afme/
Finance for Europe

Digital Finance in the EU

Priorities for fostering resilient, innovative, and competitive financial markets

August 2024

Association for Financial Markets in Europe
www.afme.eu

Disclaimer

AFME's *Digital Finance in the EU: Priorities for fostering resilient, innovative, and competitive financial markets* (the "Report") is intended for general information only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business or other professional advice. AFME doesn't represent or warrant that the Report is accurate, suitable or complete and none of AFME, or its respective employees shall have any liability arising from, or relating to, the use of this Report or its contents.

Your receipt of this document is subject to paragraphs 3, 4, 5, 9, 10, 11 and 13 of the Terms of Use which are applicable to AFME's website (available at http://www.afme.eu/en/about-us/terms-conditions) and, for the purposes of such Terms of Use, this document shall be considered a "Material" (regardless of whether you have received or accessed it via AFME's website or otherwise).

July 2024

Contacts

Stefano Mazzocchi
Managing Director
Advocacy
Stefano.Mazzocchi@afme.eu

Marcus Corry
Director
Technology & Operations
Marcus.Corry@afme.eu

Amandeep Luther
Associate Director
Technology & Operations
Amandeep.Luther@afme.eu

Coen ter Wal
Director
Technology & Operations
Coen.terWal@afme.eu

Coco Chen
Associate Director
Technology & Operations
Coco.Chen@afme.eu

Raouiya Lebbakh
Researcher
Technology & Operations
Raouiya.Lebbakh@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of Europe's wholesale financial markets.

AFME works to promote a robust, connected and competitive financial system in the EU, UK and globally. providing expertise across a broad range of regulatory and capital markets issues. We represent the leading global and European banks and other significant capital market players. AFME's members are the lead underwriters of 89% of European corporate and sovereign debt.

AFME advocates for deep and liquid secondary market, pursues changes that enable the European green and digital transformations, supports the completion of the Banking Union and Capital Markets Union and connectivity of EU and UK financial markets with the rest of the world.

Contents

Executive summary 2

Introduction 4

Chapter 1 – Digital Assets 6

1.1 Unlocking the benefits of tokenisation in capital markets 6

1.2 Effective implementation of MiCA 15

Chapter 2 – Data sharing and open finance 18

2.1 FiDA scope 18

2.2 Regulation and Supervision of Financial Information Service Providers 19

2.3 Proportionate implementation 19

2.4 Compensation 20

Chapter 3 – Cybersecurity and ICT resilience 21

3.1 DORA implementation 21

3.2 The need to avoid localisation requirements in the cloud certification schemes 22

Chapter 4 – Artificial intelligence 24

4.1 Implementation of the AI Act 26

Executive summary

UNLOCKING THE BENEFITS OF TOKENISATION IN CAPITAL MARKETS

The development of Distributed Ledger Technology ("DLT") holds promise for unlocking efficiencies and driving growth. Experiments have allowed a greater understanding of the technology and provided evidence of the benefits. Payments, settlement, and securities lifecycle events may be carried out with greater safety and more efficiency; access to capital markets, through tokenised securities / assets, may be expanded to a broader set of participants. At scale, these developments would benefit the real economy.

Adoption of DLT has been growing, but the pace could be higher. The challenges are largely linked to the need for the broad ecosystem to move in the same direction, so that larger scale use of DLT – necessary for reaping its benefits – can be achieved. A turning point is seen as being within reach but to catalyse this evolution all stakeholders need to play a role. Stronger momentum can be achieved by prioritizing the following actions:

- Large issuers, particularly public-sector issuers of debt instruments in Europe - sovereign, supranational and agency issuers – can play a key role in this process of scaling DLT-based capital markets through increasingly deploying DLT solutions in their issuances.
- Policymakers can facilitate the above objective by working towards a harmonised, technology-neutral, risk-focused regulatory framework. Possible regulatory enablers or blockers should be identified and action taken accordingly..

SUPPORTING A MORE EFFECTIVE DATA ECOSYSTEM

The EU's proposed Financial Data Access (FiDA) framework, if designed correctly, has the potential to enhance the way banks operate, encourage innovation (including across sectors, if some provisions are met) and support a more effective and efficient data ecosystem. We have identified the following key principles to support the development of a robust Open Finance Framework. These are:

- A clearer definition of the scope of FiDA: "customer data" should only include raw data; "customers" covered should exclude wholesale and corporate clients given the bespoke nature of the services they receive.
- A level playing field is crucial: – A genuine data ecosystem needs to cover multiple sectors. Consistent and appropriate regulatory oversight should apply to all potential data users.
- An appropriate framework for compensation, to ensure fair allocation of costs across the data value chain and to safeguard fair competition.
- Implementation should follow a step-by-step approach based on three main phases: assessment of FiDA readiness by data category; definition by policymakers and market stakeholders of the key elements of the data sharing scheme; implementation / operationalisation of the data sharing arrangements.
- Clear liability provisions, to provide legal clarity with respect to the access, processing, sharing, and storage of data.

PROMOTING A SECURE AND RESILIENT EU DIGITAL FINANCIAL SECTOR

Work on the implementation of the Digital Operational Resilience Act (DORA) will be central in the coming months and will lay the foundation for a harmonised, secure and resilient EU digital financial sector. We emphasise the following priorities:

- Explore mechanisms for developing best practice industry guidance on operational and cyber incidents. leveraging on the intelligence EU authorities will collate through incident reporting.
- Ensure a coherent framework, particularly for a heavily regulated sector like financial services, where the risk of overlaps and inconsistencies between horizontal and vertical regulatory frameworks is high.
- Reject efforts to introduce sovereignty/localisation requirements into EU frameworks.

LEVERAGING THE OPPORTUNITIES FROM THE USE OF ARTIFICIAL INTELLIGENCE

AI has the potential to transform financial services and capital markets to make them safer, more efficient, accessible, and better tailored to consumer needs. This, in turn, brings important benefits to consumers and the wider global economy. At the same time these opportunities require careful consideration of new risks and challenges introduced by a growing use of AI.

BUILDING A DIGITAL CAPITAL MARKETS UNION

Digitalisation and new technologies have the potential to support the development of capital markets and the objectives of the Capital Markets Union (CMU). By increasing efficiency, lowering costs, boosting transparency and availability of information, allowing greater access to data, digital technologies can support the CMU project, the removal of market barriers and the increased cross-border provision of services and, ultimately, allow greater access to capital markets both for entrepreneurs and institutions looking for funding and for investors. (See Box on page 17)

“Digitalisation and new technologies have the potential to support the development of capital markets and the objectives of the Capital Markets Union”

Introduction

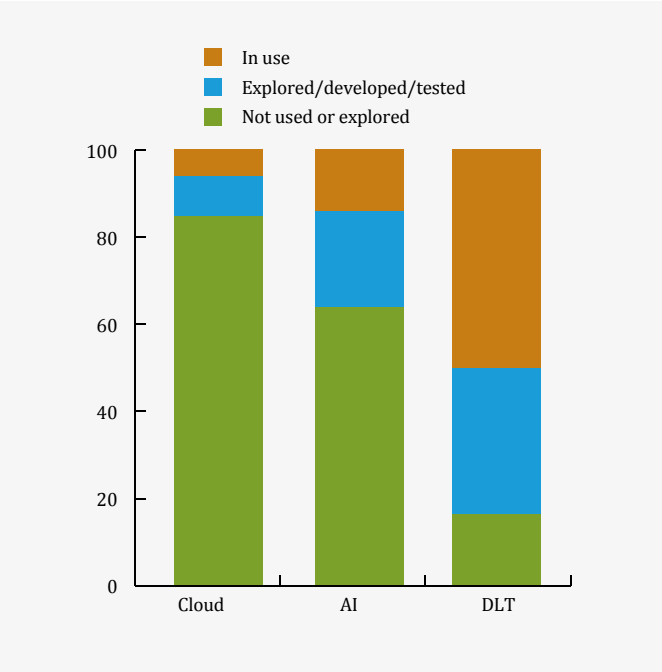
Banks have been at the centre of a profound digital transformation, a process which will continue and accelerate in the coming years. While technological innovation and digitalisation are having a profound impact on the entire economic system, the financial sector has been at the forefront of this transformation. For banks, the need to offer their customers innovative and better products, more efficiency and increased access to financial services, is a competitive imperative.

As a result, leading banks have invested increasingly in technological innovations like cloud, big data, DLT and artificial intelligence.

This fundamental transformation has required not only the mobilisation of massive economic resources, but also an extensive effort from policymakers to rethink the regulatory framework.

With its Digital Finance Strategy, the EU has been an early mover in this area, with the objective, on the one hand to facilitate digital innovation, and on the other hand to address the related challenges and risks and to foster the digital operational resilience of the financial sector.

Figure 1: **Adoption rate of new technologies by banks (as of Q3 2022) (source: ECB)**



Important milestones have been achieved over the past legislative cycle, in particular with the adoption of the Digital Operational Resilience Act (DORA), the Markets in Crypto Assets Act (MiCA) and the DLT Pilot Regime. Important work is under way on the possible introduction of a digital Euro as an additional retail payment option as well as for the creation of links between the Eurosystem's TARGET services and DLT infrastructures. The recent proposal on Financial Data Access (FiDA) is also exploring the possible opportunities of broader data sharing in the financial sector. Beyond the financial sector, the EU has adopted horizontal initiatives like the Artificial Intelligence Act, the Data Act, and the Digital Services package. These actions have been important in promoting greater legal certainty for market participants and in avoiding fragmentation that would have resulted from diverging, and potentially conflicting, local requirements.

