Consultation Response

European Commission Public Consultation on 'Revision of the NIS Directive'

2nd October 2020

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on **CONSULTATION ON THE REVISION OF THE NIS DIRECTIVE.** AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

We summarise below our high-level response to the consultation, which is followed by answers to the individual questions raised.

I. General comments

Executive Summary

AFME welcomes the European Commission public consultation on ***'Revision of the NIS Directive'*** **(the "CP").** We believe that the focus of this CP is a positive effort to propose legislative changes that can deepen harmonisation and reduce fragmentation across the European Single market, while strengthening the level of preparedness and response to cyber threats..

AFME recognises the increasing importance of digitisation, for the wider-economy, including financial services, and the potential implications for cyber and Information and Communications Technology (ICT) risks. In this respect AFME has also provided recommendations to the European Commission public consultation on 'Digital Operational Resilience: Making the EU financial sector more secure', and welcomes the policy initiatives announced by the European Commission in its 'Digital Finance Package'[1]. This will minimise the risk of diverging requirements across Member States and provide consistent and clear regulatory requirements; particularly important for firms operating cross-border.

The NIS Directive can support this objective by harmonising cybersecurity requirements and reducing fragmentation across Member States.

AFME has identified the following high-level considerations for the European Commission in response to this CP:

- **The proposed legislative changes should focus on harmonisation and reducing fragmentation in the European Singe Market. The requirements should be consistent, and not duplicate, existing regional and global principles and regulation relating to cyber and ICT risks.**
    - AFME is supportive of the NIS Directive as an effort to increase Member States capabilities to respond and recover from cyber threats. This will improve cooperation and promote a culture of security. A common standard for cybersecurity would bring benefits to for firms operating across multiple jurisdictions.

[1] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

- However, currently there is insufficient harmonisation due to fragmentation (with sectoral requirements and Member State transposition) which creates complexity and inefficiencies across the EU.
- AFME recommends the Commission address this issue in line with the Commission's objectives as part of the Digital Finance Package. AFME is supportive of the measures announced that recognise the need for increased harmonisation and removing fragmentation for ICT and cybersecurity requirements applicable to financial services.
- In this regard, we request further clarity on how the NIS Directive is complementary the measures announced in the Digital Finance Package, and other EU or Member State sectoral requirements(e.g. EBA ICT GLs, EBA Outsourcing GLs, ECB CROE).

- **The proposed legislative changes should remain principles based and focus on minimum requirements for the management of cyber and ICT risks across the EU financial services sector. They should also promote consistency at the global level.**
  - AFME is supportive of an EU regulatory framework that is principles-based, technology neutral, and promotes global consistency. This will reduce fragmentation and support the uptake of innovative technologies in financial services. This approach for cyber and ICT security risk management will ensure requirements can be implemented with proportionality in mind, across firms of various size, complexity and location, in a way that is commensurate to the risks.
  - Further, the introduction of prescriptive and detailed legislative requirements are at risk of becoming obsolete in the short to medium term as cyber threats and innovation in technology continues at pace.
  - AFME recommends the Commission maintain consistency of any legislative proposals to ongoing discussions on at the Basel Committee for Banking Supervision (BCBS), the Financial Stability Board and the G7, to ensure alignment with global efforts.

- **The proposed legislative changes should continue to support innovation in the EU.**
  - AFME recognises the increasing importance of digitisation for financial services and the wider EU economy. The European Commission, through a combination of policies (e.g. financial services specific and horizontal), has increasingly embraced digitisation and innovation for the financial sector over the past five years. In a fast-evolving and competitive environment, Europe must continue to set ambitious goals for the adoption and scaling-up of innovative technologies and ensure consumers and firms remain at the forefront of global trends (as identified in the European Commission Digital Finance Package).

AFME welcomes the opportunity to discuss our response to this CP and to identify opportunities to support this important initiative.

