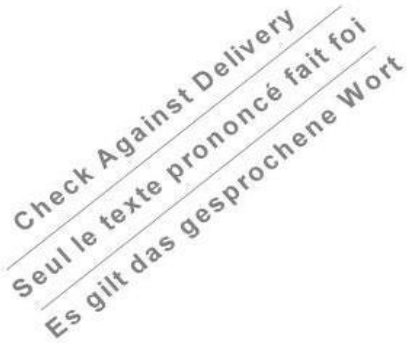
Jose Manuel Campa's keynote speech at BCBS-FSI high-level meeting for European Supervisors

Basel, 22 May 2024

Expanding the boundaries of supervision in the EU



Thank you for inviting me, it is my pleasure to speak here at the High-Level meeting of European Supervisors.

While today the word "revolution" seems to be quite misused in many contexts, it is undoubtful that the last decade experienced a series of impactful innovations that changed completely the financial sector's landscape. First, new financial institutions have acquired an increasingly important role in financial intermediation, establishing themselves as an alternative to bank financing. Second, the pervasive use of new technologies by financial entities, the increasing digitalisation of financial services, the increased operational interconnection between financial entities and ICT third-party providers. Finally, the emergence of new institutions active in the issuance of the crypto assets.

Therefore, as European supervisors, we are now facing multiple challenges, as new risks may appear which need to be monitored and addressed. In one of the masterpieces of the European literature of the last century, "The Leopard" by Tomasi di Lampedusa, one of the characters says, *"if we want that everything remains the same, everything needs to change"*. While this is often used to indicate a Machiavellian conservative attitude, promoting only shallow changes that keep the substance of matters unaltered, it also provides the hook to reflect on financial markets experiencing overarching and fast-paced changes. Of course I am not advocating a full-blown revolution of practices, let alone changes that will only scratch the surface of the problems keeping them unsolved. But if we want to keep a well-functioning financial system, able to funnel funds efficiently from savers to investors, while at the same time protecting financial stability,

we must reflect on how supervisory practices and priorities should adapt to the new reality, to ensure that they remain fit for purpose.

Before tackling each of these issues, let me make one more general point – and I am grateful to say that here in Basel at the BCBS. Those challenges are all global in their nature and - to be addressed efficiently - they need a coordinated approach. Therefore, the work carried out both by the BCBS and by the Financial Stability Board on all these three fronts has been particularly helpful, setting out global standards and best practices[1].

The surge in Non-bank Financial Intermediation

Since the Great Financial Crisis, we have witnessed a substantial increase in the size of the non-bank financial sector assets. Part of this increase reflects the substantial growth in the traditional asset management activity, but more recently there has also been an expansion in lending provided by non-banks to households and firms. In the EU, the volumes of such non-bank lending remain more modest than in some other major jurisdictions, but the growth rates have been quite important.

Banks also often partner up with non-banks in lending business. Part of this drive could be due to regulatory reform that may induce banks to focus on certain activities and reduce others as they optimise their balance sheets for the Basel III. On paper, these partnerships seem beneficial to both banks and non-banks as they combine banks' strengths in infrastructure, experience, risk management, and regulatory issues with non-bank partners' strengths in customer acquisition, product development, and user experience.

The question then arises whether the regulatory boundaries should be extended to cover also non-bank lenders. IIn the EU, non-bank lenders are regulated even if they are not classified as credit institutions. Insurance companies, which are regulated under Solvency II, have taken on some lending activities. Investment firms are covered by the new Investment Firms Directive (IRF/IRD), with the largest ones being classified as credit institutions. And alternative investment firms have their own standards and rules, including recently updated loan origination guidelines. But there are also many new players in the market, including Fintechs, which are not always regulated as financial intermediaries. All in all, going forward I think that, while keeping proportionality in mind, we should heed our usual catchphrase of "same risks, same regulation". This is to guarantee level playing field between banks and non-banks, to make sure that consumer protection and access to finance at a fair price is respected, and to satisfy that financial stability risks are properly addressed.

The arrival of new players to the lending market is as such a welcome development, since from the borrowers' perspective increased competition should improve access to finance and drive down lending margins. At the same time, there are also risks. First, lenders which are not regulated as credit institutions may not apply equally prudent lending standards as their

[1] See the work of FSB on NBFI, while one of the BCBS' strategic priorities for 2023-24 is the development of additional guidance with regards to banks' interconnections with (NBFI). On cyber-risk, see BCBS' standards on cyber resilience for financial market infrastructures and oversight expectations for critical service providers. On crypto-assets, the FSB recently published global regulatory framework for crypto-asset activities while the BCBS is incorporating the prudential treatment of banks' exposures to crypto assets in the consolidated Basel Framework

competitors in the banking sector. On the one hand, credit may be extended to less-creditworthy borrowers, creating higher default risks at the downturn. On the other hand, creditworthy borrowers may be charged excessively high fees and interest rates, leading to lower investment and slower economic activity. Second, in case non-banks were to capture meaningful market share in some lending segments, such as consumer credit or SME lending, the risk that many of them could withdraw simultaneously from the lending market, in case of economic downturn or market stress, could create unforeseen financial stability risks. Third, questions can also be asked about their resilience to cyberattacks, their ability to protect sensitive customer data and to comply with the anti-money laundering and customer identification rules. Fourth, the shareholders of some non-bank lenders may also follow different, more short-term incentives than their peers in the banking industry. Their ability to provision for expected losses and withstand unexpected losses may be weaker than that of banks which are experienced in managing risks throughout the full credit cycle. And finally, we have seen recently how even closed-end funds which prevent investors from withdrawing funds on a short notice have experienced large-scale redemptions, creating unexpected liquidity risks that these structures were precisely designed to avoid.