A new phase is now starting, during which:

- Significant resources will be needed to ensure the successful **implementation** of the already agreed legislative acts. Regulators will need to finalise the implementing measures, and all stakeholders – both in the official and private sectors - will need to build up their capacity to apply the new rules.

- The **legislative framework** for digital finance will continue to evolve and develop, with the finalisation of the legislative proposals already on the table, the potential review of adopted proposals, or potentially new legislative actions. EU's first mover role in regulating digital finance has required striking a difficult balance between facilitating innovation, understanding impacts on competition and users, and preserving financial stability. Given the pace of innovation we have witnessed in recent years, these future legislative developments provide the opportunity to reassess whether this balance continues to be achieved.

- Beyond the legislative and implementation work, the **broader policy strategy** will need to be designed to encourage the entire financial ecosystem to work towards the adoption of those new technologies that can benefit the economy. The official sector, as provider of key infrastructures and as key player in financial markets, can have a crucial role in promoting the adoption at scale of more efficient technologies and can act as a catalyst for change. Financial institutions can also facilitate change, by promoting standardisation, producing fact based assessments of opportunities and risks and fostering education of key stakeholders.

GUIDING PRINCIPLES FOR THE NEW POLICY CYCLE

- **Competitiveness** – The ability of banks in Europe to provide their clients with financial services through innovative technologies represents a competitive edge for European businesses, which can benefit from increased access to finance, increased choice and lower costs. Access to cutting edge technology will be necessary for European banks and for their clients to compete on the global stage.

- **Financial stability and safety** – Market participants need to operate within a set of rules that appropriately protect all stakeholders and meet the regulatory outcomes set by policymakers. Growth and innovation need to align with the objectives of ensuring safety and soundness, market integrity, consumer protection and overall financial stability. Also, all market participants need to be subject to the highest standards in terms of cybersecurity, operational resilience, protection of data.

- **Level playing field** – Innovation is leading to a growing range of products and players, with potential benefits in terms of competition and innovation, access to finance and inclusion. In this context, it is important to preserve the principle 'same services, same risks, same rules', regardless of the business model through which financial services are provided. New entrants, like FinTech and big tech, can increase competition but their competitiveness should not be the result of lighter regulatory requirements and lower safety standards and compliance costs.

- **Technological neutrality** – The disruptive nature of innovation might push market regulators to adopt a very conservative stance towards new technologies. While caution is justified, particularly while the impacts originated by innovation are being analysed and understood, regulatory approaches should carefully avoid stifling innovation by imposing penalising requirements. We therefore recommend that regulators take a technology neutral as well as principles- and risk based approach.

- **EU Integration** – Innovations in digital finance have the potential to foster EU integration by helping remove or reduce some of the existing barriers which create fragmentation in the single market, in line with the Capital Market Union's objectives. This can be true in many parts of the lifecycle of securities and of the payment system (areas where DLT and a wholesale digital € can play an important role). Moreover, to the extent that technology (for instance, tokenisation) will reduce the cost for accessing capital markets for SMEs, this will promote the development of deeper and more efficient capital markets. The industry can also play a role in reducing fragmentation with initiatives aimed at promoting greater standardisation, interoperability and identification of good market practices.

- **Coherence between horizontal and vertical rules** – The regulatory framework for digital finance has been developing in two dimensions: vertically, with financial sector specific rules; horizontally, with frameworks affecting market participants across sectors. This rapid development creates the challenge of ensuring that the intersections between the various initiatives promote a coherent framework. Experiences in recent months (e.g. DORA interactions with: Cyber Resilience Act; cloud certification scheme) have shown that this can be a challenging objective to achieve.

- **Global perspective and international coordination** – Innovation creates opportunities, and challenges, which are global in nature. Global coordination – leading to regulatory approaches to digital finance which allow consistency and interoperability of regulatory frameworks - is necessary to avoid fragmentation along regional boundaries and to allow market participants to choose among a broad range of technology providers and access cutting edge technology.

- **Achieving sovereignty by promoting innovation and resilience** – Economic sovereignty is a legitimate objective which, however, cannot be served by requirements that result in making EU actors more vulnerable to attacks and less able to compete. Localisation requirements – by reducing choice and increasing costs for accessing technologies – go against the objective of promoting innovation and resilience.

- **Assessment of impacts and cooperation with market stakeholders** – Legislative initiatives and implementation work should be guided by solid impact assessments, in line with the better regulation principles. This is particularly difficult for innovative technologies, for which their reach, impacts and use cases are difficult to predict and solid data not available. In these situations, policymakers should promote market led groups and solutions, to ensure that impacts are understood and that investments are encouraged in those areas where clear use cases and benefits for end users are most evident in light of the engagement with key market actors. This would also enable policymakers to discuss and identify realistic implementation timelines with such stakeholders.

Chapter 1 – Digital Assets

The application of Distributed Ledger Technology ("DLT") has been a very significant development in financial markets. **DLT holds promise for unlocking efficiencies**, which – once applied at scale - would trigger transformational impacts on capital markets **to the benefit of the real economy**. For financial services, it could generate substantial efficiencies across the securities lifecycle, improve the resiliency of market infrastructure, reduce settlement risk and ultimately change the way market participants interact with one another.

At the same time, **it is crucial that these developments take place in a safe environment** where innovation is accompanied by strong safeguards in terms of safety, soundness, market integrity, consumer protection and financial stability. These are preconditions for developing a digital assets ecosystem built on trust, a key component of effective and robust financial markets. With solid regulatory oversight, banks can play a role in ensuring that digital assets develop under strict and tested risk management practices.

Market participants have been experimenting the use of DLT for years. Several jurisdictions have developed sandboxes or pilot regimes to facilitate these experiments and the EU DLT Pilot Regime has represented an important first step in this direction. At the same time, **several use cases are already well developed beyond the experimentation phase** (for instance repo settlement or collateral management) and have achieved significant scale and realised benefits for clients.

The move from experimentation to adoption at larger scale is continuing to progress. At the same time, further scaling DLT-based capital markets and fully reaping its benefits requires addressing a number of challenges. The main challenge is the need for the entire capital markets' ecosystem to move in the same direction. This requires developing a mature understanding of the opportunities, as well as of the ways to manage possible risks and to remove any unnecessary blockers (including inconsistent or technology-biased regulations) to the adoption of DLT at scale. On the one hand, European policymakers, in their roles both as regulators and as market participants, can have a central role in acting as a catalyst for innovation. Market participants, on the other hand, need to continue developing their capacity and contribute to an environment that facilitates innovation (e.g. trough efforts aimed at promoting standards and interoperability).

AFME considers the following to be the main priority areas for the next few years:

- **Unlocking the benefits of tokenisation by enabling the use of DLT at scale** - AFME[1] members are particularly interested in unlocking the benefits of DLT in the more 'traditional'[2] parts of capital markets.
- **Prioritising the effective implementation of MiCA** - At the same time, in the coming months MiCA will bring regulatory certainty, reduce fragmentation and underpin the development of a robust and well-functioning market for crypto assets.
- **Assessing the appropriate regulatory framework for "decentralised activities" (DeFi)** to ensure that a proportionate regulation is applied**.**

1.1 Unlocking the benefits of tokenisation in capital markets

The development of Distributed Ledger Technology ("DLT") holds promise for unlocking efficiencies and driving growth. Payments, settlement, and securities lifecycle events may be carried out with greater safety and more efficiency; access to capital markets, through tokenised securities / assets, may be expanded to a broader set of participants; and markets / infrastructures may operate more effectively with improved liquidity. At scale, these developments would benefit the real economy.

1 The Global Financial Markets Association (GFMA), of which AFME is part, has last year published a report on "The Impact of Distributed Ledger Technology in Global Capital Markets", where the opportunities linked to DLT, and related challenges, are explored in detail. GFMA has subsequently contributed to the definition of an approach for the classification and understanding of digital assets (digital assets taxonomy) promoted by the US CFTC.

2 As opposed to the crypto assets and services in the scope of MiCA.

Regulatory policy should seek to create the same stability and protections in digital asset markets that exist in traditional, regulated financial markets, whilst allowing and supporting innovation. Regulated financial institutions, given their track record, from dematerialization, digitization, to off-premises cloud computing, of adopting new technology and implementing appropriate governance, controls and processes to adequately manage risks, should be allowed to promote responsible innovation and best practices to set controls based on the size, scope, and complexity of a given use case.

There is growing momentum in developing DLT use cases, and adoption of DLT-based securities is reaching a turning point. DLT-based issuances have been largely experimental, and liquidity in primary and secondary markets can improve significantly once barriers to adoption are addressed. The establishment of a broader DLT-based ecosystem will require regulators to provide, in the EU and globally, an aligned and coordinated framework to allow market participants to develop an adequate understanding of the rules and the operational capabilities required to plan, research, and launch larger-scale initiatives.

DLT is a framework and protocol that combines database technology and cryptography, allowing multiple participants to each maintain their own copy of records in a shared dataset and make updates to it. All copies remain consistent through computerised consensus mechanisms rather than through a trusted third party.

What do we mean by tokenisation in capital markets?

In the context of this paper, "tokenisation" can be defined as the digital representation of regulated financial instruments and money on a distributed ledger, reflecting an ownership right of the underlying asset, and its transfer between entities intermediated using the ledger. We also imply that DLT technology is the enabling underlying technology. Therefore **our focus is on the DLT-based forms of traditional securities** like equities, fixed income instruments and derivatives (these assets would meet the classification conditions as 'Group 1a' cryptoassets set by the Basel Committee in their recent standard on the prudential treatment of cryptoassets exposures).