II. Comments to the sections of the public consultation

1. General questions on the NIS Directive

- ***Feedback on proposed legislative changes***

Supporting Information

Question	In scope/Out of scope	Response
1.a. Relevance of the NIS Directive		
1	AFME to respond	• Increase the capabilities of Member States: Relevant • Improve the level of cooperation amongst Member States: Relevant • Promote a culture of security across all sectors vital for our economy and society: Relevant

		• AFME is supportive of the NIS Directive as an effort to increase Member State capabilities to respond and recover from cyber threats, and improving cooperation and promoting a culture of security across the EU. • However, AFME continues to believe that more should be done to reduce fragmentation of cybersecurity regulation across the financial services industry. As the FSB highlighted in its 2017 stocktake of cybersecurity regulations[2], the trend in this area is for further unilateral regulation of cybersecurity practices of financial services firms by national authorities rather than greater coherence. • A globally fragmented cybersecurity regulatory environment increases financial stability risk and complexity for individual firms. Where regulations relate to the management of incidents or the testing of systems, cross-border coordination is especially important to ensure that resources are not unnecessarily diverted away from the management of activities such as protecting critical systems. • AFME is therefore supportive of the European Commission's efforts to promote harmonisation of cybersecurity requirements in the EU and as identified in the recent Digital Finance Package.
1.b. Cyber-threat landscape		
1	AFME to <u>not</u> respond	• Don't know / no opinion.
		• During the COVID-19 pandemic financial firms and government agencies experienced an increase in COVID-related phishing and business email compromise schemes, credential stuffing, malware, ransomware and denial of service attacks, and incidences of financial fraud against unemployment systems, stimulus payments and websites selling defective Personal Protection Equipment (PPE). • Financial firms are well prepared for these types of events given the significant cybersecurity investments made to date and the level of preparation and testing conducted by business continuity and crisis managers at each financial firm. Even given the extreme nature of this event and significant swings in market volumes and volatility, the financial sector showed significant resilience – the global markets operated well, the major global equity, fixed income and derivatives exchanges performed without incident and trades cleared and settled timely without any major failures across the sector or individual financial firms.
2	AFME to <u>not</u> respond	• Don't know / no opinion.
1.c. Technological advances and new trends		
1	AFME to respond	• AFME recognises the increasing importance of digitisation for the wider-economy and financial services, and the need to continue supporting the development of digital finance in the EU. The European Commission, through a combination of policies (e.g. financial services specific and horizontal), has increasingly embraced digitisation and innovation for the financial sector over the past five years. In a fast-evolving and competitive environment, Europe must continue to set ambitious goals for the adoption and scaling-up of innovative technologies and ensure consumers and firms remain at the forefront of global trends. • AFME is supportive of EU regulatory framework that is principles-based, technology neutral and innovation-friendly. Such a framework, for cyber

[2] https://www.fsb.org/wp-content/uploads/P131017-2.pdf

		and ICT security risk management, will ensure requirements can be implemented with proportionality in mind, across firms of various size, complexity and location, in a way that is commensurate to risks.
1.d. Added value of EU cybersecurity rules		
1	AFME to respond	• Cyber risks can propagate across borders at high speed, which is why cybersecurity rules should be aligned at Union level: Agree • The mandatory sharing of cyber risk related information between national authorities across Member States would contribute to a higher level of joint situational awareness when it comes to cyber risks: Agree • All entities of a certain size providing essential services to our society should be subject to similar EU-wide cybersecurity requirements: Agree
		• AFME is supportive of the NIS Directive as an effort to increase Member States capabilities to respond and recover from cyber threats, improving cooperation and promoting a culture of security. • However, AFME continues to believe that more should be done to reduce fragmentation of cybersecurity regulation, across the financial services industry. As the FSB highlighted in its 2017 stocktake of cybersecurity regulations, the trend in this area is for further unilateral regulation of cybersecurity practices of financial services firms by national authorities rather than greater coherence. Rather than improving resilience, a globally fragmented cybersecurity regulatory environment for the industry increases financial stability risk by driving complexity into the system. Where regulations relate to the management of incidents or the testing of systems, cross-border coordination is especially important to ensure that resources are not unnecessarily diverted away from the management of cybersecurity activities such as protecting critical systems. • Alongside this need, the mandatory sharing of cyber risk related information between national authorities across Member States could reduce the burden on firms, currently having to report to individual each Member States, while fostering closer cooperation and dialogue between authorities. • AFME is supportive of the European Commission's efforts to foster greater information sharing between Member States authorities and the harmonisation of cybersecurity requirements in the EU.
1.d. Sectoral scope		
1	AFME to <u>not</u> respond	• Public administration: Don't know • Food supply: Don't know • Manufacturing: Don't know • Chemicals: Don't know • Waste water: Don't know • Social networks: Don't know • Data centres: Don't know
2	AFME to <u>not</u> respond	• Don't know / no opinion
3	AFME to <u>not</u> respond	• Don't know / no opinion
1.f. Regulatory treatment of OES and DSPs by the NIS Directive		
1	AFME to <u>not</u> respond	• Don't know / no opinion
1.g. Information sharing		

