MANAGED FUNDS ASSOCIATION
The Voice of the Global Alternative Investment Industry
WASHINGTON, DC | NEW YORK

March 19, 2020

DG FISMA
European Commission
1049 Brussels
Belgium

Via online questionnaire

Re: MFA Comments on European Commission Consultation Document – *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure*

To Whom It May Concern:

Managed Funds Association ("**MFA**")[1] welcomes the opportunity to provide comments in response to the European Commission Consultation Document on *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure* (the "**Consultation**").

MFA members, as investors in European markets and professional asset managers for European institutional investors, expend significant resources in ensuring that they maintain robust digital operational resilience. Alternative investment fund managers are fiduciaries to their investors and have an obligation to safeguard their resources. As such, they invest heavily in both operational resilience and cybersecurity. In addition, financial services firms are already subject to a number of legal and regulatory requirements relating to operational resilience.

We appreciate the Commission's consideration of ways to enhance operational resilience of EU financial services firms. We raise two general comments for the Commission's consideration: (1) enhancing security by building off of the existing regulatory framework; and (2) enhancing the public sector's stewardship of sensitive financial services data.

A. Enhancing security by building off of the existing regulatory framework

We believe the most effective way for the EC to enhance operational resilience of financial services firms is by working through the existing regulatory framework rather than developing a new digital operational resilience testing framework. Financial services firms

[1] MFA represents the global alternative investment industry and its investors by advocating for sound industry practices and public policies that foster efficient, transparent, and fair capital markets. MFA, based in Washington, DC, is an advocacy, education, and communications organization established to enable hedge fund and managed futures firms in the alternative investment industry to participate in public policy discourse, share best practices and learn from peers, and communicate the industry's contributions to the global economy. MFA members help pension plans, university endowments, charitable organizations, qualified individuals, and other institutional investors to diversify their investments, manage risk, and generate attractive returns. MFA has cultivated a global membership and actively engages with regulators and policy makers in Asia, Europe, the Americas, Australia and many other regions where MFA members are market participants.

have a vested interest in implementing and maintaining robust operational security. As technology changes quickly, firms should have the flexibility to quickly adjust their own operational resiliency testing. If a new testing framework is developed, we strongly urge that it focus only on systemic firms and incorporate a proportionate approach.

We are also concerned with the ESAs recommendation for the Commission to consider a comprehensive, harmonized system of information and communications technology (ICT) incident reporting requirement. While the intention of such a system is well-meaning, we believe it is unnecessary and would not be practical. First, the EU General Data Protection Regulation already requires firms to report personal data breaches. Second, financial services firms may receive many information security attacks a day, and imposing requirements on them to immediately report security incidents would detract firm resources from responding to and addressing attacks or incidents. Whichever authority would need to receive such data would also likely be overwhelmed by the volume and scope of security incident reports.

B. Enhancing the operational resilience of EU institutions

As the Commission considers the digital operational resilience of financial services firms, MFA respectfully urges the Commission to also address the operational resilience of regulators and how they protect data of financial firms that may be market sensitive, proprietary, and confidential. Specifically, in response to the Consultation Document question 27, we provide the below response.

Question 27: What factors or requirements may currently hinder cross-border cooperation and information exchange on ICT and security incidents?

One of the biggest factors that may hinder cross-border cooperation, or more accurately, trust in the regulatory supervisory process, is the protection, by regulators and supervisors, of the data that is reported.

Financial firms, especially asset managers, are subject to robust reporting requirements across the EU, including rules that require reporting of confidential, proprietary, or other sensitive information. MFA acknowledges that regulators need information from regulated entities to oversee financial markets effectively. However, regulators and supervisors are at least as susceptible—if not more—than the private sector to hacks, leaks and spills of sensitive data. We, therefore, strongly encourage the Digital Operational Resilience Framework to scope in public sector entities such as securities regulators, supervisors, and central banks, to ensure that these entities are handling sensitive data with appropriate safeguards.

To this end, MFA strongly encourages the EU to take the lead on requiring regulators and supervisors to implement a robust process for assessing the necessity of acquiring highly sensitive, confidential information, including valuable intellectual property. The inadvertent disclosure of confidential and proprietary data, whether by leak, hack, or other means, endangers the firm whose data is disclosed, and could impact the ability of those firms to manage risk, including on behalf of their investors.

As the European Commission continues its work, we encourage it to ensure that information reported to regulators and supervisors, including national competent authorities, is subject to robust data protection, and that cross-border exchanges of confidential and proprietary data also are subject to robust protection.

MFA advocates for three simple recommendations to protect the confidential and proprietary data of financial entities.

- First, regulators and supervisors should tailor reporting requirements to ask for only the data that is necessary to achieve their function.

- Second, regulators and supervisors should build protections into their forms and reporting systems, including alphanumeric identifiers rather than names and other identifying information.

- Third, regulators and supervisors should tier their protections and security protocols based on the level of sensitivity of the data.

* * * * * * *

MFA thanks the European Commission for the opportunity to provide comments on the Consultation Document. We would welcome the opportunity to discuss our views in greater detail. Please do not hesitate to contact Michael Pedroni, Executive Vice President & Managing Director, International Affairs, or Jennifer Han, Associate General Counsel at +1 (202) 730-2600 with any questions the European Commission or its staff might have regarding this letter.

Respectfully submitted,

/s/ Michael Pedroni

Michael Pedroni
Executive Vice President & Managing Director,
International Affairs