NORTON ROSE FULBRIGHT

Global Blockchain Business Council

Fintech Update

Norton Rose Fulbright LLP - October 12, 2020 - Private and confidential

Global, EU, UK and US Regulatory developments

FinTech		
EU	**ECONFIN ministers issue joint statement on stablecoins**	An informal meeting of the EU Ministers for Economic and Financial Affairs (ECOFIN) took place in Berlin, as part of which the ECONFIN ministers of Germany, France, Italy, Spain and the Netherlands issued the following joint statement on stablecoins. The ministers expect this to be reflected in the Commission's upcoming legislative proposals on crypto-assets. In the press conference, the ministers set out their approach which focuses on monetary sovereignty, financial stability and consumer protection. "1. As the Council and the Commission outlined in its joint statement on 5 December 2019 no asset-backed crypto-assets (so called "Stablecoins") arrangement should undermine financial stability, safety and efficiency of payment systems, fair competition and the existing financial and monetary order as well as monetary sovereignty in the European Union. Therefore, all options for handling asset-backed crypto-assets should be put on the table and no global asset-backed crypto-asset arrangement should begin operation in the European Union until the legal, regulatory and oversight challenges and risks have been adequately identified and addressed. 2. We look forward to the regulatory Proposal for Crypto-Assets announced by the Commission for the third quarter of 2020 and fully endorse the Commission's intentions to provide a precise and stable regulatory framework for asset-backed crypto-assets and to prohibit, where appropriate, those that do not meet all the prerequisites. It is of great importance that the objectives of the Proposal of Crypto-Assets are carefully aligned with the objectives of the Retail Payment Strategy to strengthen Europe's influence and consolidating its economic autonomy in the field of payments. 3. In implementing the joint statement, we firmly believe that the regulatory framework for asset-backed crypto-assets in the EU should serve two crucial priorities: on the one hand preserve our monetary sovereignty and address the risks to monetary policy, and on the other hand protect EU consumers. To that end, the EU legislation should be built around the following general principles, appropriately applied to different types of asset-backed crypto-assets: Each unit of asset-backed crypto-asset created shall be pledged at a ratio of 1:1 with fiat currency. The assets eligible for the reserve shall be limited to deposits, deposited in a credit institution approved by the European Union, or for a fraction to highly liquid assets, subject to appropriate safeguards to be put in place. The assets eligible for the reserve shall be denominated in Euro or a currency of a member state of the EU, be held separately from other reserves and be nonconvertible in order to avoid exchange rate risk.

		For asset-backed crypto-assets that are intended to be used widely for payment purposes, users shall have a direct claim on the reserve and the issuer so that the user can redeem, at any moment and at par value, the asset-backed crypto-asset into legal tender. All entities operating as part of an asset-backed crypto-asset scheme in the EU shall be registered in the EU before starting any activity. 4. Moreover, EU legislation should adequately deal with specific issues that asset-backed crypto-assets may give rise to in terms of AML/ CFT and fair competition. All types of service providers in an asset-backed crypto-assets arrangement operating within the EU must meet the requirements of the GDPR." **Published: 11 September 2020**
EU	**AFME publishes paper calling for EU regulatory framework in support of adopting new technology across Europe's capital markets**	On 14 September 2020, the Association for Financial Markets in Europe (AFME) published "European Capital Markets in the Digital Age", a paper calling for a EU digital regulatory framework that promotes innovation and competitiveness amongst capital market participants while ensuring high levels of resilience. The paper recommends the following main objectives in developing this framework: • The framework should be globally consistent and based on global standards; • The EU commission should develop a clear strategic vision promoting uptake of innovative technologies in the financial sector; • The framework should remain technology neutral, principles-based and proportionate to support technology adoption; and • The framework should provide for a competitive and level playing field, adhering to the principle of "same activity, same risk, same regulation". **Published: 14 September 2020**
EU	**Proposed European Regulations on markets in crypto-assets and DLT market infrastructure**	On 23 September 2020 the European Commission published its long-awaited draft regulation on markets in crypto-assets (MiCA), with its accompanying annex and a draft regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLTR). The proposals, which are part of the broader Digital Finance Strategy package, are the first European-level legislative initiatives aiming to introduce a harmonised and comprehensive framework for the issuance, application and provision of services in crypto-assets, and to create a bespoke legal regime for the practical application of DLT in post-trade services. The draft legislative proposals provide a set of prescriptive rules that – once formally adopted – will shape conduct of business in European markets in crypto-assets. The following provides an overview of 10 key things that you need to know about the proposed legislation. 1) Scope and subject matter When formally adopted, MiCA will apply to persons involved in the issuance of crypto-assets, as well as services related to crypto-assets in