We also need to be aware of the interconnections between banks and their non-bank competitors. In the event of stress, significant ownership or funding links may create channels of contagion from non-banks to banks. In the EU, we observe that non-bank financial institutions are major owners of bank-issued debt securities, while banks extend substantial amounts of loans and repo funding to non-banks. EU banks also have growing off-balance sheet links to non-banks in the form of undrawn credit lines and guarantees. We saw during the great financial crisis that when such off-balance sheet commitments crystallised, many banks were forced to take non-performing exposures on their balance sheets which then necessitated large-scale recapitalisations, de-leveraging of performing exposures, or both. Therefore, it is important that there is sufficient transparency about the nature and extent of the links between banks and their non-bank partners and counterparties.

Finally, on- and off-balance sheet linkages may allow non-banks to indirectly access the public safety nets that are made exclusively available for regulated credit institutions, such as public deposit insurance schemes and central bank liquidity facilities. It is important that borrowers from non-bank lenders are fully aware that these players – although typically less leveraged thank banks and funded by long-term investors in closed-end structures – are not operating under the same safety nets and access to emergency liquidity facilities than credit institutions. All in all, close monitoring of these developments and cooperation between regulators and supervisors is necessary to ensure that the risks are quickly identified and appropriately managed.

Digitalisation and the increase in ICT risk: the role of DORA

The second area where we have experienced momentous transformation in the past years relates to the increased operational interconnectedness between financial entities and ICT third-party providers, and the reliance of financial entities on their services. Financial institutions themselves have also become more technologically complex, where legacy applications coexist

with more innovative and sophisticated systems and technologies. The provision of financial services itself is increasingly taking place through digital rather than traditional channels increasing the risks from system failures, cyber attacks or other disruption. To this extent, events at Silicon Valley Bank last year highlighted how digitalisation has indirectly increased liquidity risk, as deposits have become more volatile in digitalised banking, and can move faster than before. Finally, geopolitical tensions and digital financial crime are also playing an increasing role in the technological and digital space, leading to additional cyber and information security threats, including the risk of DDoS attacks, as well as increasing risks of fraud.

In this context, cyber incidents may result in service disruptions, which may become more severe, due to increased complexity and interconnections. This is evidenced by the EBA Risk Assessment Report issued at the end of last year, which shows that cyber risk and data security continue to be by far the most prominent driver of operational risk for EU banks, which reported a growing number of new ICT risk events. More than half of the banks noted to have been victim of at least one successful cyber-attack in the first half of 2023. Ultimately, increased risks stemming from a pervasive use of ICT technologies have the potential to impact financial entities' capabilities to provide critical services, thus endangering EU financial stability.

Against this backdrop, European legislators introduced the Digital Operational Resilience Act (DORA), which became into force in January 2023, establishing a comprehensive framework for digital operational resilience for financial entities, harmonising requirements which were spread across different sectoral legislation. The introduction of DORA also brings a key novelty, as it assigns to the EBA and its sister ESA authorities, EIOPA and ESMA, oversight responsibilities over those third-party ICT service providers that will be designated as critical (CTPPs – Critical Third-Party Providers).

The full applicability of DORA from January 2025 will contribute to re-shaping the activities of the ESAs and the priorities of EU banking supervisors as well, which would also require significant cooperation between financial supervisors and the ESAs. For a start, let me say that together with our colleagues at ESMA and EIOPA we are working as a single team to ensure that the oversight framework will be operational from next year. This requires specific attentions in different aspects. First, the identification and designation of the critical providers: this process will necessarily rely on completeness of information and quality of data. This is why the ESAs recently launched a voluntary "dry-run" exercise to support financial entities to prepare for the submission of the registers of ICT third-party providers information and identify and address any potential issues before the first official submission in early 2025, and to test the reporting process.

Second, one of the main novelties of DORA is that the oversight conducted by the ESAs will complement the supervision on financial entities by competent authorities. As such, this will require close and continuous cooperation between the ESAs and competent authorities. On the one hand, competent authorities will provide resources to oversight activities conducted by the Lead Overseer, allowing to leverage on existing skills and experience on ICT risk supervision. On the other, financial supervisors and the ESAs must coordinate their actions and share information: while the Lead Overseer can issue recommendations to address any identified

issues, it will be for supervisors to assess the measures taken by the CTPPs based on such recommendations in the context of their supervisory activities. Coordination and continuous communication, ensured by dedicated structures envisaged in DORA like the Oversight Forum, will allow a smooth functioning of the oversight framework and avoid overlaps and duplication of requests to third party providers.

