12 Endeavour Square
London
E20 1JN

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

13 December 2024

Dear Chief Executive

Our Custody and Fund Services Supervision Strategy

We write to update you on the FCA's supervision strategy for firms in the custody and fund services sector.[1] This strategy reflects developments in the wider financial markets as well as the external risk environment since we sent our previous letter in March 2022.

Firms in this sector continue to play pivotal roles in safeguarding, administering, and providing oversight of assets under custody (AuC) totalling c.£14.6 trillion.[2] The effective delivery of these services to high standards remains critical to maintaining confidence and participation in UK financial markets.

Our strategy acknowledges the positive and key role that the custody and fund services industry plays in maintaining trust and credibility in the UK financial services system. In contrast to some other financial service businesses that look to take risks in both stable and volatile markets, firms in this sector generally aim to provide safety and stability, and to ensure the smooth flow of services and information irrespective of market conditions.

At the same time, we recognise the potential negative impact to market stability where sector firms' standards fall, as they perform activities that underpin important business services and can both amplify risks or have a direct impact on consumers and markets where service levels fall or are disrupted. The significant operations outsourced to custody and fund services providers could cause issues across the value chain if these risks are not managed well.

[1] The custody and fund services sector broadly covers firms acting as (i) third-party custodians; (ii) depositaries for both authorised and non-authorised funds; and (iii) third-party administrators who provide services such as fund accounting and transfer agency.
[2] An aggregate of submitted figures by firms in our Custody and Fund Services Portfolio under the Client Money and Assets Return (CMAR) as at June 2024.

We have observed trends with risk implications for the sector. These include firms' significant and increasing roles as outsourced service providers to the UK financial services sector; a heightened external cyber threat environment; changes in transactional standards and structures (such as settlement cycles); modernisation of market infrastructure; rapidly-evolving technological innovations (including digital assets and distributed ledger technology (DLT)); and firms' readiness to cope with market transformations (including growth of private markets). There is a clear need for sector firms to be prepared for these trends and changing conditions and be responsive to client needs.

This letter seeks to provide clarity on our current supervisory focus. It sets out our views on the key risks of harm that firms in the sector must manage in order for financial markets to work well. Shifts in regulation, technology and business environment may require adjustments to our supervisory strategy and we will update you as needed where these are material.

We ask you to consider the key risks of harm below and adopt strategies for mitigating them where relevant. In our future supervisory engagements with you, we will consider whether your governing bodies and Senior Managers with accountabilities have taken appropriate actions in response.

Supervisory approach

We continue to apply an outcomes-based regulatory approach by setting and testing high standards. The outcomes we seek are explained in our supervisory priorities below.

At the individual firm level, the responsibility for identifying, assessing and addressing the actual and potential risks of harm remains with your firm, in particular the executives accountable under the Senior Managers Regime as well as the management committees with delegated responsibilities. We expect those to be overseen by an appropriate governing body and governance structure.

Where we identify outliers, we will focus supervisory resources on driving appropriate remediation and risk reduction by those outliers.

Our supervisory priorities

<u>Operational resilience</u>

Our view of the risk:

Sector firms provide critical infrastructure and services to the financial markets and have high levels of operational risk. We continue to see weaknesses in the sector particularly due to operational frictions in transaction processing, settlement, delivery of outsourced services, and end-of-life technology or aged infrastructure assets.

What we will do:

Our supervisory engagements will focus on monitoring in-scope[3] firms' compliance with, and embeddedness of, rules and guidance on building operational resilience as set out in Policy Statement PS21/3.

Under those requirements, in-scope firms must have performed mapping and testing by 31 March 2025 to provide assurance they are able to remain within impact tolerances (ITOLs) for each important business service in severe but plausible scenarios. These firms must also have made the necessary investments and any operational changes to enable them to operate consistently within ITOLs.

Where an in-scope firm is dual-regulated by the FCA and the Prudential Regulation Authority (PRA), it should ensure ITOLs are considered in line with the statutory objectives of each Authority.[4] This entails setting ITOLs for the point at which there is an intolerable level of harm to consumers or risk to market integrity in respect of FCA objectives, and the point at which financial stability or a firm's safety and soundness is at risk in respect of PRA objectives.

Given the operational linkages between the custody and fund services sector and other closely related sectors (including asset management and alternatives), we will be undertaking focused assessments on how key sector firms have coordinated with clients and third parties to drive cross-sector resilience.