		the European Union (EU), which are not regulated by other pieces of European law. As such, the draft legislation sets out rules on transparency and disclosure requirements for the issuance and admission to trading of crypto-assets, the authorisation and supervision of crypto-asset services providers and issuers, the operation, organisation and governance of issuers of asset-referenced tokens and electronic money tokens and crypto-asset service providers, consumer protection rules as well as measures to prevent market abuse and to ensure integrity of markets in crypto-assets. DLTR will provide a regulatory framework for the development of DLT multilateral trading facilities (DLT MTFs) and DLT securities settlement systems, including for granting and withdrawing specific permissions and exemptions. 2) Definitions Once formally adopted, MiCA will set out harmonised EU-level definitions of all key terms relating to activities undertaken in crypto-asset markets. This includes definitions of crypto-assets, various types of tokens (asset-referenced, significant asset-referenced, electronic money, utility), crypto-asset service and service-providers, the operation of a trading platform in crypto-assets, the custody and administration of crypto-assets. The draft DLTR includes, among others, definitions of DLT MTF, DLT securities settlement systems and DLT transferable securities. 3) Offering and marketing of crypto-assets, other than asset-referenced tokens and e-money tokens Draft MiCA sets out detailed requirements applicable to persons seeking to offer crypto-assets to the public in the EU, or to request an admission for such crypto-assets to trading on a trading platform for crypto-assets. This includes specific requirements for the issuers of crypto-assets, such as an obligation to publish a white paper containing a detailed description of the planned crypto-asset offering or admission to trading. The draft legislation also includes requirements applicable to marketing communications relating to offering of crypto-assets or admission of such crypto-assets to trading, but it does not require issuers of crypto-assets to obtain competent authorities' ex-ante approval for a white paper or related communications. Finally, the draft MiCA sets out additional obligations applicable to crypto-asset issuers (such as an obligation to act honestly, fairly and professionally) and includes provisions on liability of issuers of crypto-assets. 4) Issuance of asset-referenced and e-money tokens Draft MiCA sets out a separate set of requirements applicable to the issuance of asset-referenced tokens to the public in the EU or their admission to trading on a trading platform. This includes an obligation for the issuer to obtain a prior authorisation by a National Competent Authority (NCA) and an obligation to publish a white paper approved by an NCA. In addition, issuers of asset-referenced tokens will have to comply with bespoke own funds requirements, governance arrangements, disclosure requirements, conflicts of interest and complaints handling mechanisms, obligation to hold reserve of assets, as well as having in place policies and

		procedures governing custody of the reserve assets, investment of the reserve assets and planning on orderly wind-down. Finally, the draft law includes separate, more stringent provisions applicable to issuers of asset-referenced tokens that will be designated as "significant". In addition to rules applicable to the general issuance of crypto-assets and asset-referenced tokens, the draft MiCA includes a separate set of requirements applicable to issuers of e-money tokens. Subject to exemptions, this includes an obligation for the issuer to be authorised as a credit institution or an electronic money institution, and comply with the applicable legislation, as well as publishing a white paper and notifying it to the relevant NCA. Draft legislation also provides for categorisation of certain e-money tokens as "significant", such that they will be subject to additional requirements and supervision. 5) Authorisation and operating conditions for crypto-asset service providers The draft legislation requires that the provision of services in crypto-assets should only be performed by legal persons that have a registered office in the EU and which have been authorised as crypto-asset service providers in accordance with MiCA. Authorised crypto-asset service providers will be able to provide their services cross-border in all EU jurisdictions. Authorised crypto-asset service providers will be subject to prudential requirements – composed of own funds and an insurance policy – the amount of which will depend on the nature of the service provided. The draft legislation also sets out prescriptive organisational and disclosure requirements, including rules on safekeeping of client's funds and outsourcing. Finally, the draft MiCA sets out detailed requirements applicable to crypto-asset service providers authorised to provide various services, including custody services, operating of trading platforms for crypto assets, exchanging services between crypto-assets and fiat currency or between other crypto-assets, executing orders for crypto-assets on behalf of third-parties, as well as providing placement services, reception and transmission of orders in crypto-assets and advice on crypto-assets. 6) Access to third-country crypto-asset service providers Contrary to other pieces of European capital markets legislation, draft MiCA does not include a separate regime for third-country crypto-asset service providers. Instead, it provides that persons based in the EU will be able to receive services offered by crypto-asset service providers established in a third-country on a reverse solicitation basis, i.e. on the EU person's exclusive initiative. When such a third-country firm would seek to actively solicit clients based in the EU and/or to promote or advertise its services in the EU, it will need to obtain authorisation as an EU crypto-asset service provider. The draft law includes a mandate for the Commission to assess, in due course, whether an equivalence regime should be established for third-country crypto-asset service providers. 7) Prevention of market abuse in markets in crypto-assets

