Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Global Blockchain Business Council

Fintech Updater – February 2020

EU, UK and US regulatory developments

FinTech

EU

EIOPA issues final guidelines on outsourcing to cloud service providers

The European Insurance and Occupational Pensions Authority (**EIOPA**) has published final guidelines on outsourcing to cloud service providers (**CSPs**). EIOPA identified the need to develop its guidance in the context of the analysis it performed to answer the European Commission FinTech Action plan, in addition to discussions with stakeholders.

Before the adoption of the final guidelines, EIOPA conducted a public consultation on the draft guidelines which launched on 1 July 2019 and ended on 30 September 2019, and also considered, and followed closely, the European Banking Authority's (**EBA**) final report on guidelines on outsourcing arrangements, which was published in February 2019.

Under the new guidelines, insurers will be required to comply with new obligations that will impact cloud outsourcing arrangements. The guidelines apply to individual insurers and reinsurers as well as their groups, and also provide guidance to competent authorities on how to apply the guidelines.

The guidelines aim to provide clarification and transparency to market participants to avoid potential regulatory arbitrages, as well as also fostering supervisory convergence regarding the expectations and processes applicable with respect to cloud outsourcing.

In harmony with the both the EBA's guidance and the Solvency II Directive, the guidelines differentiate general outsourcing from outsourcing of critical or important operational functions or activities, placing more onerous requirements on the latter.

The guidelines cover the following key areas:

- criteria to determine whether or not cloud services fall within the scope of outsourcing;
- contractual requirements;
- governance of cloud outsourcing requirements, which include documentation and notification;
- pre-outsourcing analysis, which includes criteria to help assess whether a cloud outsourcing arrangement relates to a critical or important operational function or activity;
- management of access and audit rights; security and data systems; specific information security requirements for critical outsourcing arrangements that must be included in the contract; monitoring and oversight mechanisms of cloud outsourcing arrangements; and clearly defined exit strategies for critical outsourcing agreements;
- principle-based instructions on how to conduct thorough risk assessment of critical outsourcing arrangements; and
- instructions on how to provide written notification to the supervisory authority with details of the critical outsourcing arrangement.

The guidelines will apply from 1 January 2021 to all cloud outsourcing arrangements which are entered into or amended on or after this date. Undertakings will have until 31 December 2022 to review and amend accordingly existing arrangements in order to ensure compliance. Undertakings which are not able to review their critical outsourcings by 31 December 2022 must notify the supervisory authority, providing details of how they intend to complete their reviews in a reasonable time.

Date: 6 February 2020

EU	**EIOPA SupTech strategy**	EIOPA has published a document that aims to define its supervisory technology (**SupTech**) strategy, which will cover prudential and conduct of business supervision, policy, and interaction with entities, for the insurance and occupational pensions sectors. SupTech is defined as "the use of technology by supervisors to deliver innovative and efficient supervisory solutions that will support a more effective, flexible and responsive supervisory system" by EIOPA. The document sets out EIOPA's own SupTech strategy, namely: "To promote the use of technology by supervisors to deliver innovative and efficient supervisory solutions that will support a more effective, flexible and responsive supervisory system by: • implementing a platform for ongoing exchange of knowledge and experience to promote a culture of innovation and initiative between supervisors; and • organising and endorsing the analysis of potential development tools chosen from the list identified by supervisors and considering the criteria and objectives described above, and to implement them after a positive decision following the analysis phase." Once an idea is identified, EIOPA explains that implementation will follow a step-by-step approach, which begins with an initial analysis phase to improve understanding of the idea (including the tool's objective, the input needed and if this is available, the output expected, and how it fits into proportionate and risk-based supervision). EIOPA may also sponsor a SupTech event during this phase, where it might cooperate with external stakeholders in order to develop specific fintech proofs-of-concepts for financial supervision. The key deliverable of this phase should be a recommendation whether or not to implement the tool. The second phase is made up of planning and development, where development might be internal, external or mixed, and even use new formulas such as SupTech accelerators. Ultimately, the analysis will be presented to EIOPA's Board of Supervisors (**BoS**), who will decide whether the idea should progress to the planning and development phase. The BoS retain the right to cancel a project at each phase and will also be responsible for deciding to analyse any new ideas. Date: 12 February 2020
EU	**Italian Ministry launches a public consultation on fintech sandbox**	The Italian Ministry of Economy and Finance has launched a public consultation on a draft ministerial decree which would implement the mandate received by the Italian legislature to create a regulatory sandbox to trial fintech-related activities within the financial, credit, and insurance sectors, and also establish a FinTech Committee. Under the draft decree, the proposed activities eligible for the sandbox would include regulated or non-regulated activities that: • use technologies that contribute to the innovation of banking, financial, and insurance products and services; • need an exemption from regulations or guidelines adopted by the supervisory authorities or require a joint testing and assessment from the supervisory authorities; and • bring added value in terms of (i) benefits for final users improving the quality of services, access conditions, competition, costs, availability and protection; (ii) general efficiency of market participants and the financial system; or (iii) more efficient and less burdensome compliance with financial regulations. The proposed maximum testing period for any project is 18 months, although this may be extended if the applicant requests. Applicant entities may informally discuss their intended

