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

31 May 2022

Dear CEO,

This is the first FCA portfolio letter to entities providing the data reporting services of approved reporting mechanisms ("**ARMs**") and approved publication arrangements ("**APAs**"). We refer to these entities, collectively, as Data Reporting Services Providers ("DRSPs"[1]).

DRSPs play a key role in market transparency and integrity: ARMs provide the service of reporting details of transactions to the FCA on behalf of investment firms. APAs provide the service of publishing post-trade transparency reports on behalf of investment firms. These services enhance transparency and effective supervision of financial markets, enabling both the FCA and investors to receive accurate and comprehensive trading data.

We supervise DRSPs according to the regulatory framework set out in:

- The Data Reporting Services Regulations 2017/699 (the "**DRS Regulations 2017"**);
- UK MiFIR;
- UK MiFID Org Regulation (Commission Delegated Regulation 2017/565);
- UK MiFIR Delegated Regulation (Commission Delegated Regulation 2017/567);
- Chapter 9 of the Market Conduct sourcebook (MAR 9); and
- Various onshored technical standards.

In this letter, we refer to these collectively as the "**DRSP Regulatory Framework**".

We divide the firms we supervise into portfolios, each made up of firms with similar business models[2]. We analyse each portfolio to identify potential risks of harm and agree a strategy to address them.

This letter outlines our view of the key risks of harm in the DRSP portfolio and communicates what we expect DRSPs to do to minimise potential risks to consumers and market integrity from failures to meet regulatory requirements. We also set out key elements of what we will

[1] There are 3 types of data reporting services: ARMs, APAs and Consolidated tape providers (CTPs). CTPs provide the service of collecting post-trade transparency reports of specific financial instruments from Regulated Markets, Multilateral Trading Facilities, Organised Trading Facilities and APAs. The CTP then consolidates these reports into a continuous electronic live data stream providing price and volume information per financial instrument. As of the publication date of this letter, there is currently no UK CTP.

[2] Your firm has either been authorised or verified to provide a data reporting service and has been allocated to the 'data reporting services providers' portfolio. If your firm has permissions to perform other regulated activities, it may also be allocated to another primary portfolio.

be doing to supervise DRSPs in the portfolio. We expect you to take the necessary action to ensure that these risks are appropriately mitigated.

It is important that you understand our approach to supervising your firm's DRSP operations, your responsibility to act to manage key risks in accordance with the requirements of the DRSP Regulatory Framework, and that you can demonstrate this to us. First and foremost, we expect you to adopt an open and cooperative relationship with us.

You should consider and discuss these key risks of harm with your Board and DRSP management body and agree what further action you should take to ensure that your firm meets the DRSP Regulatory Framework. In our future supervisory engagement with you, you can expect us to ask you about the actions you, your Board and DRSP management body have taken in response to this letter to ensure that consumers and markets are adequately protected.

Our supervisory approach

You should be able to demonstrate to us how you comply with the requirements in the DRSP Regulatory Framework. Where you undertake such regulated activity, we expect you to have adequate policies and arrangements in place to disseminate efficiently and consistently the post-trade information required to be published under Articles 20 and 21 of UK MiFIR and the transaction report information required under Article 26 of UK MiFIR. We expect DRSPs to have systems and facilities that are appropriate and robust enough to ensure continuity and regularity in the performance of the DRSP services provided.

In line with the FCA's Approach to Supervision, we take a holistic approach to supervising this portfolio. Therefore, if your firm or the group to which your firm belongs also undertakes unregulated activities, we may assess these unregulated activities as part of our supervision of the regulated activities. We will supervise DRSPs using a range of information sources and supervisory tools. Where appropriate, we will enforce in line with the FCA's Approach to Enforcement, with real and meaningful consequences for firms who do not follow the rules.

Our view of the key risks of harm in your sector:

As detailed below, we have identified the following key potential risks of harm in the portfolio:

- The market is concentrated among a small number of DRSPs; this could limit clients' opportunity to switch provider and may lead to lower incentives to provide high quality services.

- DRSPs may have inadequate systems and controls to identify incomplete and potentially erroneous trade or transaction reporting data which undermines their core function of promoting market transparency and integrity.

- Insufficient operational resilience may lead to disruption for market participants, consumers and regulators, or the loss, compromise, or lack of availability of data.

These key potential risks of harm are outlined in further detail in 'Our supervisory priorities' (see below). We have also observed 'Other risks impacting the portfolio' (see below). We expect you to take appropriate action to address all the risks outlined in this letter.