1	AFME to respond	• No
		• AFME welcomes tools and mechanisms to facilitate information sharing across the financial sector. Theses forums enable firms to prepare, respond and recover from incidents, based on voluntary sharing of non-sensitive or confidential data, between trusted parties. • AFME also welcomes the Commission's proposal under the Digital Finance Package to harmonise incident reporting requirements across the EU (e.g. reporting content and template) and the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. However, we believe that the industry should be actively involved in harmonisation process, providing feedback and supporting the development of appropriate requirements, that can be implemented in line with internal controls and with proportionality in mind. • AFME cautions the European Commission in creating additional mandatory requirements, geared towards information sharing, which may limit the qualitative input of these trusted networks. Rather, the Commission could build awareness to a broader set of firms, across the EU, to use the current existing mechanisms and tools available for information sharing. • AFME recommends the European Commission consider that the sharing of cyber threats and incidents could present challenges for firms due to the confidential/sensitive nature of the data. The benefits of information sharing could be significantly reduced if firms were too be scrutinised on the basis of the information shared. We believe that information sharing benefiting the financial sector, prepare, respond, and recover from incidents, should be based on voluntary sharing of non-sensitive or confidential data, between trusted parties.

2. Functioning of the NIS Directive

- ***Feedback on proposed legislative changes***

Question	Comment	Reasoning
2.a. National Strategies		
1	AFME to respond	• Relevant
		• AFME is supportive of common objectives set at an EU level for the adoption of national strategies on the security of network and information systems. This will reduce fragmentation and foster harmonisation of cybersecurity requirements in the EU. However, while EU harmonisation is key to reduce fragmentation in the Single Market, AFME recommends the Commission maintain consistency of any legislative proposals to ongoing discussions on at the Basel Committee for Banking Supervision (BCBS), the Financial Stability Board and the G7, to ensure alignment with global efforts.
2	AFME to not respond	• Don't know / no opinion
2.b. National competent authorities and bodies		
1	AFME to not respond	• Level of funding: Don't know • Level of staffing: Don't know • Level of expertise: Don't know • Cooperation of authorities across Member States: Don't know

		• Cooperation between national competent authorities within Member States: Don't know
2	AFME to not respond	• Level of funding: Don't know • Level of staffing: Don't know • Level of operational capabilities: Don't know • Level of expertise: Don't know • Cooperation with OES and DSP: Don't know • Cooperation with relevant national authorities (such as sectoral authorities: Don't know
3	AFME to not respond	• Don't know / no opinion
4	AFME to not respond	• Don't know / no opinion
5	AFME to not respond	• Don't know / no opinion
6	AFME to not respond	• Don't know / no opinion
7	AFME to not respond	• Don't know / no opinion
8	AFME to not respond	• Don't know / no opinion
9	AFME to not respond	• Don't know / no opinion
10	AFME to not respond	• Don't know / no opinion
2.c. Identification of operators of essential services and sectoral scope		
1	AFME to not respond	• The current approach ensures that all relevant operators are identified across the Union: Don't know • OES are aware of their obligations under the NIS Directive: Don't know • Competent authorities actively engage with OES: Don't know • The cross-border consultation procedure in its current form is an effective element of the identification process to deal with cross-border dependencies: Don't know • The identification process has contributed to the creation of a level playing field for companies from the same sector across the Member States: Don't know
2	AFME to not respond	• Definitions of the types of entities listed in Annex II are sufficiently clear: Don't know • More sectors and sub-sectors should be covered by the Directive: Don't know • Identification thresholds used by Member States should be lower: Don't know
3	AFME to not respond	
4	AFME to not respond	• Electricity: Don't know • Oil: Don't know • Gas: Don't know • Air transport: Don't know • Rail transport: Don't know • Water transport: Don't know • Road transport: Don't know • Banking: Don't know • Financial market infrastructures: Don't know • Health sector: Don't know • Drinking water supply and distribution: Don't know • Digital infrastructure: Don't know