What we expect of you:

We expect to see strong ownership of operational resilience by your governing bodies or equivalent management body. Firms' governing bodies should review and approve annual operational resilience self-assessments as required under PS21/3. We would expect governing bodies to seek relevant technical expertise where prudent to assure themselves of self-assessments' adequacy. We will be looking for evidence of prompt deployment of incident management plans; prioritisation of important business services to reduce operational and client impact; detailed mapping of third-, fourth- and N^{th}-party relationships for understanding exposure; and processes for clear communication with the regulator where required.

The UK gilt market volatility in Q3/Q4 2022 exposed significant operational challenges amid difficult market conditions. Deficiencies in transaction processing and collateral management were evident at a number of firms. Our guidance and recommendations for LDI managers set out wider lessons on resilience and risk management that may be useful for all firms in the sector.

---

[3] In-scope firms are those to which Policy Statement PS21/3 applies as well as those that have voluntarily undertaken to comply.

[4] Our expectation is that, while in-scope firms need to set ITOLs for each important business service by reference to that Authority's operational resilience rules, they will effectively manage the tolerances together. These firms may set their separate ITOLs at the same point if they deem it suitable for the purposes of each Authority, but will need to be able to justify this decision if challenged. See 3.20 of PS21/3 for further details.

Cyber resilience

Our view of the risk:

Firms' sub-optimal cyber resilience and security measures continue to create risks in this sector, particularly in view of the public alerts issued by the UK National Cyber Security Centre (NCSC) and the CBEST thematic report we published jointly with the Bank of England and the PRA in 2023 that sets out our observations from the tests carried out in this sector.

What we will do:

We continue to focus on cyber resilience, including on how effectively firms manage critical vulnerabilities, threat detection, business recovery, stakeholder communication and remediation efforts to build resilience.

What we expect of you:

Firms should remain vigilant on the external cyber threat realities; evaluate the challenges holistically; and focus resources on strengthening their operational and cyber defence environment. Firms should make effective use of threat intelligence-led penetration testing at regular intervals as a diagnostic tool to help ensure a robust environment.

Firms' governing bodies should ensure that the management information provided to them provides an assessment of the risk present in their firms and not just the effectiveness of their controls.

Third-party management

Our view of the risk:

We consider the residual risk in respect of sector firms' third-party management to remain high, noting the extent and frequency of various operational incidents involving third parties. Recent IT events are illustrative of the magnitude and speed at which third-party incidents can arise and the far-reaching impact they can have.

The likelihood of service degradation or failure increases when there is inadequate oversight and mapping of third-, fourth- and N^{th}-party providers for important business services. We also observe deficiencies in actionable exit strategies and contingency arrangements, such as the identification of alternative providers of key services and the practical capability to stand these up at sufficient pace to avoid harm.

What we will do:

We will assess firms' third-, fourth- and N^{th}-party oversight, including key material supplier relationships and management. We will review your understanding of the level of outsourcing; key vulnerability considerations; concentration risk; exit and contingency preparations; "fourth-party" visibility; and the level of bilateral co-

operation on testing and change management with key stakeholders (including clients and suppliers).

What we expect of you:

We expect firms to have effective processes to identify, manage, monitor and report third-party risks, and to perform an assessment on, and mapping of, third-party providers. We will ask you about your controls to avoid over-reliance and to identify areas where it is important to build your own core resilience.

Change management

Our view of the risk:

Technological transformation is affecting this sector and ultimately influencing client and consumer outcomes along the value chain. Firms are updating obsolete technology, increasing utilisation of automation and considering use cases for artificial intelligence (AI). These firms are having to balance the changes against other demands such as digital assets innovation and DLT, regulatory developments (such as settlement cycle changes) and market changes (notably growth of private markets).

Poor change management practices could result in firms failing to adequately address critical and changing operational demands. We are concerned that, where firms are unable to cope with these challenges, there is potential for operational and other issues to adversely affect consumers and market integrity.

What we will do:

We will seek to assess the change management frameworks in a selection of firms. This will include looking at the overall approach and methodology, including testing to understand how client and consumer outcomes have been considered as a critical aspect of the change management framework.

What we expect of you:

Our Implementing Technology Change multi-firm review highlighted key areas (such as good governance, resource sufficiency and effective risk management) that contribute towards successful change management. We suggest that you consider these best practices appropriately in your framework. We also encourage you to seek early dialogue with us in the planning phases of any major firm initiatives or strategy change that may have significant impact on your business model(s), operations (especially your important business services) and/or the broader market.

