NORTON ROSE FULBRIGHT

Global Blockchain Business Council

Monthly Fintech Updater, March

Norton Rose Fulbright LLP – 31 March 2021

Global, EU, UK and US Regulatory developments

EU	
Member States consider amendments to MiCA	On 24 February 2021, the Portuguese Presidency of the Council held a working group meeting dedicated to continue the review of the European Commission's proposal for the regulation on markets in crypto-assets **(MiCA).** The agenda for the meeting included a discussion on select issues under Title I, IV and V of the proposed regulation, as well as prudential requirements for credit institutions dealing in crypto-assets. Below is short overview of the key issues discussed: **1. Subject matter, scope and definitions (Title I)** The Presidency proposed for Member States' consideration certain drafting suggestions regarding the classification of crypto-assets and terminology regarding the holding of crypto-assets. Among other things, the Presidency proposed to remove an exemption from the scope of MiCA for crypto-assets that are structured deposits. It also proposed to remove an exemption for insurance undertakings from the scope of MiCA. Finally, the Presidency also proposed to amend a definition of the term "operation of a trading platform for crypto-assets" and align it with the MiFID definition of regulated market. **2. Select issues concerning e-money tokens (Title IV and V)** Noting that the proposed legislation does not exempt e-money institutions from MiCA authorisation if they provide services in crypto-assets, the Presidency acknowledged concerns of certain Member States that such institutions should be subject to such limited exemption that would be linked with their existing authorisations under the revised Payment Services Directive (PSD II) or E-Money Directive. The Presidency was of the view that while it would not be feasible to draw equivalence between the provision of services in crypto-assets and payment services, there was scope for amending MiCA in order to ensure that e-money institutions may provide custody services only for the e-money tokens (**EMTs**) issued by them without a need for further MiCA license. Regarding payment services, the Presidency questioned whether the services provided by the custodian to enable a client to transfer an EMT to another account is considered a transfer of funds under PSD II, and suggested that MiCA could provide some further clarity to this end. Recalling that Member States did not support a proposal to classify asset-referenced tokens with payment functionality as EMTs, the Presidency noted some of the Member States' concerns that some of the protections and rules applicable to payment services under the PSD II should also be extended to asset referenced token holders, and proposed some options for further consideration. **3. Requirements for crypto-asset service providers (Title V)** Building on an exemption for investment firms from MiCA authorisation that was included in the Commission's proposal, the Presidency put forward for Member States' consideration a similar exemption for fund managers who are authorised to provide certain MiFID services. In respect of custody and administration services for crypto-assets, the Presidency proposed two options for Member States' consideration regarding prospective amendments to the provisions of custody services and depending on whether the client is required to transfer the crypto-assets to an account of the custodian. In relation to service of operation of trading platform for crypto-assets, the Presidency noted the concerns from certain Member States that the current provisions regarding settlement prevented operators of trading platforms from settling off-chain and

	suggested two options for amendments (deletion of the requirements or creating separate options for off-chain/on-chain settlement). In respect of decentralised exchanges (DEX), the Presidency suggested to clarify that MiCA would not apply to DEX with no degree of centralisation. **4. Prudential requirements for credit institutions** A non-paper prepared by two Member States focused on the possible risks posed by the activities related to the issuance and servicing of crypto assets and noted that such activities are not sufficiently covered by the CRD/CRR framework. Noting that the MiCA proposal only allows banks to perform crypto related activities in line with their existing banking license, the non-paper stated that banks' risk management frameworks do not include specific provisions that effectively ensure proper risk management for crypto-asset-related activities. As such, the non-paper concluded that allowing banks to carry on crypto-assets activities without additional regulation concerning risk management was not prudent. To this end, the non-paper called on the Commission to conduct an assessment of the specific risks stemming from banks' crypto-asset-related activities, including the identification of specific risk drivers and information on how they are covered by the CRD/CRR. Should any such risks be identified, the non-paper suggested that the entry into force of MiCA should be postponed until a new prudential framework for credit institutions is developed. **Published: 4 March 2021**
ECON Rapporteur publishes draft report on DLT market infrastructures pilot regime	On 12 March 2021, European Parliament rapporteur Johan van Overtveldt (BE, ECR) published his draft report on the European Commission's proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology **(DLT).** The proposal is part of the Commission's September 2020 legislative package, which also includes a proposal for a Regulation on Markets in Crypto-Assets **(MiCA)** and a proposal for a Regulation on digital operational resilience for the EU financial sector **(DORA).** The draft Regulation on a pilot regime for market infrastructures based on distributed ledger technology (**DLTR**) creates a bespoke legal regime for the practical application of DLT in post-trade services. The DLTR will provide a regulatory framework for the development of DLT multilateral trading facilities **(DLT MTFs**) and DLT securities settlement systems (**SSS**), including for the granting and withdrawal of specific permissions and exemptions. In the report, the rapporteur writes that he considers that DLT can bring a number of potential benefits in the provision of financial services and that an ambitious approach should be taken in that regard. The rapporteur supports the overall objectives of the Commission, whose aim is to provide legal certainty by establishing uniform requirements for operating DLT market infrastructures and to support innovation by removing obstacles to the application of DLT in the financial sector. Yet, the rapporteur has a number of concerns on the original proposal and proposes to amend it in the following manner: **1. Scope** While acknowledging that the envisaged scope of the Regulation foresees limits in terms of both financial thresholds and instruments that can be accepted under the DLT Pilot Regime, the rapporteur proposes to amend the two thresholds: • **Financial thresholds:** the rapporteur understands the Commission's approach to establish an aggregate threshold for the total market value of DLT transferable securities, as this strikes a balance between openness to innovation and the protection against financial stability risks. However, the rapporteur proposes to take a more