These DLT-based securities can exist on a distributed ledger in two formats: 1. "Tokenized Securities", which are issued and custodied traditionally, but also converted onto a distributed ledger through a digital twin token that represents the underlying traditional security; and 2. "Security Tokens", which are issued and custodied natively on a distributed ledger only, and therefore do not have a traditional security as an underlying basis.

It is important to stress that DLT-based securities as defined above (as well as DLT-based payment instruments like tokenised bank deposit or DLT based central bank digital currencies – CBDCs) are crucially different from other digital assets which use the blockchain technology, such as cryptocurrencies (like bitcoin or ether).

Developing and scaling up use cases will require market participants to work together to build consensus on common standards, aligned and compatible technology architecture designs leading to greater interoperability of infrastructures and solutions.

Policymakers can facilitate the above objective by working towards a harmonised, technology-neutral, risk-focused global regulatory framework, which promotes the development of a transparent, and effective digital ecosystem.

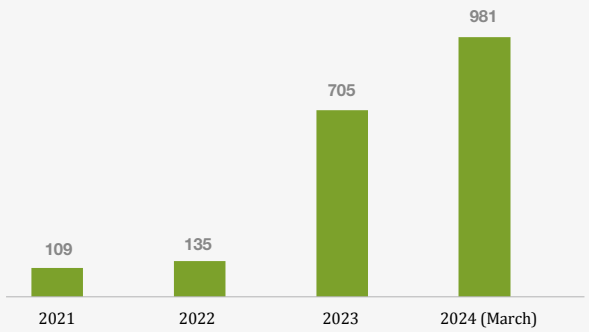
In May 2023 GFMA published a report highlighting and quantifying the potential transformative benefits of DLT for capital markets.

Many experiments have been undertaken (including the important EIB issuances of digital bonds, summarised in the graph below) and some use cases have reached a mature stage (e.g. J.P. Morgan's Digital Financing Application, running on the Onyx Digital Assets DLT platform built on a private-permissioned DLT network, enables true DvP settlement for repurchase agreements; HQLAx's Books and Records Digital Collateral Registry is a platform built on a private-permissioned DLT network which records the ownership transfers of ansecurities). As highlighted in Figures 3 and 4 below, issuance has been growing constantly in recent years. However, despite these important experiences, overall tokenisation of financial instruments has so far remained relatively limited While experimentation is a necessary intermediate stage in this evolution, there is a danger that siloed approaches, as well as diverging regulatory regimes, could undermine progress towards the tangible, coordinated outcomes required to establish a broader DLT-based ecosystem.

Figure 2: **Primary market issuances: development has been fostered by a small number of issuers, including EIB and the HK government**

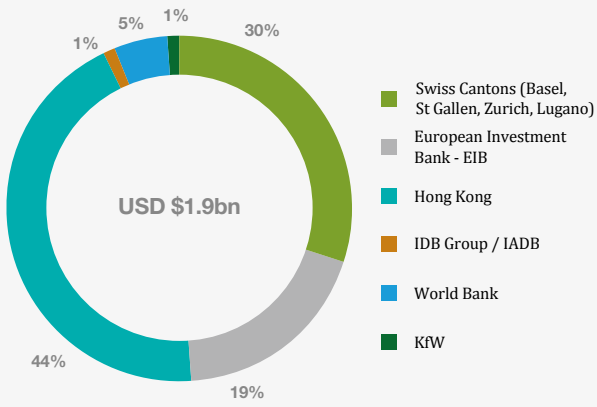
	EIB-Mercury	EIB-Venus	EIB-Mars	HK-Evergreen 1	EIB-Saturn	HK-Evergreen 2
Date	**Apr-21**	**Nov-22**	**Jan-23**	**Feb-23**	**Jun-23**	**Feb-24**
DLT network	Public Permissionless	Private Permissioned	Private Permissioned + Public Permissioned	Private Permissioned	Semi Permissioned	Private Permissioned
Currencies	EUR	EUR	GBP	HKD	SEK	HKD, CNH, EUR, USD
Total deal size (USD equiv.)	107m	107m	63m	100m	95m	750m
Number of external investors	Less than 5	Less than 5	Less than 5	Less than 5	Less than 5	More than 50
Governing law	France	Luxembourg	Luxembourg	Hong Kong	Luxembourg	HK
Digitally native or tokenised?	Digitally native	Digitally native	Digitally native	Tokenised	Digitally native	Digitally native
Access vja CSD accounts?	No	No	No	No	No	Yes
Platform	Societe Generale	Goldman Sachs	HSBC	Goldman Sachs	Crédit Agricole	HSBC
Other syndicate members	Santander Goldman Sachs	Santander Societe Generale	BNP Paribas RBC	HSBC Bank of China Crédit Agricole ICBC	SEB	Bank of China ICBC Crédit Agricole Goldman Sachs UBS

Figure 3: **Global issuance of Digital Sovereign and SSA bonds since 2021 (USD mn)**



Source: AFME Research

Figure 4: **Global Issuance of DLT-Based SSA bonds by issuer since 2021 (% of the total)**



Source: AFME Research

To identify and remove the possible blockers toward the scaling of tokenisation in capital markets, the following areas would require careful consideration:

- **Regulatory challenges:** Current laws and regulations applied to DLT assets are often based on those developed for traditional assets. This could create, sometimes inadvertently, *de facto* prohibitions or contradictory requirements. Considering adaptations to existing legal and regulatory structures is fundamental in promoting the development of transparent, disciplined, risk-focused, and effective market infrastructure. In the EU, after the implementation of its Digital Finance strategy, it is important that work under the next Commission identifies opportunities to improve the regulatory framework and areas where unnecessary impediments to innovation may exist. Examples include:

  - **Enable decentralised and distributed settlement:** Under the Central Securities Depository Regulation (CSDR) admission to trading and eligibility for inclusion in the Eurosystem's collateral framework require that the instrument is registered in an eligible CSD. Overall, CSDR is built on the assumption that different functions (registration of securities, maintenance of securities, settlement) are performed within a single centralised CSD while DLT could allow or require the separation of these activities. This decentralisation can also reduce concentration and single-point-of-failure risks, promote different business models and increase choice for market participants. By allowing DLT-based platforms to become eligible Securities Settlement Systems (SSS) would allow securities issued through them to: become eligible for admission to listing and trading on trading venues; become eligible for use in financial collateral arrangements; qualify as eligible marketable assets as monetary policy collateral under the current ECB eligibility collateral criteria; benefit from settlement finality. All these changes would significantly enhance the attractiveness of DLT-based capital markets.

  - **DLT Pilot Regime:** The EU has been bold with the EU DLT Pilot Regime initiative – which went live in March 2023 - putting in place measures faster than other regions to facilitate experimentation with DLT in trade and post-trade processes. This can represent a first-mover advantage, generating valuable knowledge and first-hand experience of how DLT can be applied in securities markets. However, the evolution of DLT-based markets has to some extent overtaken this pioneering framework and aspects of the EU DLT Pilot Regime may not encourage broad engagement in the sandbox from market participants. This could be linked to a number of design choices, including the relatively low thresholds on both the size of permitted issuances of DLT-based securities and the market capitalisation of the issuer. We therefore recommend that the thresholds are increased significantly. Also, participants might be disincentivised from investing time and money in new and innovative projects with an uncertain future: the temporary nature of the framework could represent an important hurdle for those who might need clarity on the end-state regime before investing in DLT solutions. Additionally, the requirement to set up a separate legal entity and the need for a full CSD license to run a DLT Securities Settlement System significantly limits the range of market participants able to leverage the pilot regime. These limitations could stifle the efforts to move from experimentation to application at scale. We therefore recommend the removal of the requirement to set up a separate entity and allow for authorisation for individual CSD services (see also previous bullet).

  - **Settlement Finality Directive (SFD):** The concept of settlement finality - the exact moment in time when proprietary interests pass from one party to its counterparty, and the obligations of the parties to a transaction are discharged in an unconditional and irrevocable manner - sits at the heart of any type of commercial transaction. In the EU, the Settlement Finality Directive (SFD), guarantees that transfer orders within the EU which enter the intra-bank payment system of central banks or are used for clearing and settlement of securities are legally settled. However, DLT transactions introduce new challenges to determining the exact moment of finality in public on-chain transactions. This complexity arises because the finality of the transactions relies on consensus algorithms (proof of work or proof of stake) and it is therefore considered "probabilistic", meaning that the exact moment of operational finality is difficult to determine. The SFD is not designed to deal with the type of settlement that exists in DLT consensus mechanisms. Solving this issue would require undertaking a legal analysis of the concept of finality in a probabilistic settlement and consideration of possible legal clarification in the SFD. The EC should review the applicability of existing settlement finality rules to DLT-based securities.

Moreover - as mentioned above - if a DLT settlement system can qualify a Securities Settlement Systems (SSS) settlement finality could be satisfied.

A detailed overview of AFME's recommendations on which policy actions should be prioritized in order to scale DLT-based capital markets is provided in the recent AFME document "Scaling DLT-based SSA Bond Markets – Policymakers' roadmap" (June 2024).