		projects with the FinTech Committee before submitting their applications to the sandbox. The draft decree proposes that the FinTech Committee: • monitors the evolution of fintech so that it can set goals, define programs, and foster the development of fintech, at the same time as drafting guidelines, promoting best practices, and supporting initiatives to reduce and streamline administrative requirements; • increases interactions between market participants, industry bodies, and regulators (both national and foreign); and • collaborates with foreign regulators and exchanges relevant information on fintech matters. The deadline for submitting responses to the public consultation on the draft decree is 19 March 2020. Date: 19 February 2020
EU	**Russian authorities agree to ban cryptocurrencies**	The Russian Central Bank and the Federal Security Service (**FSB**) have finally agreed to ban cryptocurrencies altogether, after failing to come to any agreement regarding crypto regulation. Although the FSB was initially in favour of regulation, it has backed the Central Bank's idea to ban the issuance and use of cryptocurrencies as a means of payment. It is expected that a Bill in this regard will pass through the Russian parliament in spring this year. Despite this ban on cryptocurrency payments, the Central Bank and FSB will leave exchanging cryptos to fiat currencies open, provided that any trading takes places through specialised authorised operators. However, crypto owners wishing to cash out their cryptos or simply hold them will undergo identification scrutiny as the FSB tries to identify all crypto owners in Russia, no matter the value they derive from these assets. Failure to comply may result in criminal liability imposed by the FSB. Notwithstanding the agreement to outlaw cryptocurrency payments, the Central Bank is pursuing blockchain and has proposed a legal framework for tokenising assets. This month, it also piloted a blockchain platform that would allow external parties to develop hybrid tokens. The stance adopted by Russia is similar to that in China, where similar bans on digital assets exist but the country is pursuing the technology underpinning the cryptocurrencies. Given this new ban on digital currency, it is likely that Russia will experience a sudden decline in the use of cryptocurrencies. Date: 21 February 2020
EU	**European Commission announces consultation on EU Digital Finance Strategy**	The European Commission (**Commission**) has published a banking and finance newsletter, providing further information on the future EU Digital Finance Strategy. The EU's Digital Finance Strategy aims to ensure that the financial services regulatory framework within the EU promotes digital finance, at the same time as regulating proportionately the risks presented by digitalisation and new technologies. The Commission intends to launch a public consultation from March to May 2020 in order to get feedback from consumers, companies and national authorities. In addition, the Commission is also planning a number of outreach events in several Member States in order to invite views on key political and ethical questions that digital finance raises, and how the EU might address them. Key questions include: • How can businesses and consumers both benefit from digital finance while also