Third, as oversight comes as a new responsibility for the ESAs, it will be essential to progressively build our knowledge of the critical providers (also in terms of their business models and organisational structure) to ensure their procedures, mechanisms and arrangements do not expose the financial entities to unmanageable ICT risk.

Finally, DORA will require a re-design of priorities for banking supervisors as well. Having in mind the four main pillars around which DORA revolves, we expect that more attention will be devoted to i) the assessment of financial entities' plans and actions in ensuring effective and prudent ICT risk management; ii) assess whether financial entities classify ICT-related incidents and cyber threats in accordance with the requirements and report them in a timely manner; iii) review the adequacy of banks' digital operational resilience testing programme and assess the preparedness of significant entities to perform threat-led penetration tests; iv) ensure that ICT services provided by third parties are adequately monitored and the contractual arrangements are in line with DORA requirements.

MiCAR and crypto-assets

The third area where we have seen a large momentum in the recent years is the advent of the crypto industry and its interconnection with the traditional financial system, which has brought forth a unique set of risks. The relentless technological developments and features of crypto ecosystem, coupled with the global reach of certain products are associated to elevated risks, including those related to financial crime area. In addition, technological complexity, market characteristics, and the lack of a strong compliance culture exacerbate the risks to investors.

Crypto markets remain highly fragmented and are characterised by significant volatility. Historical events have demonstrated that it can take from mere hours to a couple days for substantial sums, to vanish, adding a time pressure dimension to the management of such risks.

There is yet another important consideration: for an extended period, the prevailing narrative in the crypto industry have been constructed upon apprehensions of economic instability, distrust towards established financial entities, and the allure of technology alone as a gateway to newfound wealth. From this perspective, the transition to a compliance culture akin to that observed in the traditional financial sector may represent a considerable paradigm shift for those entities active in the crypto market.

In this context, the Markets in Crypto-Assets Regulation, or MiCAR, is a major step forward for the development of a safe, sound, and innovative crypto-asset market in the EU, and a clear signal of our commitment to embrace the opportunities and challenges of the digital transformation.

However, MiCAR is not the end of the story. It is only the beginning of a new era of crypto-asset regulation, which requires close cooperation and coordination among all the relevant stakeholders, both at EU and at global level.

MiCAR captures a wide spectrum of market players, from new market entrants and crypto-asset service providers to already established financial institutions such as credit and e-money institutions. MiCAR assigns different roles of the national competent authorities, EBA and ESMA to address the risks arising from different products and services. While the EBA has its supervisory mandate towards issuers of significant ART and significant EMT, issuers of non-significant tokens will still remain supervised by national authorities. On the other hand, ESMA is assigned with a specific mandate towards entities that provide crypto assets services. This diversity of actors and activities requires effective collaboration at EU level between competent authorities, the EBA, and ESMA in the following areas.

- Building supervisory capacity, sharing supervisory practices, fostering convergent approach both at the authorisation phase and during the ongoing supervision will ensure a level playing field and avoid regulatory arbitrage and forum shopping.
- Market monitoring and coordinated actions against unauthorised activities in the EU, to identify and address timely potential risks and breaches of MiCAR.
- Identifying common areas of focus and alignment in supervisory priorities among competent authorities across the EU, to ensure a coherent and proportionate approach to supervision of crypto assets.
- Ensuring continuity and stability in supervision is key, especially in the context of EBA's direct supervisory role towards significant tokens and the transition of supervisory responsibilities from the competent authorities to the EBA.

In terms of supervisory priorities, the EBA sees that emphasis should be placed on the following areas:

- Internal governance and risk management: a solid and effective framework for internal governance and risk management is essential to establish a compliance and risk culture
- Financial resilience: adequate capitalisation, alongside the prudent management of the reserve of assets are necessary to mitigate risks to financial stability and protect holders.
- Technology risk management: the centrality of technology in this sector requires enhanced scrutiny by supervisors.
- Financial crime risk management, including ML/TF risk and sanctions evasion: due to certain characteristics pertaining to transaction speed or anonymity, crypto-assets are susceptible to being exploited for illicit financial activities.

Depending on the business models and the levels of maturity of the entities, the application of the supervisory priorities may need to be adapted. For instance, credit institutions that are already familiar with the regulatory and supervisory framework should ensure they adequately manage the specific risks associated with this sector, especially in terms of ICT and financial crime risks. On the other hand, new market entrants that are not previously regulated should, in

addition to the mentioned priorities, establish a sound and transparent relationship with their supervisors.

To conclude, the challenges outlined before have a global and interconnected character, calling for coordinated supervisory actions at a global level, and the EBA is actively engaged and committed to such global dialogue to address the cross-border challenges in the regulatory and supervisory landscape.

Thank you for your attention and I am of course ready to answer any questions you may have.