- **Development of DLT-based payment instruments** – Availability of forms of money that are represented on a distributed ledger through tokenization are also key. These include tokenized commercial bank money, DLT-based deposits and special purpose forms of central bank digital currencies that may be designed for specific use by wholesale market participants (wholesale CBDC or wCBDC). The development of DLT-based payment instruments is key to realize the benefits of Delivery-versus-Payment ("DvP") settlement for DLT-based Securities transactions, the distribution of coupons, dividends, and other proceeds on a distributed ledger. For transactions between financial institutions, the ability to settle in central bank money is vital, as other settlement solutions introduce credit risk. Wholesale CBDC is the closest proxy to central bank reserves in a DLT-based ecosystem, representing a form of settlement free of credit and default risk, and limited to wholesale market participants who have central bank account access. The Eurosystem is currently looking[3] into how wholesale financial transactions recorded on DLT platforms could be settled in central bank money. The Eurosystem envisages two options for DLT-based infrastructures for settlement in central bank money[4]. The first one – more ambitious and likely to require several years to implement - involves unified ledger solutions. The second one – likely to be faster and less costly - is based on interoperability-type solutions. We are very supportive of this ECB's exploratory work. At the same time, privately created on-chain payment instruments (tokenised commercial bank money, stablecoins) could also play a role and policymakers should assess whether the current regulatory framework requires clarifications to enable their use.

- **Collateral eligibility** - The eligibility of DLT-based securities as financial collateral and central bank collateral is critical to their value and attractiveness to investors and also for banks to underwrite the securities and act as market makers. However, in accordance with the Eurosystem's current criteria to accept marketable assets as eligible collateral, debt instruments generally have to be transferable in book-entry form, held and settled with an eligible Securities Settlement System (SSS), and admitted to listing and trading on a regulated market[5]. At a minimum, securities issued through the DLT Pilot Regime should be considered eligible as central bank collateral, particularly where an exemption from the security registration requirement has been provided by the relevant competent authority[6]. In the medium-term, to facilitate technological neutrality, a reassessment of the eligibility criteria to qualify DLT-based instruments issued outside of the DLT Pilot Regime as central bank collateral should be considered.

- **Consideration of technology issues and network archetypes** – Considerations on the possible DLT network archetypes (private-permissioned, public-permissioned, public-permissionless) need to explore the opportunities and risks linked to the various solutions. Private-permissioned networks are the closest analogue to traditional financial market infrastructure (e.g., settlement systems), but may have limited built-in interoperability. Public networks have a broader connectivity and increased access, and therefore have specific risk considerations for which mitigations are in various stages of development and implementation.

3 Please see: "Central bank money settlement of wholesale transactions in the face of technological innovation" by H. Neuhaus and M. Plooij, August 2023.

4 An overview of this work is provided in a speech by Piero Cipollone, member of the executive board of the ECB "Modernising finance: the role of central bank money", February 2024

5 DLT-based securities cannot be admitted to trading on trading venues (Regulated Markets, Multilateral Trading Facilities and Organised Trading Facilities) nor be used as financial collateral unless they have been registered or kept on a CSD (or third-country entity with equivalence).

6 This is the approach taken by the UK's Digital Securities Sandbox, which allows for all securities issued through it to be eligible for securities financing transactions and as collateral.

Both permissioned and permissionless chains have specific strengths and it is not possible at the present juncture to say which one will best support use at scale. For this reason, it is important that regulation does not preclude the use of permissionless chains (e.g. public permissionless like Ethereum). Currently the BCBS has decided that on-chain securities on a permissionless blockchain are ineligible for Group 1 treatment (i.e. being assigned the same capital charge as the same securities issued on traditional infrastructure). This means that tokenised securities on permissionless chains will be subject to Group 2 treatment (and assigned a 1250% risk weight). Work should continue to explore solutions to address regulators' concerns. We note, however, that risks can be mitigated where permissionless blockchains have adopted or programmed protocols for the governance, tracking, and control of digital assets movement. To use Ethereum as a specific example, there are varying levels of token contracts that can be placed on the Ethereum blockchain that allow for graduating levels of controls, such as blacklists, whitelists and transfer restrictions[7]. Given the potential of permissionless chains and the progress that is made in addressing potential risks, it would be more beneficial for capital treatment to move from a binary permissioned vs permissionless approach to a more granular risk-based approach. We encourage regulators to specify, in dialogue with industry, what risks they would like to see addressed and what mitigants they would consider as being appropriate.

Financial institutions have a successful track record of integrating transformative technological innovation. We therefore caution against any punitive, DLT-specific prudential treatment as it and could be counter-productive, increasing both the regulatory and financial burden of DLT-related innovation by regulated financial institutions.

More broadly, all industry and official sector stakeholders will need to collaborate to identify and promote technical solution which allow scalability, cybersecurity and regulatory compliance.

- **Standardisation and smart contracts** – In addition to network archetypes, as market participants explore and adopt solutions, fragmentation in capital markets infrastructure could emerge and consolidate over time if left unaddressed. Industry work towards standardisation and interoperability (work which can involve regulators' perspectives and a role as facilitators) is therefore important. One specific area where standardisation seems important is around smart contracts (defined as self-executing contracts with the terms of the agreement directly written into code), which are central in the automatization of processed in a DLT infrastructure. This work on standardisation and interoperability should also be complemented by the consideration of legal questions around smart contracts. Smart contracts raise questions about their legal enforceability and recognition under existing contract law. Legislators might need to clarify the legal status of smart contracts to facilitate their use in DLT-based capital markets.

- **Prudential treatment of crypto assets** – The recent EU banking package (CRR3/CRD6), by introducing a temporary regime, made a first step towards the implementation in the EU of the global standards on the prudential treatment of crypto assets. Despite the temporary nature of the regime, its greater level of conservatism (than the current BCBS standard) might act as a disincentive to specific forms of tokenisation. Calibration of some aspects of the global standards is still under way but it is expected to be completed during 2024. Therefore, in the coming months the EU will need to consider the implementation of the finalised BCBS standards. As mentioned above, tokenised securities on permissionless chains are currently subject to a punitive treatment: a more proportionate and risk-based approach should be considered. Moreover, DLT-based securities should – like traditional ones – be eligible for treatment a high-quality liquid assets und the liquidity prudential standards (liquidity coverage ratio).

  The design of a digital and crypto-asset prudential framework should facilitate bringing regulated financial activities related to digital markets within the appropriate existing prudential framework where associated risks will be subject to robust capital and liquidity regulation, sound risk management and effective supervisory oversight. This will help to promote financial stability, while avoiding overly restrictive limits on innovation for regulated institutions.

7 A tangible example of this is USD Coin, which leverages the ERC20 standard, and allows for the freezing of tokens such that transfers can no longer take place after the order is given, the blacklisting of suspicious addresses and the granting of access to third-party providers to render security services such as fraud detection, risk assessment and identity management.

A prudential framework that allows regulated financial institutions to support responsible innovation also benefits supervisors by providing better insight into the evolution and growth of new technologies and activities (e.g., by requiring the reporting of digital and crypto-asset exposures). At the same time, customers and investors will benefit from more transparent, trusted regulated financial institutions and the protections of fully regulated institutions providing services. Otherwise, unregulated (or less regulated) entities are likely to be predominant providers of crypto-asset-related services. The result would be an unlevel playing field and a lack of transparency in the build-up of leverage and risk in the financial system outside the regulatory perimeter. As mentioned in the previous section, the prudential considerations around the use of permissionless chains are an important element of the discussion.

- **The role of key stakeholders in the ecosystem as catalysts for change** – DLT represents a shift towards a new type of market infrastructure and broader market paradigm where full benefits will be reaped only if DLT is adopted at a large scale. Scaling of DLT-based capital markets requires therefore the whole ecosystem (venues, sell-side, buy-side, custodians and policymakers) to move together.

  Policy makers and market participants should work together to enable the ecosystem to evolve and to identify what steps would have to be taken in the next years in order for DLT-based capital markets to scale. Particularly important would be the role that large issuers, including sovereign and supranational ones, can play in catalysing the adoption of DLT technologies.

  AFME has been exploring how this evolution could take place, including which actions could represent a catalyst and what roadmaps the main actors could consider during this journey.

Working in cooperation with a broad range of stakeholders, AFME has recently finalised two roadmap documents to this effect. The first roadmap[8] ("issuers' roadmap") is aimed at providing support to European sovereign, supranational and public-sector agency issuers in developing a strategy for issuance of debt instruments on DLT-based infrastructure. It sets out the benefits and workings of DLT-based issuance and details a phased approach for public issuers to enter and scale DLT-based issuance; from early-stage issues through benchmark issues to integration of DLT-based issuance in their regular issuance programmes. The second roadmap[9] ("policymakers' roadmap").

