount does not apply to the disgorgement of any benefit calculated at Step 1.