		Finally, draft MiCA sets out anti-market abuse rules applicable to acts carried out by any person that concerns crypto-assets that are admitted to trading on a trading platform or for which a request for admission to trading on such trading platform has been made. This includes requirements concerning disclosure of inside information, prohibition of insider dealing, prohibition of unlawful disclosure of inside information and prohibition of market manipulation. 8) Requirements for DLT market infrastructure DLT MTFs will have to be operated by an investment firm authorised in accordance with MiFID, or by a market operator, while DLT securities settlement systems will have to be operated by a central securities depository as authorised in accordance with CSDR. The operation of DLT market infrastructure will, however, be subject to a separate permission, conditions of which are set out in the draft DLTR. The draft legislation sets out limitations in respect of financial instruments that could be traded or settled by using DLT market infrastructure. Permitted DLT transferable securities will include certain shares and bond asset classes (with the exception of sovereign bonds), subject to additional threshold conditions. In addition, operators of DLT market infrastructure will have to establish a clear and detailed business plan describing how they intend to carry out their services and activities, and comply with additional organisational and conduct requirements prescribed by DLTR. 9) Exemptions for DLT market infrastructure and pilot regime time-limits Draft DLTR allows operators of DLT MTFs to request certain exemptions from MiFID and MiFIR, subject to proposing suitable compensatory measures "to meet the objectives pursued by the provisions from which an exemption is requested". Likewise, operators of DLT securities settlement systems will be able to request certain targeted exemption from the CSDR provisions, a list of such exemptions being specified in DLTR. The pilot regime for DLT market infrastructure as set out by DLTR will be initially established for five years, following which ESMA is to report to the Commission on the functioning of the regime. 10) Next steps Both draft regulations will now be transferred to the European Parliament and to the Council of Ministers for review and adoption. The legislators can introduce additional amendments so the final version of the legislation might differ to some extent from the draft proposed by the Commission. Legislative review of complex files can take between 18 and 24 months, followed by a transition period that will be prescribed in a final legal act. Stakeholders are therefore encouraged to engage in legislative review from the early stages. **Published: 23 September 2020**
EU	**Proposed Regulation on digital operational**	On 24 September 2020 the European Commission published its long-awaited draft regulation on digital operational resilience for the EU financial services sector (DORA). The proposal, which is part of the broader Digital Finance Strategy package, is a first European-level legislative initiative