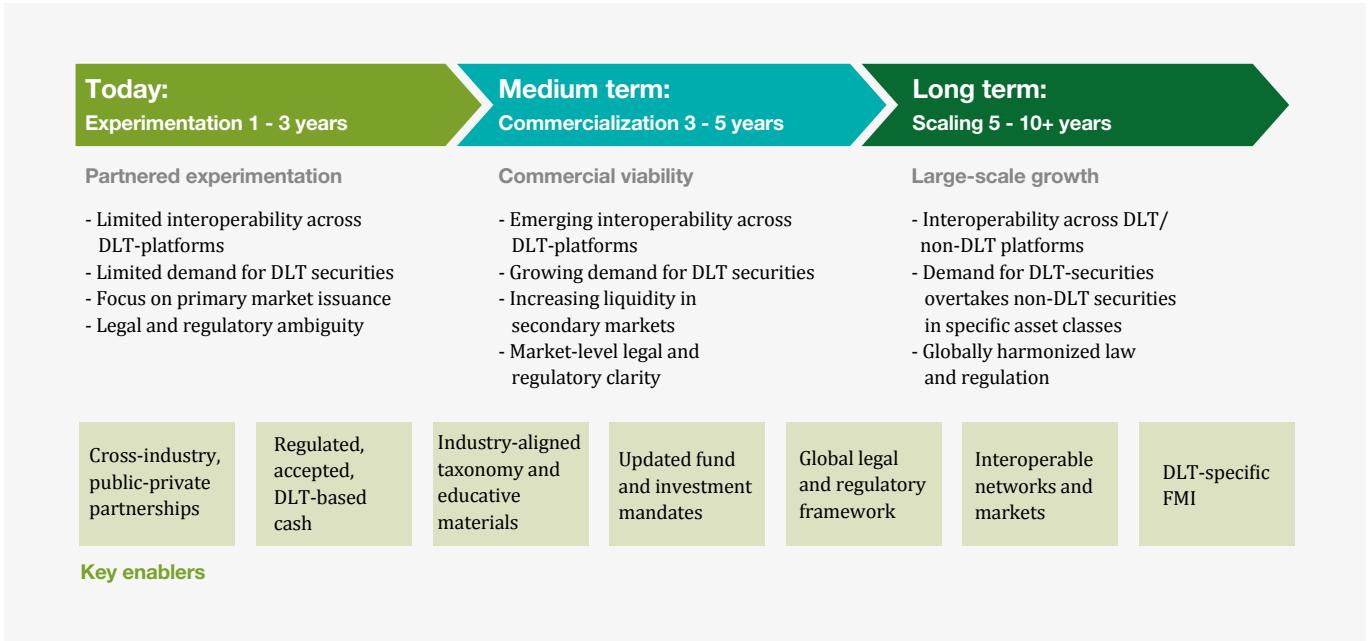
8 *"Scaling DLT-Based SSA and Government Bonds Markets – A Roadmap Strategy for European Issuers"*, AFME, June 2024

9 *"Scaling DLT-based Capital Markets - A Policy Roadmap for the EU"*, AFME, July 2024.

Table 1: **Benefits of DLT**

Policy Objective	Benefit provided by DLT
Financial stability and resilience of capital markets	• Operational resilience: reduction of single-point-of-failure risk in financial market infrastructures • Risk reduction: reduction in settlement failure and settlement-related risks due to automated, programmable and atomic settlement
Efficiency and growth of capital markets	• Making European capital markets more efficient: offering ability to streamline issuance process and compress execution and settlement time (to T+1, T+0) • Increasing access to capital markets by streamlining issuance process for smaller corporate issuers • Developing intraday repo markets: removing trapped capital through faster mobilisation of collateral compressing execution and settlement • Facilitating transition away from paper-based securities (under CSDR) • Fractionalisation of tokens enables access to issuance for a broader investor base
Innovation in capital markets	• Accelerating the Digital Transition: kick-start innovation ecosystem • Accelerating the Green Transition: DLT-based bonds can embed functionality on proceed allocation and fulfilment of sustainability KPIs • Simplifies issuance process enabling more (and smaller) corporates to finance through markets
International competitiveness of capital markets	• Early issuance and engagement enables issuer/jurisdiction to shape the parameters of DLT-based capital markets
Digital sovereignty	• Early development of DLT-based markets in Europe can enable European policymakers and market participants to shape the outlines of DLT-based capital markets. In addition, on-chain central bank money can strengthen digital and monetary sovereignty and take a lead in international monetary transmission through new forms of money

Figure 5: **Possible future developments of a DLT ecosystem**



Source: BCG analysis, GFMA member interviews

UNLOCKING TOKENISATION – RECOMMENDED PRIORITIES

Addressing the regulatory and policy challenges

- Explore possible impacts created by the Central Securities Depository Regulation (CSDR) and possible amendments to remove such impacts.
- Consider an evolution of the EU DLT pilot regime leading to a broader and more flexible scope and assess the future shape of a more permanent framework.
- Undertake a legal analysis of the concept of finality in a probabilistic settlement and consider possible legal clarifications in the Settlement Finality Directive (SFD).
- Achieve eligibility as collateral for DLT-based securities. The Eurosystem should accept DLT-based securities issued through the Pilot Regime as a first step.

Development of DLT-based payment instruments

- Development of solutions for allowing wholesale financial transactions recorded on DLT platforms to be settled in central bank money.

Prudential treatment of crypto assets and consideration of technology issues

- Assess the respective opportunities and risks – and available mitigants – of permissioned and permissionless networks and move to move from a binary to a risk-based approach.
- Move from the temporary prudential treatment of crypto assets introduced in CRR3 to a more proportionate stable one, in line with upcoming final Basel framework.
- Broader stakeholders to cooperate to foster high levels of standardisation and interoperability, to avoid growing fragmentation in DLT infrastructures. For instance, work on standardisation of smart contracts will be particularly important.

Need for the whole ecosystem to move

- Policy makers and market participants to work together to promote a roadmap for key actors in the ecosystem to scale DLT-based capital markets to scale.
- Large issuers, including sovereign and supranational ones, can play a central role in acting as catalysts in the adoption of DLT technologies.

1.2 Effective implementation of MiCA

In the EU, once implemented, MiCA will offer a comprehensive regulatory framework for market participants, fostering transparency and the attractiveness of the crypto-assets sector. In the coming years – in a context where there is no lengthy experience of the use of legal and business concepts relating to crypto-assets, regulatory papers, jurisprudence, and market practice - the implementation of MiCA will offer opportunities to assess areas where the framework could be strengthened, clarified or expanded, also in light of the recent market developments. The potential for differences in interpretation could also create legal uncertainty, and may be a major disincentive for regulated financial institutions meaningful participation in the emerging crypto-asset ecosystem. This would result in negative consequences for crypto-asset markets, market participants, as well as for consumer protection and consistency of supervisory practices should be monitored closely to avoid this.

Custody services and custodians will play an important role in the ecosystem for digital assets.[10] Article 67(8) of MiCA sets out an important principle on custodial liability provisions, capping liability where appropriate and noting that events that are independent of the provision of the service are not attributable to the crypto-asset service provider. This is welcome, however we believe that in order for there to be consistent interpretation and implementation of this liability principle further clarity is required for the following key terms: '*incident', 'attributable', 'reasonable control*' and *'market value'*. This could be achieved in the form of official sector guidelines or Q&A processes, and broader discussions with relevant stakeholders.

RECOMMENDED PRIORITIES

Work on MiCA implementing measures

- Focus on the effective implementation of the important recent reforms. MiCA is at the beginning of its journey and important Level 2 measures need to be finalised in close dialogue with stakeholders.

Ensuring consistent interpretation of custodial liability

- Develop official sector guidelines or Q&A processes, and broader discussions with relevant stakeholders to promote a common understanding around the issue of custodial liability.

"MiCA will offer a comprehensive regulatory framework for market participants, fostering transparency and the attractiveness of the crypto-assets sector"

10 Article 67(8) states, "Crypto-asset service providers that are authorised for the custody and administration of crypto-assets on behalf of third parties shall be liable to their clients for the loss of any crypto-assets or of the means of access to the crypto-assets as a result of an incident that is attributable to the provision of the relevant service or the operation of the service provider. The liability of the crypto-asset service provider shall be capped at the market value of the crypto-asset lost at the time the loss occurred. Events not attributable to the crypto-assets service provider include any event for which the crypto-asset service provider could demonstrate that it occurred independently of the provision of the relevant service, or operations of the crypto-asset service provider, such as a problem inherent in the operation of the distributed ledger that the crypto-asset service provider does not control.". In this context, it is already clear that market participants would benefit from additional interpretative guidance of provisions in Article 67(8) of MiCA

Decentralised Finance (DeFi)

An important and growing area EU policymakers will need to consider is decentralised finance (DeFi). DeFi seeks to provide financial services using blockchain or distributed ledger technologies and smart contracts in an open, decentralised and permissionless way. In principle, DeFi applications are characterised by high automation of processes, a distributed network which should have no single point of failure and not rely on a single source of information, which is not governed by a central authority and is accessible to anyone using a computer connected to the internet. In practice, depending on the design of the applications, decentralisation is often not fully achieved. Elements of DeFi, however, show important promises in terms of increased automatization and efficiency of the financial system.

DeFi applications being at nascent stage, they remain relatively small in scale globally and do not represent a significant risk to financial stability. The Financial Stability Board (FSB) [11] had also noted that the current overlap of DeFi and Traditional Finance (TradFi) is not yet significant, although it should be actively monitored and managed.

While DeFi is still at a nascent stage, it has been developing quickly and its potential uses and intersections in capital markets may lead to policymakers considering options for bringing it within the regulatory perimeter, so that risks to market integrity, financial stability, and end users, are identified and can be managed. We believe it is important to avoid the potential exclusion from such perimeter of so-called "decentralised activities" as this could open opportunities for regulatory arbitrage and weaken the application of emerging frameworks.

This should be done in a way that leaves room for promoting financial and technological innovation. DeFi, if operating within an appropriate regulatory perimeter, could provide interesting use cases. In particular, the use of smart contracts to create effective permissions on public permissionless DLT networks (i.e., with appropriate Know Your Customer (KYC)/ Anti Money Laundering (AML) mitigations) will create opportunities to increase efficiencies and decrease cross border transactional friction through the application of common global standards.

