167 Fleet Street, London EC4A 2EA, UK
+44 (0)20 7822 8380
info@aima.org
aima.org

European Commission
Directorate-General for Financial Stability,
Financial Services and Capital Markets Union

Submitted via online questionnaire

19 March 2020

RE: AIMA's response to the European Commission consultation on a potential initiative on the digital operational resilience in the area of financial services

The Alternative Investment Management Association Limited (AIMA)[1] appreciates the opportunity to submit its answers to the European Commission in relation to its online questionnaire on a potential initiative on digital operational resilience (cyber security) in the area of financial services.

AIMA answers to relevant questions in the online questionnaire:

1. Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?

We appreciate that the ever-increasing digitalisation of finance, the growing interconnectedness across financial institutions and third parties, and the increased number of cyber threats bring about the need for financial institutions to appropriately strengthen their resilience against cyber-attacks. We also acknowledge that firms of all sizes need to develop a 'security culture'. However, we believe that there needs to be an element of proportionality with any future regulation in this area. Smaller and medium- sized firms will need to take a risk-based approach to their security planning in line with their size, available resources and capabilities. The

[1] AIMA, the Alternative Investment Management Association, is the global representative of the alternative investment industry, with more than 1,900 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than $2 trillion in assets. AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides. AIMA works to raise media and public awareness of the value of the industry. AIMA set up the Alternative Credit Council (ACC) to help firms focused in the private credit and direct lending space. The ACC currently represents over 170 members that manage $400 billion of private credit assets globally. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For further information, please visit AIMA's website, www.aima.org.

expectation levels of competent authorities will clearly need to vary depending on the size of the financial entity and its associated impact on customers and the wider financial system.

We would encourage EU policy makers to strongly consider international developments in the area of cyber security governance and reporting. Firms with operations in multiple jurisdictions may be required to adapt their policies and procedures according to the local regulations and therefore a fragmented approach to rulemaking could lead to a patchwork of guidance or frameworks ultimately increasing costs and burdens for the financial services industry and their customers. As highlighted in the Commission's consultation document, it is essential that financial supervisors' efforts work in a harmonised and convergent manner.

We would also emphasize that the European Banking Authority (EBA) recently published its guidelines on ICT and security risk management for credit institutions, investment firms and payment service providers. These guidelines, due to enter into force on 30 June 2020, have set out expectations on how firms should manage internal and external ICT and security risks that they are exposed to. Firms will be incorporating, or already have incorporated, these supervisory expectations into their governance, operations, project and change management and business continuity management programmes.

We were pleased to have previously submitted input to the Financial Stability Board (FSB)'s consultation[2] last year on developing a toolkit of effective practices relating to a financial institution's response to, and recovery from, a cyber incident. Our responses to the Commission's consultation reflect many of the views that we have previously shared with the FSB.

A common challenge of running information security programmes relates to the proliferation of cyber security standards around the world. We understand that the number of standards relating to cyber security in some form exceeds 1,000 publications globally. The complex landscape can make it difficult for asset managers of different sizes and organisational patterns to identify and select the standards relevant to their organisation.

There is no one-size fits all solution to cyber incident response and recovery planning: each asset manager's reaction must be appropriate to them and proportionate to their budget. Increasing cyber-defence expenditure is not always the most effective solution. With this in mind, AIMA has made available for its members a Guide to Sound Practices for Cyber Security.[3] The Guide goes through the material considerations in the wider cyber debate to enable asset managers to have informed internal discussions to respond to the threat. This Guide is not intended to be the solution to any asset manager's cyber security issues. It is designed to frame the principles of the debate rather than directing it. The Guide seeks to enable those responsible for the implementation of a cyber security programme to really understand the range of problems as well as to consider more sensibly what is and what is not applicable to them.

---

[2] See https://www.fsb.org/wp-content/uploads/P110719.pdf

[3] See https://www.aima.org/sound-practices/guides-to-sound-practices.html

19. How do you enhance the cyber security awareness within your organisation?

There has recently been greater emphasis on training and testing of all employees regarding phishing attacks, for example. We appreciate the importance of training given that human error is considered one of the biggest contributors to cyber security breaches. However, the expectation for employees at all levels in an organisation to have a good understanding of cyber risks is an observed challenge. It can also be difficult to garner the attention of Board members on the details of cyber risk initiatives given the technical nature of cyber security issues and the multiplicity of other strategic and operational issues that are on their agendas.

Many regulators mandate that all relevant employees of firms must undertake compliance, anti-money laundering and anti-bribery training. We believe that consideration should be given to extending this to cybersecurity awareness training. It could be introduced as a requirement for firms to assess their employees' ICT security risk awareness. This step alone would significantly increase the security in financial services.

23. What level of detail would be required for the ICT and security incident reporting?

Finding the correct balance in responding to perceived cyber security threats while protecting commercial and client interests is a challenge. The potential consequences of under-reacting or over-reacting to such threats are significant, and both risks need to be carefully considered in the assessment stage. Taking drastic steps can leave a business open to criticism and reputational damage, but not taking steps could lead to fines. There needs to be clear materiality threshold guidance as to when exactly a cyber incident needs to be reported to the competent authorities or communicated to other relevant stakeholders. Another important factor to consider is the importance of designating responsible persons for determining the materiality of incidents and incident reporting.

29. Should all financial entities be required to perform a baseline testing of their ICT systems and tools?

We believe that setting requirements to perform cyber resilience testing should include flexibility and proportionality in order to address specific needs of financial actors by virtue of their size, complexity and scale of operations.

30. For the purpose of being subject to more advanced testing (e.g. threat led penetration testing, TLPT), should financial entities be identified at EU level (or should they be designated by competent authorities) as "significant" on the basis of which criteria

For the purpose of significant entities being subject to more advanced testing, we believe that financial entities should be designated by national competent authorities as "significant" on the basis of proportionality–related factors (i.e., the size, type, profile and business model of the firm).

37. What is your view on the possibility to introduce an oversight framework for ICT third-party providers?

With the engagement of external organisations in business operations, exposure to threats and risks can be increased. Threats arising from third-party engagements require asset managers to adopt a mission-critical risk management approach. For example, understanding which services are deemed crucial will help in the development of an institution's cyber incident response and recovery plan. Any new rules around increased oversight of third-party providers should be proportionate.

42. Do you consider you need more information sharing across different jurisdictions within the EU?

Many firms already share information about cyber threats and vulnerabilities in various forums because participation in such forums enhances their own situational awareness. This awareness not only helps firms better assess vulnerabilities, but improves their analysis and production capabilities. We believe there is increased need for cyber information sharing between firms as well as between competent authorities. This could be done through industry bodies (e.g., the UK-based Financial Sector Cyber Collaboration Centre - FSCCC) or through government initiatives (e.g., the UK's Cyber Security Information Sharing Partnership - CiSP). We also believe that there could be better cyber information sharing coordination on a global level, though appreciate there might be barriers including a lack of a common taxonomy/lexicon on cyber incidents.