5	AFME to not respond	• Electricity: Don't know • Oil: Don't know • Gas: Don't know • Air transport: Don't know • Rail transport: Don't know • Water transport: Don't know • Road transport: Don't know • Banking: Don't know • Financial market infrastructures: Don't know • Health sector: Don't know • Drinking water supply and distribution: Don't know • Digital infrastructure: Don't know
6	AFME to not respond	• Small companies: Don't know • Medium-sized companies: Don't know
7	AFME to not respond	• Don't know / no opinion
2.d. Digital service providers and scope		
1	AFME to not respond	• Annex III of the NIS Directive covers all relevant types of digital services: Don't know • Definitions of the types of digital services listed in Annex III are sufficiently clear: Don't know • DSPs are aware of their obligations under the NIS Directive: Don't know • Competent authorities have a good overview of the DSPs falling under their jurisdiction: Don't know • Competent authorities actively engage with DSPs under their jurisdiction: Don't know • Security requirements for DSPs are sufficiently harmonised at EU level: Don't know • Incident notification requirements for DSPs are sufficiently harmonised at EU level: Don't know • Reporting thresholds provided by the Implementing Regulation laying down requirements for Digital Service Providers under the NIS Directive are appropriate: Don't know
2	AFME to not respond	• N/A
3	AFME to not respond	• The more harmonised regulatory approach applied towards DSPs as compared to OES is justified by the cross-border nature of their services: Don't know • Subjecting DSPs to the jurisdiction of the Member State where they have their main establishment in the EU minimises the compliance burden for those companies: Don't know • The limitation related to the supervisory power of the national authorities, notably to take action only when provided with evidence (ex-post supervision), in the case of the DSPs is justified by the nature of their services and the degree of cyber risk they face: Don't know • The exclusion of micro- and small enterprises is reasonable considering the limited impact of their services on the economy and society as a whole: Don't know
4	AFME to not respond	• Online marketplaces: Don't know • Online search engines Don't know • Cloud computing services: Don't know

5	AFME to not respond	• Don't know / no opinion
6	AFME to not respond	• Online marketplaces: Don't know • Online search engines: Don't know • Cloud computing services: Don't know
7	AFME to not respond	• Online marketplaces: Don't know • Online search engines: Don't know • Cloud computing services: Don't know
2.e. Security requirements		
1	AFME to respond	• What is the impact of imposing security requirements on OES by the NIS Directive in terms of cyber resilience? Don't know / no opinion
		• The Directive introduced security requirements for continuity of service and incident notification for OES. However, there is insufficient harmonization with regards to sectoral requirements and fragmentation in Member State implementation (e.g. incident reporting). This was also identified in the European Commission Digital Finance Package. This results in increased complexity for financial services firms with cross-border activity, leading to inefficiencies, which in turn increase cyber resilience risks.
2	AFME to respond	• What is the impact of imposing security requirements on DSPs by the NIS Directive in terms of cyber resilience? Don't know / no opinion
		• Currently it is not clear if imposing security requirements for DPS, as the ones imposed to OED under the NIS Directive, would help improve cyber resilience in the EU. This is because of the fragmentation and insufficient harmonisation which could lead to further complexity in implementation. • However, if a common standard for cybersecurity could be developed and implemented consistently across firms, AFME believes there would be benefits in more firms adhering to a similar cyber resiliency standard.
3	AFME to respond	• Member States have established effective security requirements for OES on a national level: Don't know • There is a sufficient degree of alignment of security requirements for OES and DSPs in all MS: Disagree
		• Currently there is insufficient harmonization, with regards to sectoral requirements, and fragmentation, with regards to Member States implementation, for the NIS Directive. • For financial services, some Member States have implemented the NIS Directive by introducing prescriptive and detailed requirements for segregation of network for essential information systems. While these requirements are inconsistent with how other Member States have implemented the Directive, introducing fragmentation in the Single Market, they also deviated from a principles and risk based approach to cyber security requirements.
4	AFME to respond	• Prescriptive requirements make it easy for companies to be compliant: Strongly disagree • Prescriptive requirements leave too little flexibility to companies: Strongly agree • Prescriptive requirements ensure a higher level of cybersecurity than general risk management obligations: Strongly disagree • Prescriptive requirements make it difficult to take into account technological progress, new approaches to doing cybersecurity and other developments: Strongly agree