prudent approach for the accomplishment of the Commission's objectives. The proposed amendments limit the maximum market capitalisation of the issuer of DLT transferable securities to less than EURO 50 million for both shares and bonds.

- **Admissible securities:** the rapporteur amends the proposal by making it possible for sovereign bonds to be admitted to trading or to be recorded on a distributed ledger. Furthermore, an amendment is proposed which includes DLT exchange-traded funds (ETFs) under the list of admissible securities.
- **Technology-neutral wording on use of DLTs**: the rapporteur proposes to include an amendment making it clear that liability for the functioning of any particular DLT should always remain with the DLT market infrastructure, regardless of the type of DLT it operates.

2. Level playing field

New type of DLT infrastructure: the Commission proposal provides DLT MTFs the possibility to undertake central securities depository activities under the DLT Pilot Regime, but at the same time the DLT SSS would be unable to perform MTF activities. In this context, the rapporteur proposes to ensure that a DLT MTF doing settlement services must follow the same requirements as a DLT SSS, and vice versa, and proposes to create a new type of market infrastructure, a "DLT Trading and Settlement System" for operators wishing to combine both trading and post-trading roles.

3. Early-exit assessment

In the original proposal, the Commission provided that the DLT Pilot Regime should last five years, after which the Commission should assess the costs and benefits of extending the regime on DLT market infrastructures or not. The rapporteur keeps this time period in his legislative report, but includes a provision stating that the Commission should publish such a report after the third year of the DLT Pilot Regime as well.

4. Next steps

Following the publication of the report, the rapporteur will present it in the European Parliament's Economic and Monetary Affairs (ECON) Committee. The legislative report is likely to be amended during the course of discussions with other committee members and shadow rapporteurs. We expect these discussions to take place in Q2 2021. After the adoption of the legislative report in the ECON Committee, the European Parliament plenary as a whole must adopt the report. Trilogue negotiations with the Council will start once both co-legislators have adopted their legislative report.

View the full report here

Published: 12 March 2021

UK	
FCA warns that younger investors are taking on big financial risks with investments like cryptocurrency	On 23 March 2021, the FCA published a research report that seeks to gain a better understanding of investors who engage in high-risk investments like cryptocurrencies and foreign exchange. The research report shows that there is a new, younger, more diverse group of consumers getting involved in higher risk investments, potentially prompted in part by the accessibility offered by new investment apps. However, there is evidence that these higher risk products may not always be suitable for these consumers' needs as nearly two thirds (59%) claim that a significant investment loss would have a fundamental impact on their current or future lifestyle. The research also shows that investors often have high confidence and claimed knowledge. However, it notes a lack of awareness and/or belief in the risks of investing, with over 4 in 10 not viewing 'losing some money' as one of the risks of investing, even though as with most investments their whole capital is at risk. The research found that these younger investors may have the lowest levels of financial resilience making them more vulnerable to investment loss. Research showed that a significant loss could have a fundamental lifestyle impact on 59% of self-directed investors with less than 3 years' experience, who are more likely to own high risk investment products, compared with 38% of investors with greater than 3 years' experience. Alongside the publication of the research report, the FCA has launched its digital disruption campaign to prevent investment harm. The FCA advises consumers to consider five important questions before they invest: **1.** Am I comfortable with the level of risk? **2.** Do I fully understand the investment being offered to me? **3.** Am I protected if things go wrong? **4.** Are my investments regulated? **5.** Should I get financial advice? **Published 23 March 2021**