Our supervisory priorities

You should consider the potential risks outlined above and further below with regards to your business, how you monitor these risks and whether you have appropriate strategies in place to address them.

Concentration risk and quality of service

Our view of the risks

The market is concentrated among a small number of DRSPs. We have observed that DRSPs often look to offer 'one-stop-shop' services, providing data reporting services alongside a range of regulated and unregulated regulatory reporting services within the entity or group. This may increase concentration in the market and limit client incentives to switch provider in search of the best value for money or quality of service. Associated costs, such as onboarding fees and technical system testing requirements might also discourage clients from switching providers.

The concentration within the DRSP market is not necessarily an issue in itself - provided DRSPs are providing a high-quality service to their clients. However, concentration within the market could potentially lead to issues with DRSPs being insufficiently incentivised to provide high quality service to their clients. We also note the link between concentration risks and operational resilience (see below).

What we expect from you

We expect you to review the services you provide to clients to ensure they are of a high quality, to enable your clients to meet their regulatory reporting obligations. We also expect you to review your fees to ensure that clients are getting good value for money, in line with our expectations that firms should compete for customers on the basis of service, quality, price and innovation, as set out in our 3-year strategy.

What we will do

We will review the services you provide to assess whether there are issues due to the concentrated DRSP market. We will look to use a variety of information sources to input into our work, which may include information requests to you and your clients to understand price-cost margins, complaints, customer support arrangements, the on and off-boarding processes and related costs and client views on the quality of service provided by DRSPs. Depending on the outcome of the review, we will look to you to address any issues. We will employ supervisory, policy and enforcement tools, as appropriate.

Data quality - systems and controls

Our view of the risks

DRSPs must have arrangements in place to manage incomplete or potentially erroneous information. ARMs should have "appropriate arrangements to identify transaction reports that are incomplete or contain obvious errors caused by clients", as well as "errors or omissions caused by the ARM itself." [3] APAs must set up and maintain "appropriate arrangements to

[3] Article 11 (*Management of incomplete or potentially erroneous information by ARMs*) of the retained EU law version of Commission Delegated Regulation (EU) 2017/571 ("**MiFID RTS 13**")

identify on receipt trade reports that are incomplete or contain information that is likely to be erroneous."[4] We expect such arrangements to be robust and effective to enable prompt identification and remediation of any issues.

We have observed that DRSPs have varying levels of systems and controls in place to identify incomplete or potentially erroneous information in trade and transaction reports. This could undermine the function of DRSPs in promoting market transparency and market integrity, for example, by compromising their ability to send accurate transaction reports to us, to enable identification and investigation of potential market abuse.

What we expect from you

The submission of complete and accurate transaction and/or publication of trade report data by the reporting deadline is a key function of a DRSP. Reviewing your data quality systems and controls and addressing any weaknesses should be a priority. We expect you to monitor that the information you have published or submitted to us is complete and accurate and in accordance with the applicable reporting deadline. As required under Articles 10 and 11 of MiFID RTS 13, you should ensure that you have appropriate systems and controls to manage incomplete or potentially erroneous information caused either by your clients or the DRSP itself. This should include, for example, reconciliations between data your clients submit to you and data you publish or submit to us, as applicable. The frequency and extent of such reconciliations should be proportionate to the volume of data the DRSP processes.

What we will do

We will use a range of information sources and supervisory tools to assess the effectiveness of the systems and controls you have in place to identify incomplete or potentially erroneous data.

Operational resilience

Our view of the risks

Operational resilience is key for all firms in this portfolio. Failure to provide complete, accurate and timely information could result in inaccurate and potentially misleading information being published to the market or provided to regulators, undermining market transparency and integrity. Given the dependence on technology, market disruption may occur if a DRSP's IT systems or critical functions are not sufficiently robust to ensure continuity and regularity in the provision of the data reporting service. We also note that risks associated with a lack of operational resilience may be heightened by concentration in the DRSP market, as observed above.

The delivery of a data reporting service depends on adequate systems and controls and effective oversight of outsourced or insourced critical functions. We have observed that many DRSPs significantly rely on insourcing to affiliated group entities and/or outsourcing to third party providers.

We have observed a reliance on the use of data vendors for reference data to enrich or validate trade and transaction reports. We have also observed that failure to monitor the data

[4] Article 10 (*Management of incomplete or potentially erroneous information by APAs and CTPs*) of the retained EU law version of Commission Delegated Regulation (EU) 2017/571

a data vendor provides has, in some cases, caused the publication and submission of incomplete or erroneous trade and transaction reports.

