Overview

The European Commission (the Commission) adopted on September 24, 2020, a new digital finance package that includes legislative proposals to: (1) regulate crypto-assets and crypto-asset service providers; (2) run a pilot regime for market infrastructure based on distributed ledger technology; and (3) promote increased cybersecurity resilience across the financial sector.

The initiatives build on the work carried out in the context of the 2018 FinTech Action Plan[1] and the subsequent initiatives by the European Parliament and European supervisory authorities.[2]

Below is a summary of the key takeaways on each of the proposals, their potential impacts for the financial sector if adopted in their current shape as well as how the EU approach compares to the one in the United States.

Dedicated EU Framework for Crypto-Assets

The Commission’s proposal for a Regulation on Markets in Crypto-assets (MiCA) creates a new regulatory framework for crypto-assets which are not currently addressed under existing EU financial services legislation. It covers crypto-assets categorized as utility tokens, and stablecoins (the latter are split into asset-referenced tokens and e-money tokens under the proposed Regulation), as opposed to assets categorized under other EU rules as financial instruments, as well as those covered under the EU electronic money directive.[3] As its title suggests, the proposed regime, in particular requirements for crypto-asset service providers, has a number of common features with the current EU securities markets/investment services legislation (namely, MiFID II). However, MiCA represents a substantial effort to grapple with the unique characteristics of different types of crypto-assets, and a recognition that these assets do not fall neatly under existing categorizations as financial instruments or currency equivalents.
MiCA will apply to issuers of covered crypto-assets as well as to crypto-asset service providers. It sets out transparency and disclosure requirements for issuers of utility tokens who wish to offer these crypto-assets to the public in the EU or seek an admission to trading. Meantime, crypto-asset service providers and issuers of stablecoins will face, when MiCA is adopted, rather extensive requirements relating to authorization, supervision, operation, organization and governance.

In order to provide their services in the EU, crypto-asset services providers will need to be established in the Union and get authorized by a regulator of the Member State of their establishment. Service providers will have to meet a number of prudential and organizational requirements to obtain authorization. MiCA also includes requirements for specific crypto-asset services, such as custody of crypto-assets, trading platforms, crypto-to-fiat and crypto-to-crypto exchange, etc. Once authorized, service providers will be able to pursue business throughout the EU under the so-called EU passport.

Similarly, issuers of asset-referenced tokens will only be able to offer their tokens to the public in the EU/get admitted to trading on a trading platform if they are established and authorized in the EU and publish an approved white paper. An issuer of asset-referenced tokens will need to fulfill numerous requirements to obtain an authorization, including capital and governance requirements, rules on conflicts of interest, rules on the stabilization mechanism and the reserve of assets backing the asset-referenced tokens, requirements for the custody and investment of the reserve assets, etc.

MiCA also creates the categories of: "significant asset-referenced token" and "significant electronic money tokens" to delineate tokens of these types with the potential to reach extremely broad audiences, make use of widely-used electronic platforms, be used in substantial numbers of transactions, and other criteria. These "significant" tokens will be subject to enhanced supervision and other requirements.

MiCA splits the supervision of market participants between national regulators and the European Banking Authority (EBA). Crypto-asset services providers and issuers of asset-referenced/e-money tokens will be supervised by the regulator of their home Member State. Meantime, the EBA will authorize and directly supervise issuers of significant asset-referenced tokens; it will also participate in the supervision of issuers of significant e-money tokens.

MiCA will apply directly throughout the entire EU and will not need to be implemented into the national law of each Member State. This should provide more clarity and legal certainty to issuers of crypto-assets and crypto-asset service providers which are currently exposed to specific national regimes. At the same time, MiCA risks creating "Fortress Europe" in a business sector that is fundamentally based on cross-border operations. Some non-EU service providers might be able to rely on reverse solicitation (similar to MiFID II) and the Commission could add an equivalence regime to MiCA in the future. However, if MiCA is adopted in its current form, most crypto-asset service providers and issuers of stablecoins will likely require a physical presence in the EU and will have to bear the associated organizational and compliance costs.

The majority of MiCA’s provisions will take effect 18 months after its effective date, except for those governing electronic money tokens, which will take effect immediately in conjunction with the EU electronic money directive, as applicable.

A Sandbox Approach to DLT Market Infrastructure

Along with MiCA, the Commission proposed a regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLT).

The pilot regime represents a so-called “sandbox” approach that allows temporary derogations from existing rules. The goal is to enable regulators to gain experience on the use of DLT in market infrastructures, while ensuring that they deal with risks to investor protection, market integrity and financial stability.

Specifically, the pilot regime provides for requirements and exemptions regarding DLT multilateral trading facilities, DLT securities settlement systems and DLT market infrastructures. It also sets out the conditions for specific permissions to operate a DLT multilateral trading facility and a DLT securities settlement system.

The pilot regime will put in place certain safeguards, such as limitations on the types of financial instruments that can be traded.