Australia	
Australia to impose tighter restrictions on new challenger banks	Statement released on 18 March as follows: The Australian Prudential Regulation Authority (**APRA**) has commenced consultation on an updated approach to licensing and supervising new authorised deposit-taking institutions (**ADIs**). In an information paper published today, APRA has outlined stronger requirements for being granted a banking licence, and closer supervision of new entrants as they seek to establish themselves. The revised approach follows a review of APRA's ADI licensing regime aimed at incorporating learnings since the launch of the Restricted ADI licensing pathway in 2018. The review, announced last August, found the approach needed a greater focus on longer term sustainability, rather than the short-term ambition of receiving a licence. Among the changes outlined in the information paper: • Restricted ADIs must achieve a limited launch of both an income-generating asset product and a deposit product before being granted an ADI licence; • There is increased clarity around capital requirements at different stages for new entrants, aimed at reducing volatility in capital levels and facilitating a transition to the methodology for established ADIs over time; and • New entrants are expected to have more advanced planning for a potential exit, including a focus on return of deposits as an option. APRA Deputy Chair John Lonsdale says the updated approach would support newly licensed banks so they are better equipped to succeed. "Since launching the Restricted ADI regime three years ago, we've gained a deeper understanding of the challenges new and aspiring banks face as they try to establish themselves in an industry that is capital intensive and dominated by some of the best resourced companies in Australia. "This revised approach effectively targets key risks for new entrants, setting a higher bar for gaining a bank licence, while enhancing competition by making it more likely new entrants can find their feet and gain a firm foothold in the market. "New entrants will start from a stronger capital position and be ready to attract depositors and earn revenue immediately; they'll receive additional supervisory attention from APRA until they're firmly established; and – should they ultimately not succeed – they will be better placed to exit the industry in an orderly fashion," Mr Lonsdale said. A consultation on the proposals closes on 30 April. Copies of the information paper and a high-level discussion paper are available on APRA's website at: Licensing for authorised deposit-taking institutions. **Published: 18 March 2021**

South Korea	
AML requirements of virtual asset service providers to take effect from March 25	Statement released on March 16 as follows: The FSC announced that the revised rule that mandates AML duties on virtual asset service providers (**VASPs**) will go into effect on March 25, 2021, as the government approved the revised Enforcement Decree of the Act on Reporting and Using Specified Financial Transaction Information at a cabinet meeting held on March 16. Key Provisions: **1. Scope of VASPs** Virtual asset service providers are virtual asset trading service providers, virtual asset safekeeping and administration service providers and virtual asset digital wallet service providers that are engaged in the purchase and sales, exchange and transfer, safekeeping and administration, intermediation and brokerage of virtual assets and virtual asset transactions. **2. Business registration of VASPs** VASPs are required to register their business with the Korea Financial Intelligence Unit (**KoFIU**) prior to the commencement of their business operation. Existing businesses that qualify as VASPs should register within six months (until September 24, 2021) or they will be subject to penalties. **3. AML duties of VASPs** Beginning on March 25, 2021, the registered VASPs will be subject to the anti-money laundering (**AML**) requirements, such as duties to verify identities of customers, file reports on suspicious transactions, etc. The authorities will carry out inspection and supervision on VASPs with regard to their compliance of AML requirements from the time of business registration. As the requirement to check and verify the identity of customers applies only to the registered businesses, consumers are advised to check the status of business registration and practice caution against VASPs requesting information about their resident registration numbers. **Published: 16 March 2021**