	resilience for the EU financial sector	aiming to introduce a harmonised and comprehensive framework on digital operational resilience for European financial institutions. When formally adopted, DORA will also bring critical third-party service providers – such as cloud computing services – within a direct oversight of the European Supervisory Authorities. The following provides an overview of 10 key things that you need to know about DORA. 1) Scope and subject matter The Commission proposes DORA to have very broad application and to cover credit institutions, payment institutions, electronic money institutions, investment firms, crypto-asset service providers, central securities depositories, CCPs, trading venues, trade repositories, AIFMs, management companies, data reporting service providers, insurance and reinsurance undertakings, insurance and reinsurance intermediaries, institutions for occupational retirement pensions, credit rating agencies, statutory audit and audit firms, administrators of critical benchmarks, crowdfunding service providers, securitisation repositories and ICT third-party service providers. The proposed legislation sets out requirements applicable to financial entities in respect of information and communications technology (ICT) risk management, contractual arrangements between ICT third-party service providers and financial entities, the oversight framework for critical third-party service providers and rules on cooperation between competent authorities. 2) Definitions The draft legislation includes a comprehensive set of definitions concerning persons and services within the scope of DORA, including definitions of digital operational resilience, ICT risk, ICT third-party risk, ICT third-party service provider (including cloud computing services) and ICT third-party service provider established in a third country. 3) ICT Risk Management When formally adopted, DORA will require financial entities to have in place comprehensive internal governance and control frameworks for ICT risks. Financial entities will also be obliged to build and maintain a sound, comprehensive and well-documented ICT risk management framework. This will include an obligation for financial entities to have and maintain updated ICT systems, protocols and tools, as well as to identify and document that pose a potential source of an ICT risk, especially those configurations that interconnect with internal and external ICT systems. Draft DORA sets out prescriptive measures that financial entities will need to comply with for the purpose of protection and prevention, detection, response and recovery from ICT risks, including having a dedicated and comprehensive ICT Business Continuity Policy. Finally, financial entities will also need to have in place measures allowing for monitoring the effectiveness of the implementation of their digital resilience strategy as well as a bespoke communications plan enabling a “responsible disclosure of ICT-related incidents or major vulnerabilities”. 4) ICT Related Incidents: Management, Classification and Reporting

		When formally adopted, DORA will require financial entities to establish and implement a specific ICT-related incident management process to identify, track, log, categorise and classify ICT-related incidents. Such process will have to allow for classification of ICT-related incidents in accordance with a set of criteria that is to be further developed by a Joint Committee of the European Supervisory Authorities (the ESAs Joint Committee). Finally, financial entities will be obliged to report all major ICT-related incidents to the competent authority, within the timeframes prescribed and by using harmonised reporting templates. 5) Digital Operational Resilience Testing For the purposes of their ICT risk management framework, financial entities will have to put in place a sound and comprehensive digital operational resilience testing programme, comprising of ICT testing tools, systems and methodologies as set out in the proposed regulation. 6) Key Principles for a Sound Management of ICT Third-Party Risk The draft legislation sets out key principles for managing ICT third-party risk, and covering responsibility of the financial entity, proportionality, strategy on ICT third-party risk, documentation and record-keeping, pre-contracting analysis, information security, audits, termination rights and exit strategies. The rights and obligations of the financial entity and of the ICT third-party service provider will have to be clearly allocated and set out in a contractual agreement, the detailed scope of which will be set out in the legislation. Among other obligations, financial entities will have to perform a preliminary assessment of concentration risk and further sub-outsourcing arrangements. The objective of such assessment will be to identify whether entering into a contractual arrangement would lead to contracting with a dominant ICT third-party service provider that is not easily substitutable, or having in place multiple contractual arrangements. 7) Oversight Framework of Critical ICT Third-Party Service Providers The draft legislation sets out a separate set of provisions applicable to critical third-party service providers (CTPPs), which will be designated by the ESAs Joint Committee and on the basis of a list of criteria set out in DORA. The proposed legislation also requires the establishment of an Oversight Framework of CTTPs responsible for, among other things, verifying that CTPPs have in place and respect “sound, comprehensive and effective rules, procedures and arrangements” that are appropriate to manage risks that CTPPs may “pose to financial entities and to overall financial stability”. In accordance with the draft proposals, the Oversight Framework will be equipped with far-reaching powers, including the unrestricted right to access all information deemed necessary by a Lead Overseer – this being one of the ESAs. The Lead Overseer will also have powers to conduct general investigations (including on-site inspections) of ICT third-party service providers. Finally, CTPPs will be charged oversight fees designed to cover all of the ESA’s “necessary expenditure” in relation to conduct of Oversight tasks. 8) Information Sharing Arrangements