		• The different level of prescriptiveness of requirements increases a regulatory burden for companies operating across different national markets: Strongly agree • The companies should have the possibility to use certification to demonstrate compliance with the NIS security requirements: Don't know • The companies should be required to use certification for their compliance with NIS security requirements: Disagree
		• In line with global standardisation, technology neutrality and principles-based legislation provide the flexibility needed for firms to implement appropriate control, in a risk based and proportionate manner, that meet the continuously evolving nature of cyber risks and technology. Firms of different size and complexity may present different risks, and therefore implement different controls, while mitigating risks and demonstrating similar outcomes. AFME believes that the introduction of prescriptive and detailed legislative requirements are at risk of becoming obsolete in the short to medium term, as cyber threats and innovation in technology continues at pace. • Certifications can be useful to promote standards and drive more trust. However, the activity of creating, issuing, monitoring (e.g. auditing) and maintaining a certification can be complex and burdensome, in particular for ICT products, which require a principle and risk-based approach due to the complex and evolving nature of cyber threats. In addition, while certifications coming out of the EU may help reduce barriers within the EU, it may introduce additional barriers with regards to other jurisdictions, which could be burdensome for firms operating cross-border. In this case this will lead to additional complexities, increasing operational and compliance costs for those firms.
2.f. Incident notification		
1	AFME to respond	• The majority of companies have developed a good understanding of what constitutes an incident that has to be reported under the NIS Directive: Disagree • Member States have imposed notification requirements obliging companies to report all significant incidents: Disagree • Different reporting thresholds and deadlines across the EU create unnecessary compliance burden for OES: Strongly disagree • The current approach ensures that OES across the Union face sufficiently similar incident notification requirements: Strongly disagree

		• Financial services firms with operations and customers in the EU are subject to mandatory regulatory cyber incident reporting requirements:
		  o NIS Directive: major incident reporting for operators of essential services
		  o GDPR: data breach notification
		  o eIDAS: incident reporting for trusted services providers
		  o PSD2: incident reporting for payment service providers
		  o ECB SSM: incident reporting for significant institutions
		  o Target 2: incident reporting for critical participants
		• This means that a single incident could trigger firms having to report to different authorities, complying with the applicable impact assessment details and thresholds, timeline, data set, and communication means. In addition to applicable EU regulatory requirements firms could be subject to National Competent Authority reporting requirements in Members States where they have operations. Multinational financial firms will also have further applicable incident reporting and data protection requirements outside of the EU.

		• Incident reporting obligations under the NIS Directive add to the fragmented EU cyber incident reporting framework. AFME is supportive of the Commission's proposal under the Digital Finance Package, to harmonise incident reporting requirements across the EU (e.g. reporting content and template) and the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. However, while this is a positive step, we believe that the industry should be actively involved in the harmonisation process, providing feedback and supporting the development of appropriate requirements, that can be implemented in line with internal controls and with proportionality in mind. • Financial firms naturally link their cyber incident response and recovery to the overall business. Cybersecurity is a key resource leveraged as part of the enterprise incident response to both inform and react to enterprise events. Within the financial services industry there is a criticality and importance placed on incident response capabilities that support the restoration and recovery of the business; Cyber incident response is a major component to that process. If a business application is affected by a cyber incident, the response teams will make it a top priority to do several things: 1) properly communicate to all affected and involved parties; 2) recover such that the scenario. Financial firms typically maintain a dedicated cybersecurity program responsible for protecting the firmwide cyber incident response framework that outlines the processes.
2.g. Level of discretion on transposition and implementation given to Member States		
1	AFME to respond	• The approach leads to significant differences in the application of the Directive and has a strong negative impact on the level playing field for companies in the internal market: Agree • The approach increases costs for OES operating in more than one Member State: Agree • The approach allows Member States to take into account national specificities: Don't know
		• One of the key differences in the local transposition of NIS Directive across EU Member States regards the identification criteria for OES. The definitions and thresholds are often different from one EU country to another. Additionally, the measures imposed by Members State on OES, have different scope and requirements. This fragmentation and lack of consistency increases complexity and cost in the Single Market, in particular for those firms operating cross-border. • Further, the differences scope and responsibility of Member State National Agencies, coupled with sector specific versus cross-sectoral requirements, adds further complexity in assessing applicable regulatory requirements. This is particularly valid for the financial sector.
2.h. Enforcement		
1	AFME to <u>not</u> respond	• Member States are effectively enforcing the compliance of OES: Don't know • Member States are effectively enforcing the compliance of DSPs: Don't know • The types and levels of penalties set by Member States are effective, proportionate and dissuasive: Don't know • There is a sufficient degree of alignment of penalty levels between the different Member States: Don't know
2.i. Information exchange		
1	AFME to <u>not</u> respond	• The Cooperation Group has been of significant help for the Member States to implement the NIS Directive: Don't know