Decentralised Finance – Risks and Opportunities

Risks

- The difficulty in applying existing investor and market protections – due to data gaps and technological complexities
- Operational, technology, code vulnerabilities, and security risks
- Vulnerability to illicit activities, facilitated by the pseudonymous nature of transactions
- Full transparency could be an issue in those cases where some level of privacy is needed
- Immutability might create challenges for upgrades or error corrections

Opportunities

- Programmability, composability and openness
- Automation, leading to increased speed and cost efficiency
- Transparency
- Immutability and censorship resistance
- Reduced reliance on single points of failure and centralised institutions
- Opportunity to develop innovative financial products, leading to greater access to markets and inclusion

11 https://www.fsb.org/wp-content/uploads/P160223.pdf

A Digital Capital Markets Union

Digitalisation and new technologies have the potential to support the development of capital markets and the objectives of the Capital Markets Union (CMU). By increasing efficiency, lowering costs, boosting transparency and availability of information, allowing greater access to data, digital technologies can support the CMU project, the removal of market barriers and the increased cross-border provision of services and, ultimately, allow greater access to capital markets both for those looking for funding as well as for investors. Digitalisation and CMU are mutually reinforcing objectives: if digital finance can support the development of deeper and more integrated capital markets, a successful CMU can mobilise the resources needed to finance the digital transformation, improve access to finance for innovative companies and make the EU more competitive.

More efficient capital markets	• The use of DLT technologies can provide greater efficiency across the lifecycle of a security, allow automation of work flows (through smart contracts), lowering issuance and transaction costs. • The increased transparency of distributed ledgers can inform and guide issuance and investment strategies. Greater transparency can also support the allocation of green bonds' proceeds. • Greater efficiency (e.g. in settlement processes) can translate into lower risks and increased liquidity. • Greater access to data and to AI technology can improve issuers and investors' strategies.
Increased access to funding	• The use of DLT technologies can simplify and reduce the costs of issuance of securities allowing more SMEs to tap capital markets.
Larger investor base **Increased retail participation**	• Fractionalisation of security tokens allows access to issuance for a broader investor base. • Retail investors access to financial services can be greatly increased through digital technologies, as well as their ability to access education resources and disclosures in digital form. • Data availability and AI technology can support personalisation of financial services. • Technology can give retail investors easier control of their overall financial situation and greater ability to compare products.
Removal of cross-border barriers	• Greater access to data and removes the information barriers for cross-border investments. • Automation of actions to exercise investors' rights (votes, dividends, coupons, access to information) can support cross-border engagement. • Automation of administrative processes (e.g. for taxation) can reduce challenges for cross-border flows.
Increased competition, choice, inclusion	• New technologies can allow both incumbents and new entrants to provide a new products, increasing choice and competition. • Technology can give investors easier control of their overall financial situation and greater ability to compare products and to switch providers.
Resilience	• Decentralised infrastructures can contribute to greater resilience by removing single points of failure. • Adoption of cloud technology allows financial institutions more agility in their innovation strategies (avoiding heavy up-front investments) to remain competitive and to leverage data and AI. • Reduced failures of transactions due to greater automation.

Chapter 2 – Data sharing and open finance

AFME believes that the EU's proposed Financial Data Access (FiDA) framework, if designed correctly, has the potential to enhance the way banks operate, encourage innovation (even across sectors, if some provisions are met) and support a more effective and efficient data ecosystem.

While EU legislators are progressing their work on the proposal, negotiations and implementation efforts are likely to span over several years and will therefore be part of the key priority areas EU policymakers will be focusing on during the next legislative cycle.

Importantly, these initiatives will interact with the horizontal framework which will be introduced through the recently agreed Data Act. It will be important that the EU open finance framework is designed in a way that takes into account the impact and the lessons that will originate from the implementation of the Data Act.

As to the FiDA proposal, we have identified the following key principles necessary to support the development of a robust Open Finance Framework. These are:

- A clearer definition of the scope of FiDA;
- A level playing field is crucial - In order for an Open Finance Framework to flourish not only in financial services but across multiple sectors, there must be consistent and appropriate regulatory oversight;
- Interoperability and an appropriate level of standardization, promoted through market-led initiatives;
- An appropriate framework for compensation, to ensure fair allocation of costs across the data value chain and to safeguard fair competition;
- Clear liability provisions, to provide legal clarity with respect to the access, processing, sharing, and storage of data.

We provide below an overview of some key issues[12]. A more detailed analysis is provided in our position paper.

2.1 FiDA scope

The scope of the data to be included in FiDA, as set out in proposed Article 2(1) and Article 3(3), is overly broad. It should capture only raw data provided by a customer and transactional data related to services in scope of FiDA where they are available and exclude any inferred data, which will have required significant investment by those institutions and constitutes their own intellectual property. We therefore strongly support the exclusion of inferred and derived data.

In addition, we also view that the definition of "customer" is too wide. For instance, it would not be useful for wholesale and corporate clients (including financial institutions, institutional clients or multinational corporates and their affiliated entities) to be included. This is because such "customers" tend to use very specific products of services, have dedicated data access interfaces and would also likely have risk management policies which would prevent the use of a third-party provider for this purpose.

12 A more detailed analysis is provided in our position paper. https://www.afme.eu/Portals/0/DispatchFeaturedImages/231020%20Position%20Paper%20on%20FIDA-PSR%20vF.pdf

2.2 Regulation and Supervision of Financial Information Service Providers

We have some concerns about the status assigned to the new category of entities – the Financial Information Services Providers (FISPs), defined as "data user[s] authorised to access the customer data for the provision of financial information services". Given that FISPs will receive large quantities of highly sensitive customer data from in-scope financial institutions, they should be subject to strong regulation and effective supervision, controls and obligations when receiving such data. As a consequence, we believe that FISPs should be subject to the full scope of DORA and should not be able to benefit from a simplified framework. This is key from the perspective of strengthening the data security and operational resilience of the whole financial data ecosystem, as well as maintaining a level playing field between different market participants.

We welcome that, under the proposal, FISPs would be prohibited from sharing onwards its data without user consent to entities within their groups.

As to the possible role of institutions that are defined as "gatekeepers" under the Digital Markets Act, given their strong presence in the data markets, we think that gatekeepers should not be authorised as FISPs (at least until the Commission has deemed that data sharing under the Digital Markets Act has been achieved).

2.3 Proportionate implementation

The implementation of FiDA faces many challenges surrounding data standardisation, updating of legacy systems, creating data sharing schemes and ensuring their governance structures are robust. Given the scale of FiDA as noted above, along with the current fragmented nature of the data landscape, the implementation of FiDA will be amongst the largest upcoming technical builds for many institutions. In addition, reaching agreement on the design of data access schemes and their implementation will take time. In particular, the schemes will require consultation and agreement with a large number of diverse stakeholders.

Therefore, it is crucial that a suitable, realistic and gradual implementation timeframe is adopted.

This step-by-step implementation should follow three main phases:

1. **FiDA readiness assessment by data category**, followed by a decision on its inclusion in the implementation phase. This assessment would be carried out by the EC, in consultation with the European Supervisory Authorities (ESAs) and taking into account market stakeholders' feedback. Factors to consider include: Market demand and benefits by customer category; data quality and availability; implementation costs.

2. **Definition of financial data access schemes**. For specific financial services that have demonstrated potential use cases and have been assessed as "FiDA ready", the phase of implementation should begin with the definition of data access schemes through negotiation among scheme participants (data holders, data users, customers, and prospective FISPs) on the scheme. This would then lead to an agreement on the key elements of the scheme including: Use cases and data categories; customer categories; compensation methodologies; governance and liability framework; resources for the oprationalisation of the scheme; dispute management arrangements. The timelines for the definition of the schemes should be scheme-specific. This is necessary because of the heterogeneity of data, varying number and nature of participants in the scheme.

3. **Implementation phase**. The implementation of the schemes will involve significant investments aimed at operationalising data sharing. The technical solutions (including data access standards, APIs) agreed by scheme members are implemented during this phase, following an agreed implementation plan.

2.4 Compensation

The principle of the data holder being able to receive reasonable compensation for making the data available to a data user is an important step forward to create a fair distribution of value in any data sharing frameworks and an incentive structure that is aligned with the policy objective of developing data markets and enabling innovation. In our view, the FiDA proposal's more restrictive stance on compensation should be changed to be aligned with the more market-driven approach under the Data Act.

RECOMMENDED PRIORITIES

Scope

- The scope of "customer data" in FiDA Article 3(3) should be clarified to encompass only raw data, including transactional data while inferred data should be excluded.
- The definition of "customer" should exclude wholesale and corporates clients, which use specific institutional and corporate banking services and may have risk management policies against sharing data with third parties.

Regulation and supervision of FISPs

- FISPs should be subject to strong regulation and supervision of, including DORA and cybersecurity rules, and support the obligations on them when receiving customer data (e.g. prohibition from sharing data onwards, within the group they might be part of, without user content).
- The authorisation of BigTech gatekeepers as FISPs should be prohibited until the clear implementation of data sharing under the Digital Markets Act has been achieved.
- Third-country FISPs should be regulated and supervised to the equivalent outcome as the conditions for EU FISPs under FiDA, especially when they do not have physical presence in the EU.

Proportionate implementation timelines

- There should be a staggered implementation, beginning with targeted use cases identified as delivering the most significant benefits.