Dubai	
Dubai Financial Services Authority consults on regulation of Security Tokens	On 29 March, The Dubai Financial Services Authority (DFSA) published its "Framework for Regulating Security Tokens" for public consultation for a period of 30 days. The DFSA is proposing a comprehensive and innovative regulatory framework for regulating Security Tokens, a new and growing area of interest for many industry participants. We are actively engaged with key stakeholders in Dubai and around the world on the future of finance and the rapidly growing area of financial technology, including various Distributed Ledger Technology (DLT) applications. Security Tokens create rights and obligations that are the same as, or are substantially similar to conventional investment instruments. We use the term Security Tokens as this is a commonly used term in the industry, but the framework goes beyond typical securities to cover derivatives as well. This enables the use of DLT and similar technologies across the full spectrum of investments in a consistent manner. We propose updating our regulatory regime to facilitate DLT-based activities of: • the offer of Security Tokens to the public, and the admission to trading of Security Tokens on trading facilities; • the trading of Security Tokens; and • the provision of other financial services relating to Security Tokens, such as providing custody relating to Digital Wallets holding Security Tokens, and advising and arranging. Some of the key changes proposed are: • allowing facilities that trade Security Tokens to have direct access members, including retail clients; • enhanced systems and controls requirements to address risks associated with the use of DLT or similar technology; • enhanced disclosure in prospectuses; and • enhanced requirements for those providing custody of Digital Wallets. Allowing direct access is a significant shift from the current intermediated model of trading in markets. Our proposals include appropriate safeguards to tackle investor protection needs and misconduct risks, whilst also addressing market integrity, financial stability and, crucially, money laundering and terrorism financing threats in the direct access environment. We will soon issue proposals for other types of tokens that are not Security Tokens, such as exchange tokens and utility tokens, later in 2021. Bryan Stirewalt, the Chief Executive of the DFSA, said: "The proposal for regulation of Security Tokens is a key milestone in paving a clear and certain path for those issuers who wish to raise capital in or from the DIFC using DLT and similar technology, and for those firms who intend to be involved in this market, by conducting or providing financial services. Our proposals promote and facilitate innovation, while also protecting consumers, addressing market integrity and mitigating ML/FT and other risks. We have drawn on the experience of other regulators who have taken cautious steps in this rapidly developing area, while addressing DIFC specific needs. We look forward to receiving public comments on these proposals." **Published: 29 March 2021**

Canada

Canadian securities regulators issue guidance on disclosure by crypto assets issuers

The Canadian securities regulators have published guidance on continuous disclosure obligations for reporting issuers dealing in digital assets, including cryptocurrencies, tokens, stablecoins, and other digital assets relying on blockchain technology **(crypto assets**).

Key recommendations:

1. **Safeguarding of Crypto Assets**
   Issuers are expected to identify controls adopted (or not adopted) to protect against the risk of theft or loss of crypto assets. Appropriate controls may vary depending on the size of the issuer, the type and quantity of crypto assets held, and the frequency at which the crypto assets are moved. Issuers that have retained a third-party custodian should disclose sufficient information on that custodian. Issuers that have not retained a third-party custodian should disclose their reasons for not doing so. The staff notice lists several examples of the information the Canadian securities regulators (CSA) would expect to see in this regard.
2. **Use of Crypto Asset Trading Platforms**
   Issuers that hold crypto assets through a crypto asset trading platform without holding a private key or control over the assets are subject to the solvency, integrity and proficiency of the platform's operators. Accordingly, such issuers are expected to disclose the extent to which they rely on crypto asset trading platforms, and the controls adopted to protect against theft or loss.
3. **Description of Business**
   In complying with the requirement to describe their businesses, issuers are expected to all include material information, which would likely include the nature of their operations, how they intend to generate revenue, their specialized skill and knowledge, the competitive conditions they face, the sources, pricing, and availability of equipment they use and any reliance on third-party service providers.
4. **Risk Factors**
   In complying with the requirement to disclose relevant risk factors, issuers are expected to be specific and sufficiently tailor risks that relate to the issuer and its business. Such risk factors may include availability and/or cost of electricity, potential declines in crypto asset prices, decreased rewards for mining, and access to crypto assets held by third parties.
5. **Promotional Activities**
   Issuers are cautioned against providing unbalanced or unsubstantiated material claims about their businesses and corresponding opportunities for profit. Promotional statements should be supported by objective data that provides a reasonable basis on which the conclusion is based. If such an issuer were to file a prospectus absent appropriate investor protections, regulators may not issue a receipt if determined to be contrary to the public interest.
6. **Financial Statements and Auditing Issues**
   There are particular accounting policy and control considerations of relevance to issuers involved in cryptocurrencies, as a subset of crypto assets. The CSA has included in its guidance expectations related to recording cryptocurrencies at fair value, accounting for cryptocurrency mining and the equipment involved, and settling non-monetary transactions in cryptocurrency. Issuers are reminded to include the specific disclosures required under IFRS, and to review guidance published by the Chartered Professional Accountants of Canada and communications from the Canadian Public Accountability Board.