		remaining protected? • How can innovative technologies be regulated without being killed off? • How can a level playing field be ensured between banks, fintechs and bigtechs? The opinions and feedback received will help determine the key priorities to feed into the strategy, which the Commission plans to present in Q3 of 2020. The newsletter follows a package of measures already started by the Commission to develop the strategy, which include public consultations on the future EU legislative framework for markets in cryptoassets and the establishment of an enhanced framework for digital operational resilience in the financial sector. The deadline to submit comments on such consultations is 19 March 2020. Any legislative proposals that the Commission thinks are necessary will be published in Q3 2020, presumably in conjunction with the launch of its Digital Finance Strategy. Date: 26 February 2020
EU	**Protecting the European financial sector: the Cyber Information and Intelligence Sharing Initiative**	The European Central Bank (**ECB**) has published the introductory remarks from Fabio Panetta (ECB Executive Board member) at the fourth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures. Key points in the remarks include: • the ECB's 2018 cyber resilience oversight expectations are now being followed by financial infrastructure operators across Europe; • the European Framework for Threat Intelligence-based Ethical Red Teaming has been adopted by the ECB in its oversight capacity and, at the national level by Belgium, Denmark, Germany, Ireland, Italy, the Netherlands, Romania and Sweden. It is close to adoption in Norway and Finland; and • the ECB is launching the Cyber Information and Intelligence Sharing Initiative. This initiative will allow the most important financial infrastructures to share vital technical information among themselves using an automated platform. Members will create a trusted community where they will meet to discuss cybersecurity threats and share related intelligence and best practices. Date: 27 February 2020
UK	**BoE launches the COP26 private finance agenda**	The Bank of England (**BoE**) has published a press release announcing the launch of the 2020 UN climate change conference (**COP26**) private finance agenda. COP26 is scheduled take place in Glasgow in November 2020. The COP26 agenda has been designed to help private finance support the whole economy transition to net zero. The objective is that every professional financial decision will take climate change into account. At the launch event, Dr Mark Carney, the outgoing Governor of the BoE, explained in a speech that achieving net zero will require a whole economy transition, where every company, bank, insurer and investor will have to adjust their business models, adding that this could turn an existential risk into a great commercial opportunity. By developing the right framework for reporting, risk management and returns, these climate change considerations will be embedded, which in turn will help finance a whole economy transition: • reporting - the aim is to help the private sector to refine and implement the Task Force on Climate-related Financial Disclosures (**TCFD**) by implementing a common framework built on TCFD and to commit to pathways to make climate reporting mandatory; • risk management - the aim is to ensure that both firms and investors can

		measure and manage the risks in the transition to a net zero world; and • return - the aim is to help both firms and investors identify the opportunities in the transition to net zero. A summary of these overarching goals can be found here. In his speech, Dr Carney outlined specific actions under each of these goals. The full strategy will be published when Dr Carney's term as Governor ends in March 2020 and he takes up his roles as UN Special Envoy for Climate Action and Finance, and Prime Minister Johnson's Finance Adviser for COP26. Date: 27 February 2020

US	**"Crypto Mom" proposes 3-year safe harbor for token projects**	In a speech to the International Blockchain Congress on February 6, 2020, Securities and Exchange (**SEC**) Commissioner Hester Peirce, sometime referred to as "Crypto Mom," has proposed a three-year safe harbor for virtual currency token projects. The safe harbor would exempt (i) the offer and sale of tokens from the provisions of the Securities Act of 1933, other than the anti-fraud provisions, (ii) the tokens from registration under the Securities Exchange Act of 1934 and (iii) persons engaged in certain token transactions from the definitions of "exchange," "broker" and "dealer" under the Securities and Exchange Act.
		
		To date, the SEC's policy has been to enforce (perhaps selectively) against virtual currency companies that have raised funds through token sales that have appeared to violate US federal securities laws. Many of these companies have argued that while their sale of tokens may seem like securities offerings at first, the ultimate intent is to create a decentralized network where the tokens can be used in exchange for a service or product and not merely as an investment.
		
		Peirce described the current "regulatory Catch 22" that has arisen – "Would-be networks cannot get their tokens out into people's hands because their tokens are potentially subject to the securities laws. However, would-be networks cannot mature into a functional or decentralized network that is not dependent upon a single person or group to carry out the essential managerial or entrepreneurial efforts [that is the hallmark of securities] unless the tokens are distributed to and freely transferable among potential users, developers and participants of the network." Peirce's proposal would give these companies a three-year grace period to achieve such network decentralization.
		
		This is also not the first time the SEC has grappled with this issue. For example, William Hinman, SEC Director of Corporation Finance, has previously described how the virtual currency Ether may have originally started as a security but in later years the network evolved and Ether was decentralized enough that it could no longer be considered a security.
		