Compensation

- The calculation of compensation in FiDA and PSR should be market driven and not only "directly" linked to making the data available. The approach to compensation should be aligned with that agreed under the Data Act
- Any compensation cap should benefit only small and micro enterprises.

Chapter 3 – Cybersecurity and ICT resilience

3.1 DORA implementation

The Digital Operational Resilience Act (DORA) took effect on 16 January 2023, with final industry compliance required by 17 January 2025. The regulation underscores the importance of digital operational resilience in today's increasingly interconnected and digitised landscape and seeks to expand the reach of European regulators by bringing both financial institutions that operate in Europe and providers of information and communication technology (ICT) to these firms in scope. Compliance with DORA is a top priority given financial entities' increasing use of ICT and dependence on third-party ICT service providers, as well as the heightened focus on ICT and cyber-related risks impacting these third parties.

Work on the implementation of DORA's comprehensive requirements will be central in the coming months and will lay the foundation for a harmonised, secure and resilient EU digital financial sector. In this respect we emphasise the following priorities for the next phase:

- **Explore mechanisms for developing best practice industry guidance on operational and cyber incidents**: In the future, EU authorities will be in possession of a high level of cyber related intelligence, collated through incident reporting, resilience testing and regulatory supervision. Formal mechanisms are required to enable this information to be strategically leveraged at the aggregate level and factored into best practice guidance. Rather than sharing live incident reports, the authorities should focus on rationalising inconsistent reporting frameworks that fragment reporting across products and sectors with different reporting classifications and thresholds serving to inhibit the cybersecurity of the EU. Such coordination and collective action would build upon the legislative developments of the last Commission. In this context EU policymakers should also explore whether a public-private community could identify key trends from recent periods of disruption, distilling best practice techniques for financial entities in mitigating and responding to such risks.

- **Review and consolidate the existing EU frameworks addressing operational risk and resilience and third-party risk management**: With DORA being part of a broader regulatory framework where sector specific rules interact and sometimes overlap with horizontal or product specific rules, it will be important to ensure a coherent regulatory environment, particularly for a heavily regulated sector like financial services. In recent years EU regulatory requirements on outsourcing, operational risk and cyber security and incident response have been significantly enhanced, through both sectoral legislation and horizontal proposals. The result is an increasingly fragmented landscape with several overlapping, and at times inconsistent frameworks. The Commission should map the interdependencies and resolve duplications and inconsistencies in regulatory expectations (including across outsourcing and registers, and incident reporting), before introducing further requirements. This should include reviewing issues which have arisen through Member State application of EU initiatives and conflicting or overlapping horizontal product regulation[13].

- **Reject efforts at the national level to introduce sovereignty/localisation requirements into EU frameworks**: As the sector has increased their reliance on technology services provided by large technology companies (Big Tech), the associated risks are being managed through effective third-party oversight, operational resilience and cybersecurity frameworks. Seeking in future to restrict EU firms from accessing non-EU providers, such as global Big Tech firms, could severely risk both operational stability and market choice. It additionally undermines the careful balance which was achieved in the milestone DORA Regulation, where attempts to impose data localisation obligations were rightly rejected. Such obligations should not be reproposed in the form of technical measure (e.g. cybersecurity certifications).

- **Adopt a proportionate approach in the early phases of DORA implementation**: At a more operational level in the short term, there remains a significant uplift challenge associated with DORA. Financial entities will be rolling out their DORA programmes over the course of 2024/25, spanning multiple operational and technological domains, with little opportunity for preparation where final technical standards were only released 6 months in advance. A proportionate and risk based approach to supervision, especially in the early phases, will be critical.

13 One example where such overlap could emerge is the Cyber Resilience Act (CRA) where "products with digital elements" within the scope of the CRA will already be captured under the Digital Operational Resilience Act (DORA).

A more detailed overview of implementation issues is provided in an AFME-Protiviti paper on "*DORA compliance: untangling key hurdles to implementations*" (May 2024)[14].

RECOMMENDED PRIORITIES

- During the early phases of DORA implementation, adopt a proportionate and risk based approach, given the short term operational challenges linked to the initial roll-out of DORA programmes.
- Assess the interplay between the sector-specific DORA regulation and the various horizontal frameworks being introduced to bolster cybersecurity on a cross-sectoral basis, in particular the hybrid nature of products and services in the digital age.
- Address the overlap between the EBA Outsourcing Guidelines and the DORA requirements on registers of information, contracting and subcontracting ICT services, taking account of the practical complexities in simply trying to distinguish between ICT and non-ICT assets/services.
- Consolidate outsourcing registers and the incoming DORA register of information, which will in many cases contain the same information (only in a different format).
- Harmonise incident reporting obligations for significant credit institutions, in conjunction with the ECB, addressing inconsistencies in reporting timelines and requirements for example on cyber-attacks.
- Explore whether a public-private community could identify key trends from recent periods of disruption, distilling best practice techniques for financial entities in mitigating and responding to such risks.
- Ensure that the development of technical schemes on cybersecurity certifications, do not introduce significant policy changes which are non-technical and would instead require a fuller impact assessment and discussion at legislative level.

3.2 The need to avoid localisation requirements in the cloud certification schemes

Cloud adoption in financial services is steadily increasing, leading to improved capacity, resilience, client experience and cost efficiency. Cloud services provide agile, highly available and scalable technology platforms that significantly alleviate the effort required for financial institutions to manage their own infrastructure (e.g. data centres), while enabling greater levels of digitisation and security across technology services. This can allow financial institutions to deliver more innovative, unique and client-focused services.

In addition to technology infrastructure, the software market is also moving rapidly to the cloud. Many software providers now distribute their products through a cloud-based model called "software as a service" (SaaS). This shift makes using the cloud increasingly necessary for any financial institution needing to remain digitally competitive. As a result, many institutions are already adopting a 'cloud-first' approach, with cloud becoming a core element of how they design, build and deliver technology services.

DORA has introduced an effective regulatory framework for banks' use of cloud services. Recognising the fact that access to the most advanced technology and geographical diversification are important factors in ensuring competitiveness and resilience for banks operating in the EU, policymakers have chosen not to impose strict localisation requirements for cloud providers. It is crucial that this approach will not be undermined through the introduction of digital sovereignty requirements in the context of the EU cloud certification scheme (EUCS). While AFME supports efforts to build a competitive cloud market, larger choice opportunities for users and greater cloud capacity in the EU, this should not lead to undue restrictions to EU firms' ability to access non-EU providers.

14 At a more operational level: the final technical standard for ICT-related incident classification has been released, and along with the additional draft requirements for compulsory and standardised incident reporting further raises concerns that a strict interpretation could result in a disproportionate amount of reporting at the expense of effectively managing ICT related incidents. The potential for over-reporting could dilute the effect of truly meaningful notifications.

One of the key elements of DORA is an introduction of the oversight framework for the designated "Critical Third Parties" (which may include Cloud Service Providers), that is designed to cover also such Critical Third Parties that are located in third-countries. Importantly, whilst DORA requires that a designated Critical Third Party that is based in a third-country will have to establish a subsidiary in the EU, it also explicitly acknowledges that ICT services can be provided to EU-based financial entities by Critical Third Parties established in third-countries without the need to locate their operations in the EU.

Similarly, the EUCS should refrain from introducing far-reaching localisation requirements (such as the need to operate and maintain a cloud service from the EU, the need for employees to be based in the EU, the need to locate the headquarter in the EU, the need for contracts to be governed by EU law) which raise strong industry concerns over the impact on operational resilience, market choice and digital innovation.

EUCS – RECOMMENDED PRIORITIES

- Given their significance, any measures which could result in the imposition of localisation requirements, should be subject to an impact assessment and allow a broad and transparent consultation with all affected industries. An implementing act is by nature not able to ensure this.
- Any regulatory measures should target specific risks identified (e.g. unlawful data access) and be designed to increase operational resilience, rather than broadly imposing an unnecessary compliance burden on industry, enforcing contract localisation or restricting access to key third country services;
- Measures should be subject to economic impact assessment involving all affected industries;
- Alignment with global data and technology standards should be pursued (to avoid increasing regional compliance costs for industry) as well as compliance with WTO commitments.