		• The Cooperation Group has played an important role in aligning national transposition measures: Don't know • The Cooperation Group has been instrumental in dealing with general cybersecurity matters: Don't know • The Cooperation Group is dealing with cross-border dependencies in an effective manner: Don't know • The CSIRTs network has effectively managed to fulfil its tasks as laid down in the NIS Directive: Don't know • The CSIRTs network has helped to build confidence and trust amongst its members: Don't know • The CSIRTs network has achieved swift and effective operational cooperation: Don't know • The Cooperation Group and the CSIRTs network cooperate effectively: Don't know
2	AFME to <u>not</u> respond	• Don't know / no opinion
3	AFME to not respond	• Don't know / no opinion
2.j. Efficiency of the NIS Directive		
1	AFME to <u>not</u> respond	• Don't know / no opinion
2	AFME to <u>not</u> respond	• Don't know / no opinion
		• AFME welcomes the Commission's efforts in establishing a common baseline for cybersecurity requirements across the EU. This can support the standardisation of cybersecurity requirements across the EU and support the increase of capabilities in Member States or sectors, where cybersecurity has not been priority. • However, challenges due to fragmentation (e.g. with sectoral requirements) and a lack of harmonisation (e.g. with regards to Member State transposition), introduces complexity and inefficiencies across the EU. • While EU harmonisation is key to reduce fragmentation in the Single Market, AFME recommends the Commission maintain consistency of any legislative proposals to ongoing discussions on at the Basel Committee for Banking Supervision (BCBS), the Financial Stability Board and the G7, to ensure alignment with global efforts.
2.k. Coherence of the NIS Directive with other EU legal instruments		
1	AFME to respond	• Don't know / no opinion
		• AFME is supportive of the European Commission measures announced as part of its Digital Finance Package. In particular, regarding ICT and cybersecurity requirements, the Commission recognises the need for increased harmonisation and removing fragmentation in the Single Market. • To support this effort, it would be beneficial for financial services firms, to understand how the NIS Directive is complementary to other measures announced by the European Commission under the Digital Finance Package. • In addition, AFME welcomes further clarity on how the NIS Directive is complementary or overlaps with other EU sectoral requirements, whether pan-European (e.g. EBA ICT GLs, EBA Outsourcing GLs, ECB CROE) or National.

3. Approaches to cybersecurity in the European context currently not addressed by the NIS Directive

- ***Feedback on proposed legislative changes***

Question	Comment	Reasoning
3.a. Provision of cybersecurity information		
1	AFME to respond	• AFME welcomes tools and mechanisms to facilitate information sharing across the financial sector. Theses forums enable firms to prepare, respond and recover from incidents, based on voluntary sharing of non-sensitive or confidential data, between trusted parties. • AFME cautions the European Commission in creating additional mandatory requirements for information sharing, which may impact the trusted networks that currently exist. Rather, the Commission could build awareness to a broader set of firms, across the EU, to use the current existing mechanisms and tools available for information sharing. • In particular, AFME is supportive of the European Commission measures announced as part of its Digital Finance Package, to remove potential barriers to information sharing, incentivising firms to leverage and use current mechanisms in place. • Additionally, AFME believes firms would benefit from dual information sharing with authorities, who are in a position to aggregate and anonymise reported information, potentially identifying threats to the sector.
2	AFME to respond	• Under the NIS Directive, Member States shall require companies to report events having an actual adverse effect on the security of network and information systems (incidents). Should the reporting obligations be broadened to include other types of information in order to improve the situational awareness of competent authorities? No
		• Given the existing challenges with the Directive, due to fragmentation (with sectoral requirements) and lack of harmonisation (with regards to Member State transposition), introducing further requirements could introduce additional complexity and inefficiency in the Single Market.
3	AFME to respond	• Financial services firms with operations and customers in the EU are subject to mandatory regulatory cyber incident reporting requirements: o NIS Directive: major incident reporting for operators of essential services o GDPR: data breach notification o eIDAS: incident reporting for trusted services providers o PSD2: incident reporting for payment service providers o ECB SSM: incident reporting for significant institutions o Target 2: incident reporting for critical participants • Incident reporting obligations under the NIS Directive add to the fragmented EU cyber incident reporting framework. This is why AFME is supportive of the Commission's proposal under the Digital Finance Package, to harmonise incident reporting requirements across the EU (e.g. reporting content and template) and the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. • This could form the basis to support dual information sharing between firms and with authorities, who would be in a position to aggregate and anonymise reported information, and identifying threats (e.g. threat intelligence briefings, sectoral threat landscape, cross-sectoral risks/impacts) to the sector and the EU. • However, while EU harmonisation is key to reduce fragmentation in the Single Market, AFME recommends the Commission maintain consistency of any legislative proposals to ongoing discussions on at the Basel Committee for Banking Supervision (BCBS), the Financial Stability Board and the G7, to ensure alignment with global incident reporting and response efforts.