		The proposed legislation will permit financial entities to exchange amongst themselves information and intelligence about cyber threats, including indicators of compromise, tactics, techniques, procedures, cyber security alerts and configuration tools. 9) Competent Authorities Finally, the proposal includes detailed rules concerning supervisory powers. By deciding against a centralised supervisory body, the Commission proposes to place supervision of compliance with the requirements of DORA with the respective competent authorities responsible for overseeing the in-scope financial entities. 10) Next steps The draft legislation will be transferred to the European Parliament and to the Council of Ministers for review and adoption. Both legislators can introduce additional amendments so the final version of the legislation might differ to some extent from the draft proposed by the Commission. Legislative review of complex files can take between 18 and 24 months, followed by a transition period that will be prescribed in a final legal act. Stakeholders are therefore encouraged to engage in legislative review from the early stages. **Published: 24 September 2020**
FRANCE	**Digital assets: the AMF describes its requirements for DASP registration or license**	Press release as follows: "The Autorité des Marchés Financiers (AMF) has published a Q&A that presents the key points of the digital asset service provider regime created under the PACTE Law. It answers the most frequently asked questions from French and international businesses that wish to apply for DASP registration or license. The law of 22 May 2019, known as the PACTE Law, created an innovative regime for digital assets by establishing a status of digital asset service provider in France, covering a wide variety of activities. This regime provides for mandatory registration with the AMF for some participants and an optional license system. Only licensed DASPs may engage in direct marketing. Registration with the AMF is mandatory for two types of services: the purchase and sale of digital assets in legal tender (for example, exchanging bitcoins for euros) and the custody of digital assets for third parties (custody of private keys for clients with the ability to use them on their behalf). Service providers who began their activity before the law entered into force have until 18 December 2020 to register. Project owners who had not yet begun conducting their activity must obtain registration before offering such services. The Questions & Answers specify, for example, the criteria according to which a foreign-based digital asset service provider is deemed to provide these services to clients resident or established in France and is thus subject to the registration requirement. Foreign-based participants who provide digital asset services in France must register and be established in

		France or in a Member State of the European Union or of the European Economic Area. However, service providers who apply for a license must be established in France, at least via a subsidiary or a branch in the country. The document also sets out the obligations regarding anti-money laundering and counter-financing of terrorism, as well as the obligation to verify the identity of clients. To date, the AMF has granted registration to two DASPs, after receiving positive opinions from the Autorité de Contrôle Prudentiel et de Résolution (ACPR). There are currently some twenty applications being processed. Although several licensing applications have been submitted, no entity has been licensed to date. The AMF points out that it is a criminal offence to claim to be registered or licensed without having completed the process (Articles L. 572-23 and L. 572-26 of the Monetary and Financial Code)." **Published: 22 September 2020**
UK	**FCA continues to promote innovation through DataSprint and digital sandbox to solve Covid-19 challenges**	On 2 September 2020, the Financial Conduct Authority (FCA) launched a new webpage updating market participants on the pilot of its "digital sandbox" and recent DataSprint. The FCA notes that its latest DataSprint, held in July and August 2020, enabled 120 market participants from multiple sectors and disciplines to collaborate to develop data models and typologies, critically evaluate methodologies and produce reliable reference data to fuel future sandbox testing. The focus of the digital sandbox at present is to enable firms to test and develop innovative solutions to challenges arising due to the Covid-19 pandemic, including fraud and scams; handling vulnerable customers; and enhancing access to financial services for small and medium-sized enterprises. The FCA will be opening applications for participation in the digital sandbox in the coming few weeks. **Published: 3 September 2020**
UK	**Reinventing the wheel (with more automation) – speech by Andrew Bailey**	On 3 September 2020, the Bank of England (BoE) published a speech by its Governor, Andrew Bailey, in which he looks at recent innovations in payments and the challenges they bring. Mr Bailey also examines the benefits and risks that stablecoins present. Mr Bailey states that a stablecoin that intends to launch with sterling-based activities in the UK must first meet relevant standards and be appropriately regulated. If a sterling stablecoin wishes to operate at scale in the UK, then the BoE will strongly consider the need for the entity to be incorporated in the UK. This is similar to the subsidiarisation of banks that the BoE requires if they are holding UK retail transactional customer deposits above a de minimis level. In terms of a global stablecoin, which is a cross-border phenomenon, Mr Bailey mentions that the BoE is looking forward to the Financial Stability