Market integrity

Our view of the risk:

The size, scale and complexity of sanctions imposed by the UK Government and international partners in response to significant geopolitical events in recent years have

increased the risk of firms' sanctions systems and controls failing to comply adequately with the evolving requirements.

What we will do:

Our supervisory engagements will review the effectiveness of select firms' systems and controls, governance processes and resource sufficiency in connection with sanctions regime compliance. Where material deficiencies are discovered, we will use appropriate regulatory tools to drive effective and sustainable remediation and step-change for achieving better market integrity outcomes.

What we expect of you:

We expect firms to have effective governance and oversight, skills and resources, screening capabilities, Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures and regulatory breach reporting mechanisms. You should ensure that your firm has proper risk procedures and internal control mechanisms to detect, prevent and deter financial crime. These need to be appropriate and proportionate to the nature and scale of your business. Senior management should take clear responsibility for managing financial crime risks and be actively engaged in addressing these risks. Your firm's efforts to combat financial crime should be subject to challenge, including having robust internal audit and compliance processes that routinely test the firm's defences against specific financial crime threats.

Depositary oversight

Our view of the risk:

Depositaries play a critical role in overseeing the activities of authorised fund managers as well as alternative investment fund managers (collectively, AFMs), safekeeping of fund assets and cashflow monitoring. In discharging their duties, depositaries are expected to act independently, honestly, fairly, professionally and solely in the interest of the relevant fund and its investors.

We see a gap in expectations among market participants, the FCA and, potentially, consumers over the role of depositaries. Engagement with depositaries over the last two years have shown that in practice depositaries have often demonstrated a less than proactive approach to their oversight, risk identification and escalation processes. We continue to see examples of ineffective intervention or challenge which risks investors not receiving adequate protection and could result in or contribute to harm such as financial loss.

What we will do:

As we set out in our discussion paper DP23/2, we will look for opportunities to clarify our rules and expectations of depositaries.

What we expect of you:

We expect depositaries to act more proactively in the interests of fund investors. They should be providing effective independent oversight of AFMs' operations and funds' adherence to FCA rules on investment and borrowing powers, liquidity, valuation, pricing and dealing. They are expected to have processes in place to ensure they receive the information needed to perform their duties.

Protection of Client Assets (CASS)

Our view of the risk:

Compliance with CASS is a fundamental component of the FCA's public commitment to reducing harm in firm failure. This is a regulatory priority set out in our 2024/25 Business Plan.

We have observed weaknesses in books and records, change management and dependency on legacy or end-of-life IT infrastructure and high levels of manual processing and controls. We believe these challenges in CASS compliance have root causes in poor governance and oversight, under-investment in systems and failure to fully consider CASS impacts when managing change. We highlighted these risks in our 2022 portfolio letter and continue to identify residual challenges in these areas for firms.

What we will do:

We will continue to use a range of supervisory tools, from proactive engagements with firms to CASS assessments, to identify weaknesses. For the worst cases, we will use our formal intervention powers.

What we expect of you:

We expect firms to review their practices and take action on the issues identified. As technological change in this sector remains significant, we continue to expect firms to have considered and be appropriately prepared for developments such as the increasing use of distributed ledger technology and the future financial services regime for cryptoassets as set out in our discussion paper DP23/4.

Next steps

Please discuss this letter with your governing body and Executive Committee.

You should take all necessary actions to ensure the relevant FCA requirements and expectations are met and reinforce accountabilities with your Senior Managers for the risks set out above. You can expect us to exercise appropriate supervisory scrutiny on these matters (including asking for supporting evidence on your actions, success measurements and outcomes) during our future supervisory engagements.

Contacts

Should you have any queries or feedback, please contact your usual FCA supervisor or via our contact page if you do not have a named supervisor. For those of you with dedicated supervisors, this letter supplements your Firm Evaluation letter and the ongoing supervisory programme.

In the event your firm faces or anticipates urgent issues of strategic or systemic importance, please contact Christopher Davis, the Head of Department for Market Interventions – Asset Management & Funds, at Christopher.Davis@fca.org.uk.

Yours faithfully

Camille Blackburn
Director – Wholesale Buy-Side
Financial Conduct Authority