What we expect from you

We expect you to be operationally resilient against different forms of disruption and to address the root cause to avoid repeated incidents. Where disruption does occur, you should notify us promptly and we expect you to have robust and quick-to-implement alternative arrangements to mitigate adverse consequences. We expect your insourcing and outsourcing arrangements to consist of robust monitoring and oversight, systems and processes, and knowledgeable and experienced people.

We expect you to review your reliance on the services of data vendors and to assess how critical the service is to the operations of your data reporting service. If your reliance on a data vendor meets the criteria for a critical function as prescribed under Article 6 of MiFID RTS 13, we expect you to implement the necessary governance to ensure that the outsourcing of the critical function does not impair your ability to meet your obligations under the regulations. You should be able to demonstrate sufficient oversight and control over services data vendors provide to you, regardless of whether the use of data vendors is deemed to be a critical function.

What we will do

We may conduct work to assess your operational resilience capabilities. Where you have service or connection disruptions, or electronic or physical security breaches, you should notify us in accordance with the DRSP regulatory regime. We will engage with you to understand the root cause and the effectiveness of your remediation plan. Where you are undergoing a material change to your IT systems, you should also notify us. We will engage with you to understand how you are managing associated risks appropriately to mitigate any operational disruption. For DRSPs that form part of wider groups where other entities are also subject to FCA supervision, we may look to leverage operational resilience work being conducted by other FCA supervision and operational risk teams.

<u>Other risks impacting the portfolio</u>

Lack of focus on DRSP business: Particularly where DRSPs form part of a wider group that offers other regulated financial services, we have noted a lack of profile and prioritisation of the activities of the DRSP, compared with other activities of the entity/group. Issues relating to the DRSP are often insufficiently delineated, prioritised and addressed. We have observed varying levels of controls to proactively identify issues with the DRSP; in some cases, too many of these issues are being identified by us or your clients, rather than by your internal controls. We have observed various instances of shared group resource which can lead to a lack of resource being dedicated to the DRSP's operations. We have observed untailored group-level documents that do not reference or sufficiently embed the DRSP Regulatory Framework. In many cases, we have observed a lack of formal DRSP-specific training, with a heavy reliance on on-the-job training. We have also observed instances of key person risk, where DRSP-specific knowledge is concentrated in a small number of staff members. Key person risk is exacerbated by a lack of documentation detailing DRSP-specific processes and procedures.

We expect you to have enough people with the right knowledge, skills, and experience to effectively run your DRSP business. We expect you to review, among other things, DRSP documentation, resource allocation to the DRSP, DRSP training programmes and key person

risk, to ensure that your DRSP is well-resourced and has sufficient profile within the wider business to provide compliant and high-quality data reporting services to the market.

Communication with the FCA/notification regime: We have noted that the frequency of DRSP notifications varies across the portfolio. You should promptly notify us, and your clients if appropriate, of issues affecting your DRSP service. For example, as per the DRSP Regulatory Framework (in particular MiFID RTS 13), you must notify us and clients of service disruptions, or breaches in the physical or electronic security of a DRSP.

As noted above, we expect an open and co-operative supervisory relationship with you. We expect you to meet your obligation to provide regulatory notifications with the appropriate level of detail, to ensure we are consistently and promptly notified of breaches that may impact the provision of the DRSP service, or impact the regulatory reporting requirements of your clients, in compliance with the DRSP Regulatory Framework. You should also notify us of any material change to the information provided at the time of your authorisation, including significant IT system changes or changes to your management body, using the notification procedures as set out in MAR 9. You should therefore regularly review your policies and procedures relating to regulatory notifications to ensure you are fulfilling these requirements. You should have clear and consistent criteria for escalating incidents internally, to clients, the market and us.

Unregulated services: We have noted that operators of DRSPs offer a variety of unregulated services to clients to facilitate trade and/or transaction reporting. These unregulated services may also be operated by the parent entity or an affiliate within the group.

We expect you to have controls to prevent any unregulated services adversely impacting the regulated DRSP service. We do not view issues caused by unregulated services provided by an intragroup entity as any less serious than issues caused by unregulated services provided by the same legal entity as the DRSP. We expect you to be mindful of your responsibilities to ensure accurate and complete data when clients use the unregulated services for their regulatory reporting, regardless of whether these services are being offered by the entity that operates the DRSPs or an affiliated entity.