	7. Conclusion The emerging nature of crypto assets and the novel risks associated with them can create challenges for issuers seeking to comply with existing disclosure obligations. The CSA guidance provides clarity for issuers dealing in crypto assets, serving as a useful guide to assist issuers and their advisors in adequately preparing disclosure. CSA Staff Notice 51 363 Observations on Disclosure by Crypto Assets Reporting Issuers is available here. **Published: 22 March 2021**
US	
Securities and Exchange Commission includes FinTech in its top priorities for 2021	Statement released 3 March as follows: The Division publishes its examination priorities annually to provide insights into its risk-based approach, including the areas it believes present potential risks to investors and the integrity of the U.S. capital markets. In relation to FinTech, the examinations will focus on evaluating whether registrants are operating consistently with their representations, whether firms are handling customer orders in accordance with their instructions, and review compliance around trade recommendations made in mobile applications. Examinations of market participants engaged with digital assets will continue to assess the following: whether investments are in the best interests of investors; portfolio management and trading practices; safety of client funds and assets; pricing and valuation; effectiveness of compliance programs and controls; and supervision of representatives' outside business activities. See the full press release here **Published: 3 March 2021**

International developments

G20
The 3rd G20 Infrastructure Working Group meeting focused on local, digital and green infrastructure On 23 March 2021, the Members of the Infrastructure Working Group (**IWG**) gathered virtually for their third official session. The Covid-19 crisis demonstrated how crucial a well-functioning digital infrastructure is to sustain productivity, promote social inclusion and ensure that basic services get consistently provided to the entire population. The Group made an assessment of the digital infrastructure investment needs and the existing financing gaps. The meeting offered an occasion to the Italian G20 Presidency to outline some of the key deliverables on digital infrastructure including on how fostering high-quality broadband connectivity for a digital world. With the support of the OECD, G20 members discussed the importance of extending high-quality connectivity and identifying policies to further strengthen networks resilience and performance, while eliminating connectivity divides. In this IWG third meeting, the Italian G20 Presidency also presented its proposal to progress on infrastructure investments related matters with specific focus on sustainable infrastructure, notably through the organization of the G20 Infrastructure Investors Dialogue, in collaboration with the OECD and the D20 Long-Term Investors Club. Given the key challenges brought to light by the pandemic, this initiative aims to mobilise resources that can lead to more and

better infrastructure in all countries, create quality jobs and achieve sound economic recovery, aligned with climate and development goals. One of the objectives of the Italian G20 Presidency is to go beyond official closed door meetings. In order to do so, the working group meeting are often paired with workshops open to stakeholders and the civil society. In this sense, the debate on infrastructure related issues saw an extensive dialogue among global experts, facilitated by leading international think tanks.

Two of these workshops were organised by the International Affairs Institute (**IAI**) and Bruegel. Representatives from the two prestigious think tanks presented the main outcomes of their workshops on, respectively, “Financing infrastructure investments for local communities”, held on 4 February 2021, and “Think green act local: the role of the G20 in sustainable infrastructure”, which took place virtually on 15 March 2021. Both IAI and Bruegel stressed the relevance of local governments for understanding the communities’ needs, starting from a bottom-up approach, including by sharing best practices and experiences. Their open discussions aim to gain a better understanding of the financial instruments and practices to promote effective local infrastructure investment, spanning from private investors financing to establishing a more efficient enabling environment for investments. In addition to this, local authorities can play a key role in promoting green infrastructure investments and turning current challenges into opportunities for sustainable recovery and social inclusion.

The debate on building and maintaining sustainable and inclusive infrastructure will continue at the 2nd Finance Ministers and Central Bank Governors meeting on 7 April and at the next meeting of the Infrastructure Working Group scheduled in early May 2021.

Published: 23 March 2021

Bank for International Settlements (BIS)

Bigtechs in finance: regulatory approaches and policy options

Statement released 16 March as follows:

At present, financial services represent a relatively small part of big techs' overall activities, though this can change rapidly due to the unique features of their business models and they could quickly become systemically important – or "too big to fail". Big techs' financial operations are subject to the same requirements as those of other market participants. As such, big techs need to hold appropriate licences to perform regulated financial activities or provide their services in partnership with financial institutions that meet the regulatory requirements.

Risks connected with big tech activities in finance may not be fully captured by the regulatory approach up to now, which is geared towards individual entities or specific activities and not the risks that are created by substantive interlinkages within big tech groups and their role as critical service providers for financial institutions. An effective oversight of big tech activities in finance calls for going beyond a piecemeal policy framework and considering recalibrating the mix of entity-based and activity-based rules, in favour of the former in certain policy areas. A step further would be to assess the possibility of introducing a bespoke approach for big techs encompassing a comprehensive public policy framework. In any case, there is a need for enhancing cross-sectoral and cross-border cooperative arrangements.