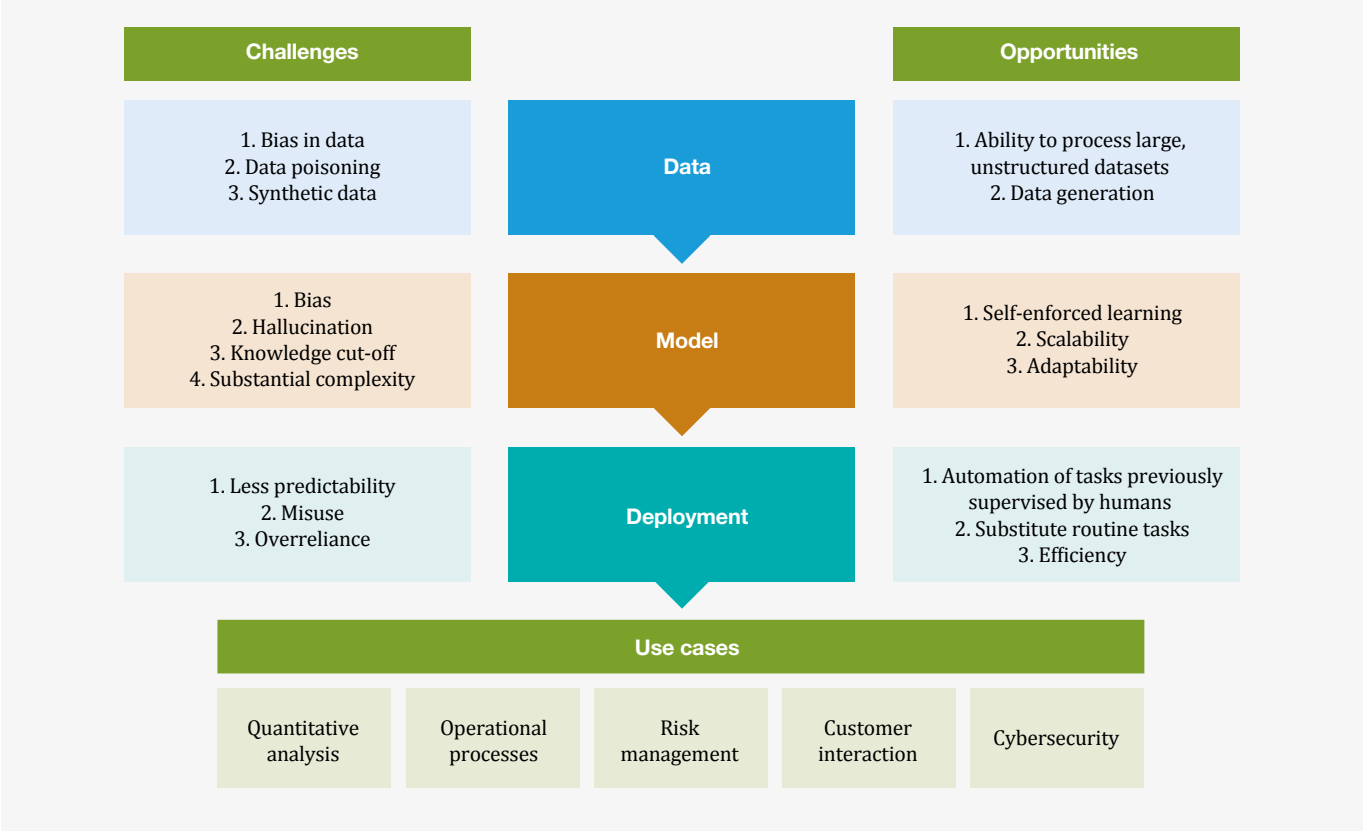
"The EUCS should refrain from introducing far-reaching localisation requirements which raise strong industry concerns over the impact on operational resilience, market choice and digital innovation"

Chapter 4 – Artificial intelligence

Many financial institutions have been integrating artificial intelligence[15] (AI) into their operations across a wide range of business functions and use cases. The use and application of AI tools and systems are diverse and include enhanced and more tailored customer experience and improved ability to detect anomalies, risks or frauds; automated processes and improved trading strategies; support in complying with regulatory requirements and risk management processes in particular, firms have utilized "traditional" forms of AI and machine learning for many years, and consequently have developed governance processes to oversee, manage and monitor their application of AI, in accordance with their existing regulatory obligations. The significant leap forward represented by the rapid emergence of generative AI has the potential to bring additional opportunities.

Overall, AI has the potential to transform financial services and capital markets to make them safer, more efficient, accessible, and tailored to consumer needs. This, in turn, brings important benefits to consumers and the wider global economy. At the same time these opportunities require careful consideration of new risks and challenges introduced by a growing use of AI. These include the need to ensure fairness, avoiding biases, and ensuring transparency. With AI applications becoming more sophisticated and complex, regulatory frameworks can struggle to keep pace. Complex AI models can also be difficult to interpret, making it difficult to understand / explain how a decision has been reached. Adoption at large scale of AI could make critical functions increasingly reliant on such technology, and be accompanied by a possible concentration of AI suppliers, requiring effective risk management[16].

Figure 6: **Overview of challenges and opportunities**



Ssource: ECB analysis, AFME elaboration

15 In this document we will use the OECD definition of AI systems: An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

16 A comprehensive overview of AI developments and implications for the financial system has been published in the recent ECB Financial Stability Review: "*The rise of artificial intelligence: benefits and risks for financial stability*", by Georg Leitner, Jaspal Singh, Anton van der Kraaij and Balázs Zsámboki; May 2024.

The proliferation of AI tools and rapid pace of AI adoption have led policymakers around the world to propose new principles and guidelines or new regulatory initiatives. In the EU this has led to the adoption of the AI Act, with the overall goal to encourage the adoption of trustworthy AI within the EU economy and to ensure that AI is safe and lawful.

Financial services is a highly regulated sector and existing regulations largely address and mitigate the key risks which might be caused or increased by the use of AI. These include rules in respect of outsourcing, technology risk management, conduct[17], cybersecurity, duty to clients, internal governance, and model risk management, in addition to sector-agnostic requirements around data privacy and data protection and established internal risk management and governance frameworks.

There is a real concern that a fragmented regulatory approach, with overlapping regimes mandating different requirements, could end up being a major risk for financial entities when using AI, and could prevent them from realizing the genuine benefits of this technology.

We recommend that regulators take a principles- and risk based approach to AI, giving financial institutions flexibility in how best to operationalise the principles in relation to their AI adoption, in recognition of the fact that the technology is still evolving.

Table 2: **Examples of areas where existing regulations already apply to AI**

Market Protection	Financial firms that use AI systems in connection with providing services to investors may find that their AI systems are subject to the requirements of various market protection legislation, such as MiFID II. For example: • Financial entities using AI systems for trading or investment decision-making must ensure that they produce detailed and interpretable logs and records of all decisions and transactions to help meet transparency and reporting obligations under certain of these laws. • AI systems used in trading must be designed to operate in a way that complies with market abuse requirements and are auditable. • Certain market-specific regulations require financial firms to take all sufficient steps to obtain the best possible result for their clients when executing orders. AI systems used in automated trading must therefore be designed to consistently consider multiple factors (such as price, cost, speed, and likelihood of execution) to ensure compliance with such a best execution requirement. • Market-specific regulations, that apply to general obligations and trading practices regardless of whether AI is used, would also continue to apply. • There are various existing controls that are designed to mitigate the impact of volatility in the markets.
Risk Governance	Firms need to have effective risk governance structures in place to identify, understand and manage risks associated with applications of AI systems. This includes having oversight of the full model development cycle, from proposal to deployment and ongoing monitoring.
Risk Monitoring & Management	While there are potentially some novel risks to consider from the use of AI (for instance, related to the use of third-party systems), identifying, addressing, and monitoring AI-related risks need not be fundamentally different to firm's existing risk management frameworks
Cybersecurity	As firms consider integrating AI systems into their business practices, they must consider the cybersecurity of their valuable data and operational significance. In particular, data poisoning, data leakage, and data integrity attacks are particularly important risks to be mindful of given AI systems' dependency on the data used to train and test it. In addition to the cybersecurity risks presented from the use of AI, financial institutions also need to be aware of how threat actors may use AI to increase the propensity and sophistication of existing cybersecurity threats.
Data Privacy	The data entered into or associated with AI systems (as training, prompt or reference data) may involve personal data that is subject to, and protected by, data privacy laws.
Transparency	Transparency in AI is important to help facilitate confidence and trust in AI. There are broadly three categories of transparency considerations: (1) requirements to disclose when individuals are interacting with an AI system, or output created by and AI system; (2) in certain circumstances, requirements to disclose where an individual is subject to a decision created by an AI system; and (3) requirements for developers of AI systems to disclose certain information to the users and deployers of those systems.
Operational resilience	As firms consider deploying AI systems, firms' operational resilience posture in connection with those AI systems is gaining increasing importance.

17 ESMA has on 30 May published a statement on the use of AI in the provision of retail investment services.

4.1 Implementation of the AI Act

With the EU Artificial Intelligence Act now the key priority is implementation of the Act and ensuring clarity[18] as to how the financial services industry can best comply with the requirements set out.

While the AI Act applies more generally, sectoral guidelines have the potential to become particularly useful for the industry, for instance guidance related to financial sector use cases (such as creditworthiness assessments of natural persons). Importantly, there should be coordination between the different implementing bodies cross-border and EU wide. It is essential that there is work undertaken to synchronise these elements to ensure smooth implementation of the AI Act for financial services.

Going forward, we would therefore welcome greater clarity on the timeline of processes and how the different bodies will interact with each other. We encourage policymakers to consult industry in the creation of standards and Level 2/3 measures for the AI Act which would greatly benefit from closely considering the sector's view on AI and the Act's implementation.

"The key priority is the implementation of the EU Artificial Intelligence Act and ensuring clarity as to how the financial services industry can best comply with the requirements"

18 Key implementation issues for the industry are: Compliance with Article 8-18 on high-risk AI systems; The working of 'substantial modification' definition; What the Fundamental Rights Impact Assessment means in practice; The process for designating systemically risky General-Purpose AI models; How the supervision model will work across subject areas and Member States.

Notes

Notes

/ 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.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim 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.

Focus
on a wide range of market, business and prudential issues

Expertise
deep policy and technical skills

Strong relationships
with European and global policymakers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)

afme/
Finance for Europe

London Office
Level 10
20 Churchill Place
London E14 5HJ
United Kingdom
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 883 5540

Frankfurt Office
Frankfurt Office
Große Gallusstraße 16-18
60312 Frankfurt am Main
Germany
+49 (0)69 710 456 660

Press enquiries
Rebecca O'Neill
rebecca.oneill@afme.eu
+44 (0)20 3828 2753

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

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