		Board's final report on the topic which is expected in October. He also adds that current proposed global stablecoin offerings will need to demonstrate how they meet domestic and international standards. They must do so before the global regulatory community can be comfortable with their launch and widespread adoption. Mr Bailey also discusses central bank digital currency (CBDC) and the discussion paper that the BoE published earlier this year that sets out the key considerations and an illustrative model based on a central bank core ledger and private payment interface providers offering overlay services to users. Mr Bailey reports that the discussion paper received a wide range of responses that the BoE is working through and it will set out more information next year. **Published: 3 September 2020**
Asia	**Press release by Korea's Financial Services Commission on the launch of consultative body on digital finance**	Press release as follows: "The FSC launched a public-private joint consultative body on digital finance, composed of leaders and experts representing financial sectors, big techs, fintechs and major financial labor unions, and held a kick-off meeting on digital finance via teleconference on September 10. The joint consultative body has been set up to tackle diverse challenges arising from the era of digital finance and offer balanced perspectives and solutions. The consultative body will operate four thematic working groups on (i) big tech-fintech relations, (ii) rules and regulations, (iii) financial data security and (iv) financial consumer protection. During the meeting, Vice Chairman Sohn Byungdoo spoke about the need to (i) continue regulatory reforms to promote innovation in financial services, (ii) build a fair competition environment for market participants, (iii) ensure consumer safety in digital finance, (iv) review risk factors related to financial market stability and (v) evaluate the impact of digital transformation on the society as a whole. The participants agreed on the need to have ongoing discussions on how to further develop the traditional financial industry and to promote close cooperation and a win-win strategy between financial enterprises and digital platform businesses including fintechs. The joint consultative body will hold meetings regularly throughout this year and make its findings available to the public." **Published: 10 September 2020**
US	**SEC and OCC issue guidance on authority of national banks and federal saving associations to**	On 21 September 2020, the Securities and Exchange Commission (SEC) and the Office of the Comptroller of the Currency (OCC) issued guidance on the authority of national banks and federal saving associations to hold stablecoin reserves. In particular, the SEC reiterates that whether a particular digital asset, including one labelled as a stablecoin, constitutes a security will depend on the specific facts and circumstances. In its guidance, the OCC concludes

	hold stablecoin reserves	that national banks may hold stablecoin "reserves" as a service to bank customers. **Published: 21 September 2020**
	State Regulators Roll Out One Company, One Exam for Nationwide Payments Firms	Press release as follows: "Money transmitters operating in 40 or more states will benefit from streamlined state examinations in 2021. The Conference of State Bank Supervisors (CSBS) announced the launch of a state-initiated program whereby nationwide payments firms will undergo one comprehensive exam in 2021 that seeks to satisfy all state examination requirements. Known as MSB Networked Supervision, the initiative applies to 78 of the nation's largest payments and cryptocurrency companies that currently meet the 40-state threshold. These companies combined move more than $1 trillion a year in customer funds. Building on years of multistate coordination, this exam protocol will enable states to fine tune a risk-based approach to each company's operations. When compliance issues arise, the states will be better positioned to follow up throughout the year. Each exam will be led by one state overseeing a group of examiners sourced from across the country. By relying on experts across the state system — including in cyber security and anti-money laundering — regulators will gain more insight while also freeing up state resources. This initiative has broad support from the full CSBS and Money Transmitter Regulators Association (MTRA) membership, which spans all state regulators that regulate money transmission. The program is being launched after the completion of the One Company, One Exam pilot, which was conducted in 2019 and early 2020 and included several companies, including Western Union. **Published: 15 September 2020**

International developments

G20

There has been no reported activity.

Financial Stability Board (FSB)

There has been no reported activity.

FICC Markets Standards Board (FMSB)

There has been no reported activity.

Bank for International Settlements (BIS)

There has been no reported activity.

International Organisation of Securities Commissions (IOSCO)

There has been no reported activity.

Committee on Payments and Market Infrastructures (CPMI)

On 29 September 2020, the CPMI published a report titled 'Payment aspects of financial inclusion: application tools', which aims to assist national authorities in applying the Payment aspects of financial inclusion (PAFI) guidance published in 2016. It also complements the 'Payment aspects of financial inclusion in the fintech era' report published in April 2020. In particular, the new report sets out a PAFI questionnaire to assist in the authorities' fact-gathering exercises, containing key actions for considerations (KACs) along with 'fintech focus' considerations.