The full paper is available here.

Published: 16 March 2021

BIS releases a report on the FinTech gender gap

Statement released 11 March as follows:

Financial inclusion is a key goal for policymakers around the world. Yet women remain unbanked or underbanked relative to men: they have lower access to transaction accounts, credit and other financial services. Hopes are high that new financial technology ("fintech") can enhance financial inclusion and close the gender gap in access to financial services. Yet evidence on adoption rates of FinTech products and services by gender has so far been scarce.

FinTech promises to spur financial inclusion and close the gender gap in access to financial services. Using novel survey data for 28 countries, this paper finds a large 'FinTech gender gap': while 29% of men use FinTech products and services, only 21% of women do. The gap is present in almost every country in our sample. Country characteristics and several individual-level controls explain about a third of the unconditional gap. Gender differences in the willingness to use new financial technology or FinTech entrants if they offer cheaper services account for over half of the remaining gap. It is roughly the same size for products provided by FinTech entrants and those offered by traditional financial institutions. The paper concludes by suggesting potential explanations for the gender gap and implications for challenges in fostering financial inclusion with new technology.

View the full report here

Published: 11 March 2021

BIS releases a report on big data and machine learning in central banking

The world is changing and so is the way it is measured. For decades, policymakers and the private sector have relied on data released by official statistical institutions to assess the state of the economy. Collecting these data requires substantial effort and publication often happens following a lag of several months, even years. However, the last years have seen explosive growth in the amount of readily available data, as well as in the technology and software used to analyse it. These developments have spurred central banks' interest in big data and machine learning.

The analysis highlights four main insights. First, central banks define big data in an encompassing way that includes unstructured non-traditional as well as structured data sets. Second, central banks' interest in big data and machine learning has markedly increased over the last years: around 80% of central banks discuss the topic of big data formally within their institution, up from 30% in 2015. Third, the vast majority of central banks are now conducting projects that involve big data. Institutions use big data and machine learning for economic research, in the areas of financial stability and monetary policy, as well as for suptech and regtech applications. And fourth, the advent of big data poses new challenges, among them data quality, legal aspects around privacy, algorithmic fairness and confidentiality, as well as budget constraints. Cooperation among public authorities could relax the constraints on collecting, storing and analysing big data.

View the full report here

Published: 4 March 2021

Financial Action Task Force (FATF)

Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers

On 19 March 2021, the Financial Action Task Force (**FATF**) issued a public consultation on proposed revisions to its 2019 guidance on the risk-based approach to virtual assets (**VAs**) and virtual asset service providers (**VASPs**).

The FATF is proposing to update its guidance in order to:

- Clarify the definitions of VA and VASP to make clear that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by the FATF Standards (either as a VA or as a traditional financial asset).
- Provide guidance on how the FATF Standards apply to so-called stablecoins.
- Provide additional guidance on the risks and potential risk mitigants for peer-to-peer transactions.
- Provide updated guidance on the licensing and registration of VASPs.
- Provide additional guidance for the public and private sectors on the implementation of the ‘travel rule’.
- Include Principles of Information-Sharing and Co-operation Amongst VASP Supervisors.

The guidance is also being updated to reflect the passage of time and the publication of other relevant FATF reports.

The deadline for comments on the consultation is 20 April 2021. Separate to the consultation, the FATF is also considering the implementation of the revised FATF Standards on VAs and VASPs, and whether further updates are necessary, through a second 12-month review. The FATF will consider the report of this review in June 2021.

Published: 19 March 2021

Global Legal Entity Identifier Foundation (GLEIF)

GLEIF Launches New Stakeholder Group to Accelerate the Integration of LEIs in Digital Certificates

On 11 March 2021 The Global Legal Entity Identifier Foundation (GLEIF) announced a new collaboration with Certification Authorities (CAs) and Trust Service Providers (TSPs), to drive the use of Legal Entity Identifiers (LEIs) within digital certificates.

GLEIF has launched a CA Stakeholder Group to facilitate communication between GLEIF, CAs and TSPs from across the world, as they collectively aim to coordinate and encourage a global approach to LEI usage across digital identity products. Participation has already been confirmed by China Financial Certification Authority (CFCA), DigiCert, InfoCert, Entrust Datacard, ICAI India, and SwissSign. The collaboration announcement follows news last year that ISO has standardized the process of embedding LEIs in digital certificates. In accordance with ISO 17442-2, the CA Stakeholder Group will develop and promote best practice guidelines and use cases for LEI integration across the digital identity industry. This will help members of the group, who are all committed to incorporating the LEI into their digital identity products, to progress their own implementations. GLEIF will also welcome participants' views on current and future LEI services.