(Much) More About the Same, A Boost to Cybersecurity Resilience

Cybersecurity resilience is a precondition to sustainable innovation in an increasingly digitalized financial sector. Cybersecurity awareness elevated to board-level in recent years. This is due both to: (i) the exponential increase (in absolute number and in severity) of cyberattacks and (ii) EU regulatory developments in this area. The sector had to digest a number of minimum harmonization directives (NIS),\(^4\) PSD2\(^5\) and principle-based regulation (such as GDPR)\(^6\) with a cybersecurity component. Such multiplication of rules and the room left for substantial diverging approaches across member states lead to a patchwork that is difficult to navigate. As an example, a credit institution operating in a cross-border context may be designated as an operator of essential services in one country under the NIS Directive but not in another. Existing consistency mechanisms under the NIS Directive have often fallen short to resolve practical issues such as the need to go through multiple sets of national regimes to assess the severity of cyber incidents.
The proposal for a regulation on digital operational resilience for the financial sector[7] (DOR), if adopted, is seeking to bring the EU financial sector cyber preparedness to the next level. The two key enhancements that DOR might bring, in its current shape, are:

- First, and probably foremost, DOR promotes cybersecurity resilience widely, i.e., to many, not to say most, of the financial entities regulated at Union level.[8] Here, DOR shifts from the NIS Directive* approach that was focusing solely on a limited number of essential operators.[9] DOR still includes some softening measures such as: (i) de minimis thresholds allowing microenterprises to stay light on requirements; or (ii) the introduction of a proportionate approach to compliance with some measures being imposed only on critical/significant actors. Nevertheless, the wide reach represents a policy shift.

- Second, DOR is building a comprehensive (and prescriptive) cyber resilience ecosystem around:
  - ICT risk management: DOR incorporates (with some EU-added flavor) internationally recognized best practices and standards of ICT cyber risks management (such as the US NIST framework) into an EU regulation;
  - Harmonized reporting of major cyber incidents: that includes communication requirements (under specific deadlines) for entities towards their regulators but also affected users and clients;
  - Testing: by introducing specific requirements for regular (at least every 3 years) and proportionate (penetration) testing to be conducted by duly approved testers with an oversight from the relevant supervisory authorities;
  - Tools for managing ICT third-party risks: ranging from: (i) precisely identified mandatory due diligence on providers to (ii) set of required terms in contractual arrangements with third-party to be developed by the supervisory authorities (going deeper than existing outsourcing frameworks), reducing the bargaining power of ICT providers;
  - An opportunity for cyber threat information and intelligence sharing: that includes the requirement to develop information-sharing arrangements framing the cooperation within industry members, including with public authorities and in compliance with competition and privacy laws.

The ambition of the EU with DOR should be recognized; DOR has great potential achieving higher cybersecurity resilience in the financial sector. It will require investments for the sector to comply. Whether or not DOR will be a success would depend not only on its adoption in its current format but also on future work that DOR commands. Indeed, upon adoption, supervisory authorities will still have to come up with methodologies, standards, forms, templates, procedures and explore future developments, such as the set-up of a single EU hub centralizing incident reports. It is however likely that the financial sector will be used as a test case. Further spread in other sectors of our digitally-driven economies may follow should the test be positive.

### How Is the EU Doing Compared to US?

The EU digital finance package is far-reaching with the EU as frontrunner in many ways; MiCA, DLT and DOR stand in some contrast to more modest and disjointed efforts in the US.

- MiCA's comprehensive regulatory scheme for three specific types of crypto-assets (utility tokens, asset-referenced stablecoins, and electronic money tokens) fills a critical gap while demonstrating unique considerations applicable to these types of tokens. By excluding financial instruments on the one hand and e-money on the other, MiCA stands firmly for the proposition that the crypto-assets it regulates are a different category of asset; this departs from the US approach, which depends overwhelmingly on whether a crypto-asset constitutes a “security” under US law. While the US has been a leader in anti-money laundering regulation concerning crypto-assets, having issued guidance applying the US Bank Secrecy Act to crypto-assets years before the 5th Anti-Money Laundering Directive (AMLD5) did the same in the EU, the US has lagged in terms of similar regulatory clarity in other areas involving crypto-assets. MiCA creates a comprehensive regulatory scheme with clear expectations that can be understood and met.

MiCA also recognizes that with respect to utility tokens, asset-referenced stablecoins, and electronic money tokens, **investors and users are different communities of people**, meaning that while investors may benefit from one type of protection of the type typically reserved for investors, users may benefit from another type of protection more typically categorized as consumer protection.

- In the same vein, the EU’s proposal of a regulatory sandbox for DLT projects mirrors more closely the UK FCA approach of using a sandbox to encourage innovation, as opposed to that of US regulators who have resisted the use of formal regulatory sandboxes to date.

- Finally, while the US has been a frontrunner in the promotion of threat information sharing in general, including in the financial sector with the set up more than 20 years ago of FS-ISAC, DOR’s sector-specific prescriptive provisions is a very different setup.

Non-EU based crypto-asset developers and operators of crypto-asset service providers may not like elements of the digital finance package (and there are provisions on which much consideration and debate should be focused), they are at least clear, understandable, and consistently applicable across projects. Whether this is the best possible way to promote a digital single market for finance with the EU as an innovation hub remains to be seen.


[8] See Article 2 of DOR listing credit institutions, payment institutions, electronic money institutions, investment firms, crypto-assets service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens, central securities depositories, central counterparties, trading venues, trading repositories, managers of alternative investment funds, management companies, data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, institutions for occupational retirement pensions, credit rating agencies, statutory auditors and audit firms, administrators of critical benchmarks, crowdfunding service providers, securitization repositories, ICT third-party service providers.

[9] We should remind ourselves that the consequences of NIS go beyond the designated operators of essentials services within the financial sector, as those operators are typically passing some of the NIS compliance burden onwards, within the entire supply chain. One another note, the interplay between DOR and NIS is a topic that will need specific attention considering the potential for overlap between the two frameworks for those financial entities (or providers) captured by both.

Practices
Privacy & Cybersecurity

Financial Services

Blockchain & Cryptocurrency

© 2020 STEPTOE & JOHNSON LLP. ALL RIGHTS RESERVED. ATTORNEY ADVERTISING.