Effectiveness of DRSP management body**:** Regulation 13 of the DRS Regulations 2017 prescribe requirements for a DRSP's management body. For this portfolio, we have observed that composition of the DRSP management body varies from firm to firm, which may lead to differing levels of DRSP business oversight.

We expect you to review your organisational arrangements to ensure the management body is effective in making key decisions and maintaining oversight of the day-to-day operations of the DRSP operations, in line with the requirements in regulation 13 of the DRS Regulations 2017. DRSPs should review their arrangements to ensure that their governance structure drives strong accountability for the DRSP, minimises gaps in management oversight and enables independent challenge as part of a strong internal control framework.

Conflicts of interest: We have noted several instances where DRSPs do not have DRSP-tailored policies and procedures around the identification, management and disclosure of Conflicts of Interest (COIs). We view operating an ARM or APA as a distinct service, which should be delineated appropriately from any other activities that the entity/Group may perform.

We expect you to have sufficiently tailored policies and procedures in place, in accordance with the requirements in Article 5 of MiFID RTS 13 (*Conflicts of interest*), to "identify, manage and

disclose" existing and potential DRSP-specific COIs. We expect you to review your policies and procedures accordingly.

Other areas of work impacting the DRSP portfolio

This letter does not provide an exhaustive list of the risks to market transparency and market integrity that could arise if DRSPs fail to meet their regulatory requirements. Nor is it an exhaustive list of the work we intend to undertake. Our supervision priorities may change to reflect the evolving nature of your business and markets, and our view of the potential risks.

Here are other priority areas where the FCA will be undertaking work relevant to the DRSP portfolio:

Accessing and using wholesale data
The FCA's Feedback Statement FS22/1: Accessing and using wholesale data identified that competition may not be working as effectively as it should in relation to the provision of trading data. We announced that we will undertake an information gathering and analysis exercise in Spring 2022 to assess the use and value of data in wholesale financial markets, focussing on the pricing of trading data, underlying costs and the terms and conditions of the sale of trading data. This information gathering and analysis exercise will include APAs. We will publish our findings later in 2022.

Wholesale Markets Review
In July 2021, HM Treasury published the UK Wholesale Markets Review: Consultation. The Consultation Response was published in March 2022. The FCA is working closely with the Treasury on the Wholesale Markets Review and will take the outcome of the consultation into account when considering amendments to the transparency regime, as well as in its work in relation to consolidated tape providers. The FCA will consult on changes to the equity transparency regime by the end of Q2 2022 and the non-equity transparency regime in late 2022 or early 2023.

Russia-Ukraine conflict
You are legally obliged to report to the Office of Financial Sanctions Implementation (OFSI) if you know or suspect that a breach of financial sanctions has occurred; if a person you are dealing with, directly or indirectly is a designated person; if you hold any frozen assets; if knowledge or suspicion of these come to you while conducting your business. You must contact OFSI at the earliest opportunity, and you should also notify the FCA. Where transactions give rise to concerns about sanctions evasion or money laundering you should also consider your obligations to report to the UK Financial Intelligence Unit (UKFIU) at the National Crime Agency (NCA) under the Proceeds of Crime Act 2002.

On our website, we have set out points that firms should consider regarding their operational and cyber resilience, following Russia's invasion of Ukraine. Although the UK's National Cyber Security Centre (NCSC) is not aware of any current specific cyber threats to the UK following events in Ukraine, the NCSC has supported US President Biden's call for increased cyber security vigilance among firms in response to Russia's invasion of Ukraine. We're actively encouraging firms to follow the NCSC's guidance as a priority, which covers actions to take to reduce firms' risk of cyber compromise. Alongside this, firms should be ready to report material operational incidents to the FCA in a timely way. During this period, it could be particularly valuable to the FCA and other UK authorities to be notified quickly of operational disruptions.

Our overall expectation of the firms

We remind you that you must disclose to the FCA appropriately anything relating to the firm of which we would reasonably expect notice. That means taking the initiative in doing so, as well as responding to our questions, in an open and timely manner. You are responsible for ensuring that you understand the DRSP Regulatory Framework and comply with it.

You should consider the issues raised in this letter, and how you have ensured that you have addressed them.

Next steps

Should you have any queries about this letter, please contact us on MDIS@fca.org.uk. This is the primary contact for your firm's day-to-day interactions with the FCA.

We recognise there may be occasions when your firm faces urgent issues of strategic importance. In such circumstances, please contact Kirstie Boardwell, Manager, Market Data Infrastructure Supervision on MDIS@fca.org.uk.

Yours faithfully,

Clare Cole

Director of Market Oversight
Financial Conduct Authority