The use of the LEI in digital certificates will deliver significant identity management benefits in a digital environment. Certificates linked to verified, regularly updated and freely available entity reference data by a unique, universal identifier are easier to manage, aggregate and maintain. There will also be greater transparency overall across the digital identity ecosystem."This is an important step in promoting the LEI's capacity to enhance trust and add enormous value across the digital identity management systems which power the private sector," comments Stephan Wolf, GLEIF CEO. "A unified and proactive global approach to embedding LEIs in digital certificates will rapidly extend the benefits of LEI adoption beyond regulatory use cases. Our aim is for the LEI to be harnessed as an enabler of advanced transparency in digital transactions and exchanges, and for its positive impact to deliver advantage and opportunity across the economy and society. We look forward to working with our new stakeholder group members and reporting developments in this space very soon."

Naijin Lu, from CFCA's Strategic Development Department, comments: "CFCA is committed to incorporating the LEI into our digital identity products and we are already advanced in our related work efforts. We fully support this industry collaboration and are happy to be part of an initiative which brings the benefits of the LEI to a broad global audience, through an enhanced digital ID ecosystem." Dean Coclin, Senior Director of Business Development at DigiCert, comments: "DigiCert looks forward to participating in this important initiative to advance standards that strengthen online identity protections for users. Widespread use of LEIs, among other enhancements, may improve user confidence in websites, devices and online applications, and this is in the best interest of all internet participants." Cristina Andreoli, Business Compliance Consultant at InfoCert, adds: "InfoCert is fully behind participation in the GLEIF CA Stakeholder Group initiative. We recognize the value in the industry collaboration intended to share knowledge and coordinate efforts and actions to promote usage of the LEI within digital certificates and more widely, across the digital identity industry. We are excited to play our part."

GLEIF welcomes CAs and TSPs to join and participate in the CA Stakeholder Group's quarterly meetings. For more information or to join the group, please email info@gleif.org.

Published 11 March 2021

Our blog series on Regulation Tomorrow

Senior management and boards are increasingly acknowledging the threat of financial crime as a critical risk to their business that must be addressed. This has been exacerbated in the last 12 months through the impact of the pandemic as well as rising domestic and international tensions. Our financial crime compliance specialists, located in the UK, US, Canada, Australia and Asia, are looking ahead to 2021 to identify the incoming legislative changes, growing role of technology and the need for an effective regulatory response. This forms part of a seven part series which will assess amongst other things the expansion of virtual currencies, the growth of the role of the money laundering reporting officer, the changing world of sanctions regimes, and how the Biden Presidency could shape financial crime compliance into the future.

Part 5: The increasing emphasis of RegTech and FinTech in combating financial crime

Regulators across the globe are increasingly expecting and welcoming the use of technology to combat financial crime. Arguably, it's imperative that firms invest in compliance tech solutions to not only maintain compliant, but also keep pace with the ever-increasing sophistication of criminals seeking to subvert the law. The term financial technology ("FinTech") has become prevalent over the last decade to refer to technological solutions employed by financial services firms to enhance the use and delivery of their products/services to customers. Regulatory technology ("RegTech") is a subset of FinTech referring to when technology is used to optimise compliance and regulatory-related activities.

The digital revolution has paved the way for a wide range of RegTech players to make waves in the anti-financial crime space, and many have become embedded within business-as-usual processes. For example, a number of institutions now use facial recognition to enable users to access their online banking services, and tech to enable remote customer onboarding (whereby a customer's identity can be validated using a selfie augmented with uploaded photos of their passport or driving license) are now commonplace. However, the RegTech landscape continues to evolve at pace, and it's vital for financial crime compliance teams as well as senior management to remain aware of what's out there to proactively identify and resolve their unique compliance challenges in relation to their specific business operating model and footprint.