3.b. Information exchange between companies		
1	AFME to not respond	• Electricity: Don't know • Oil: Don't know • Gas: Don't know • Air transport: Don't know • Rail transport: Don't know • Water transport: Don't know • Road transport: Don't know • Banking: Don't know • Financial market infrastructures: Don't know • Health sector: Don't know • Drinking water supply and distribution: Don't know • Digital infrastructure: Don't know • Digital service providers (online marketplaces): Don't know • Digital service providers (online search engines): Don't know • Digital service providers (cloud computing services): Don't know
2	AFME to not respond	• Don't know
3	AFME to respond	• AFME welcomes tools and mechanisms to facilitate information sharing across the financial sector. Theses forums enable firms to prepare, respond and recover from incidents, based on voluntary sharing of non-sensitive or confidential data, between trusted parties. • AFME cautions the European Commission in creating additional mandatory requirements, geared towards information sharing, which may limit the qualitative input of these trusted networks. Rather, the Commission could build awareness to a broader set of firms, across the EU, to use the current existing mechanisms and tools available for information sharing. • In particular, AFME is supportive of the European Commission measures announced as part of its Digital Finance Package, to remove potential barriers to information sharing, incentivising firms to leverage and use current mechanisms in place.
3.c. Vulnerability discovery and coordinated vulnerability disclosure		
1	AFME to not respond	• Don't know / no opinion
2	AFME to not respond	• Not applicable
3	AFME to not respond	• N/A
4	AFME to not respond	• Don't know / no opinion
3.d. Security of connected products		
1	AFME to not respond	• Don't know / no opinion
3.e. Measures to support small and medium-sized enterprises and raise awareness		
1	AFME to respond	• Such measures have proven to be effective in increasing the level of awareness and protection amongst SMEs: Don't know • European legislation should require Member States to put in place frameworks to raise awareness amongst SMEs and support them: Don't know
		• AFME is supportive of efforts than can increase the level of cyber resilience for small and medium sized companies, that may improve the overall level of cyber resilience.

		• As such, AFME is supportive of efforts by the Word Economic Forum (WEF) to support Fintech cyber resilience. However, while large firms face significant challenges with cybersecurity fragmentation so to do smaller firms, which may face resource limitations. • To further promote consistency across the sector and reduce regulatory fragmentation, financial institutions from various jurisdictions along with other industry associations developed in 2018, the Cyber Risk Institute's (CRI) Cybersecurity Profile ("Profile"). • The CRI Profile is a globally recognised, scalable and extensible assessment tool that financial institutions of all types can use for internal and external (i.e., third-party) cyber risk management and as a mechanism to evidence compliance with various regulatory frameworks, globally. The Profile leverages existing international and regional standards to globally align cybersecurity laws, rules, guidance and assessment frameworks . • The CRI Profile has since been adopted by over 200 financial institutions of differing sizes and maturity levels. Based on the development and wide use of the Profile, the industry believes its existing CIRR processes and controls are well-developed and are designed to continue to mature as markets evolve.

Contacts

AFME	Andrew Harvey	+44(0)20 3828 2694	aharvey@gfma.org
AFME	David Ostojitsch	+44 (0)20 3828 2761	david.ostojitsch@afme.eu
AFME	Emmanuel Le Marois	+44 (0)20 3828 2761	emmanuel.lemarois@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. AFME represent the leading global and European banks and other significant capital market players. AFME advocates for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. AFME aims to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work. For more information, visit https://www.afme.eu/