		Peirce's proposal includes a set of strict requirements that would have to be met in order for a token issuer to rely on the safe harbor. The requirements include the following:
		
		• the initial development team must intend for the network on which the token functions to reach network maturity – defined as either decentralization or token functionality – within three years of the date of the first token sale and undertake good faith and reasonable efforts to achieve that goal;
		
		• the team would have to disclose key information on a freely accessible public website including:
		
		  • the source code and transaction history
		
		  • total number of tokens to be created, the number to be issued in the initial allocation and the release schedule of the tokens
		
		  • information regarding how tokens are generated and mined
		
		  • process for validating transactions and the consensus mechanism

- governance mechanisms for implementing changes to the protocol
- the plan and timeline of development of the network
- how many tokens each member of the development team owns and disclosure when they sell more than 5% of their tokens

- the token must be offered and sold for the purpose of facilitating access to, participation on, or the development of the network;
- the team would have to undertake good faith and reasonable efforts to create liquidity for users;
- the team would have to file a notice of reliance on the SEC EDGAR database; and
- it is noteworthy that the proposed safe harbor includes a conduct standard of "good faith and reasonable efforts." The team does not have any fiduciary duty to the token holders, although anti-fraud rules still would apply.

Despite many of the safe harbor's required disclosures lining up with what is disclosed anyway in countless token project whitepapers, potentially problematic for nascent token projects is the requirement to publish source code that could be considered proprietary and confidential, especially during the competitive development timeframe that the safe harbor is intended to protect.

While Peirce's safe harbor proposal may be a great step for the SEC in providing more regulatory clarity in the digital asset space, there is still a long road ahead for any type of proposal to eventually become a final rule. As Peirce herself states, the final rule, if any, after deliberation and comment by the SEC and industry participants, may look nothing like what she has laid out in this speech.

Date: 6 February 2020

International developments

G20

G20 wants countries to adopt strict crypto rules

In order to combat money laundering and terrorist financing, as well their wider macroeconomic implications, the Group of Twenty (**G20**) has published a communiqué urging more countries to implement regulations compelling cryptocurrency exchanges to collect customer information.

In making this appeal, the G20 referred to the FATF standards adopted in June 2019 on virtual assets and related providers and urged countries to implement such guidelines to help stop financial crimes.

The FATF's so-called travel rule, which requires virtual asset service providers such as cryptocurrency exchanges "to obtain, hold and transmit required originator and beneficiary information in order to identify and report suspicious transactions, monitor the availability of information, take freezing actions and prohibit transactions with designated persons and entities", is designed to limit money laundering by extensively collecting such identifying information with respect to cryptocurrency transactions. Having already endorsed the FATF's guidelines, the G20 is now trying to establish further support for the initiative.

The G20 also reiterated its statement made in October 2019 supporting the regulation of "global stablecoins" (cryptocurrencies that are backed by specific assets such as fiat currencies or commodities, and not backed by sovereign governments) and other similar arrangements, saying that "such risks need to be evaluated and appropriately addressed before they commence operation". Furthermore, it supports the FSB's efforts to develop regulatory recommendations in relation to these arrangements and looks forward to reports by the FSB, FATF, and the International Monetary Fund.

Date: 22 February 2020

Financial Stability Board (FSB)

There has been no reported activity.

Bank for International Settlements (BIS)

There has been no reported activity.

International Organisation of Securities Commissions (IOSCO)

IOSCO publishes key considerations for regulating crypto-asset trading platforms

The International Organization of Securities Commissions (**IOSCO**) has published a final report on issues, risks and regulatory considerations relating to crypto-asset trading platforms (**CTPs**). In preparation for this report, IOSCO first issued a consultation report on 28 May 2019 which surveyed the approaches currently being undertaken or considered by member jurisdictions in relation to CTPs.

The key considerations from the final report relate to:

- access to CTPs;
- safekeeping of participant assets, including custody arrangements;
- identification and management of conflicts of interest;
- transparency of operations;
- market integrity, including the rules governing trading on the CTP, and how those rules are monitored and enforced;
- price discovery mechanisms; and

- technology, including resiliency and cyber security.

IOSCO states that many of the issues related to the regulation of CTPs are common to traditional securities trading venues but may be heightened by the business models used by CTPs. It reasons that where a regulatory authority has determined a crypto-asset is a security and falls within its remit, the basic principles or objectives of securities regulation should apply.

IOSCO will continue to monitor the evolution of the markets for crypto-assets to ensure the issues, risks and key considerations identified in this report remain relevant and appropriate.

Date: 12 February 2020

Committee on Payments and Market Infrastructures (CPMI)

There has been no reported activity.

Basel Committee on Banking Supervision (Basel Committee)

There has been no reported activity.

Financial Action Task Force (FATF)

There has been no reported activity.

World Economic Forum

There has been no reported activity.