The up-and-coming RegTech use cases

There are a wealth of technology solutions which are geared up to address a number of financial crime compliance challenges. Many, such as artificial intelligence-led transaction monitoring alert hibernation and e-Know Your Customer tools (**eKYC**) are already playing a critical role in control environments at various institutions. However, some examples of more on-the-horizon technologies include:

1. **Machine learning for sanctions name screening**
   Sanctions name screening generates a high proportion of alerts which need to be dispositioned and, more often than not are closed as false positives. Machine learning can be used to review large historical decision-making which led to determination of false positives by human analysts to "learn" patterns and trends in order to apply similar logic for future dispositions. This is called supervised machine learning, whereby the user defines what is being looked for, and then the machine seeks to find "the needle in the haystack".
2. **Artificial intelligence in anti-money laundering (AML) transaction monitoring**
   Whilst supervised machine learning is good, often criminals deliberately make transactions appear legitimate. Therefore, the industry is moving towards unsupervised machine learning in the world of AML transaction monitoring to seek to uncover deliberately hidden behaviours (finding "the hay in the haystack") through overlaying large historic datasets with probability analysis and analytics.
3. **Enhanced workflow platforms for dynamic know your customer (KYC)**
   Whilst periodic reviews are to an extent effective in assessing a customer's risk profile on an ongoing basis, a better target state is dynamic KYC which updates following every customer transaction. This is currently being

piloted in simpler retail banking populations in some firms, with business banking set to follow in the short-term future and wholesale banking further down the track.

There are also a range of resources which can be leveraged to better understand AML technology use cases, such as those included in SAS's recent white paper on the topic of next generation AML.

Identifying the right solution to fit your needs and planning for implementation

With so many options now available from a RegTech perspective, deciding what solution is right for your institution can be a challenge. We recommend considering the following when determining which RegTech solution to invest in:

1. **What problem(s) do you need to address?**
   Starting with a use case and finding a solution to resolve that specific challenge is more beneficial than identifying a preferred technological solution and trying to reverse engineer it to fit the problem. This may mean that you need multiple technology solutions to address multiple challenges or pain points
2. **How will the solution integrate into your existing technology (and data) framework?**
   Any new RegTech solution risks becoming obsolete if it doesn't fit within your existing workflow. During the planning and implementation phase it is therefore crucial to conduct robust systems integration testing to help ensure optimal integration.
3. **What is the quality of your data that will feed the tech solution?**
   The performance of any RegTech solution is likely to be only be as good as its input(s). Therefore, you may need to consider whether a data overhaul/uplift is required prior to implementing a tech solution, such as standardising the way in which Know Your Customer (KYC) or transactional information is captured in the first place and inputted through your solution.
4. **To what extent does the tech solution need to be calibrated to your specific operating environment?**
   Many tech houses provide "out of box" or "off the shelf" solutions which often hold the allure of a lower price point. However, if your solution isn't tailored to your specific business and risk profile, you could risk generating output which is misleading. This could leave you (inadvertently) exposed to facilitating criminal behaviour.

Once you have concluded which technology solution(s) to implement, a pragmatic approach to implementation would be to start small. Following a risk-based approach, it would be most prudent to pilot your solution on lower risk perhaps more static populations. This will help to streamline the process of resolving teething issues and refining calibrations whilst keeping unnecessary additional risk exposure to a minimum.

Sustaining the change

It's vital that you can explain the outcomes generated by your tech solution. Whilst regulators don't expect every role in the firm to be able to talk to algorithms and data mining, there is an expectation that senior management display a level of tech savvy-ness. Buying a black box and blindly replying on the output which it generates would not be considered acceptable. This may require consideration for whether you and/or your compliance team need additional training and upskilling in order to be able to talk tech to your own Board, to other staff and to external regulators.

Finally, like with any anti-financial crime control, it's crucial to continually monitor the effectiveness of your RegTech solution to gain comfort that it generates anticipated outcomes and materially contributes to a reduction in residual risk. This will likely require close collaboration with your chosen RegTech partner to gain a mutual understanding of your business strategy, risk exposure and compliance needs to tailor your technological solution accordingly.

Conclusion

Seismic evolution in the capability and availability of technology has certainly led to a distinct uplift in adoption of RegTech solutions. This has been supported by regulators globally demonstrating support for tools which both optimise efficiency as well as drive effective financial crime risk management. New use cases and solutions continue to

develop, and confidence in the right technology has arguably elevated from both a regulator and financial institution perspective.

The use of technological solutions for financial crime compliance is anticipated to continue to grow, and therefore firms need to be actively assessing where their pain points lie and what solution(s) can be explored to resolve these. A key takeaway is that one size does not fit all and there is a strong expectation for any tech solution implemented to be reflective of the size, nature and risk exposure of the firm.

Published: 11 March 2021

Contact details:

Hannah Meakin
Partner and Co-head of FinTech Regulation
London
Norton Rose Fulbright LLP
Tel +44 20 7444 2102
Hannah.Meakin@nortonrosefulbright.com