Published: 29 September 2020

Basel Committee on Banking Supervision (Basel Committee)

Pablo Hernández de Cos, Governor of the Bank of Spain and Chair of the Basel Committee, gave a speech at the Virtual OMFIF-Banque de France Seminar on 25 September 2020, on the topic of 'how central banks can use digitalisation to better serve the public - the case of payments'. In particular, he set out a number of considerations relating to the potential issuance of a digital euro, including active dialogues with stakeholders, developing a rigorous experimentation agenda and international cooperation. He also evaluated the pros and cons of issuing a central bank digital currency and considered the growing interest in cross-jurisdictional payments.

Published: 25 September 2020

Financial Action Task Force (FATF)

On 14 September 2020, the Financial Action Task Force (FATF) published a report, Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing. The report is based on more than 100 case studies and is designed to help national authorities and financial institutions identify potential money laundering and terrorist financing activity involving virtual assets by highlighting the most important red flag indicators that could suggest criminal behaviour. The report will also help reporting entities' application of a risk-based approach to their customer due diligence requirements, which require knowing who their clients and the beneficial owners are, understanding the nature and purpose of the business relationship, and understanding the source of funds.

Key red flag indicators in the report focus on:

- Technological features that increase anonymity – such as the use of peer-to-peer exchange websites, mixing or tumbling services or anonymity-enhanced cryptocurrencies.
- Geographical risks – criminals can exploit countries with weak, or absent, national measures for virtual assets.
- Transaction patterns – that are irregular, unusual or uncommon which can suggest criminal activity.
- Transaction size – if the amount and frequency has no logical business explanation.
- Sender or recipient profiles – unusual behaviour can suggest criminal activity.
- Source of funds or wealth – which can relate to criminal activity.

The report complements the June 2019 FATF guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers which explains how to understand the money laundering and terrorist financing risks of virtual assets, how to license and register the sector, actions the sector needs to take to know information about its customers, how to store this information securely, and how to detect and report suspicious transactions.

Published: 15 September 2020

World Economic Forum

On 10 September 2020, the WEF published a report on the effects of emerging technologies such as AI and 5G on the financial services industry.

The four key sections of the report cover:

- key takeaways including a perspective on future value sources and risk areas;
- new opportunity spaces and industry areas where disruption is most likely;
- use cases of different technologies in each sector of financial services; and
- capability descriptions, development timelines and critical business applications of the most relevant emerging technologies.

Published: 10 September 2020

SWIFT

In September 2020, SWIFT (a global member-owned cooperative and provider of secure financial messaging services) published a report to support market participants in understanding the money laundering techniques which underpin large-scale cyber-attacks.

The report sets out the end-to-end journey commonly used by criminals to launder funds obtained through illicit cyber-crime related activities, and focusses on how criminal activity is conducted during the three stages of money laundering (placement, layering and integration). For example, SWIFT explains the use of money mules in ATM-related heists; how other third parties (such as front companies and financial representatives) can be exploited; and the growing appeal of virtual currencies in the money laundering arena.

SWIFT highlights five strategies which firms should consider to mitigate the risks highlighted in the report. These include:

1. Enhancing domestic information sharing, especially between the public and private sectors.
2. Facilitating international information sharing, in particular pertaining to jurisdictions identified as high risk by the Financial Action Task Force (FATF).
3. Investing in technology to enable the identification and disruption of money mule activity.
4. Enhancing customer due diligence and reporting requirements and standards, especially in jurisdictions where these are known to currently be weaker and thus entice criminals for exploitation purposes.
5. Increasing investment and training in cyber-security initiatives focussing on data centric security.

These are particularly important given that SWIFT anticipates that large-scale cyber-crime is likely to continue and evolve, as criminals find new ways to leverage technology, exploit gaps and circumnavigate controls.

Whilst many institutions heavily invest in technology and resource to combat financial crime, including that stemming from cyber-crime, SWIFT notes that cyber-attacks not only lead to commercial damage but also bring institutional reputational repercussions. Therefore, firms are urged to not become complacent and keep these continually-evolving risks at the forefront.

Published: 7 September 2020