Creating innovative, competitive environments

Chapter 6

Part of the Evolving Asset Management Regulation report

June 2018

kpmg.com/eamr2018

Creating innovative, competitive environments

Even if divergence is the regulatory watchword of 2018, in some areas of asset management, regulators seem to be in lockstep. Chief among these is the necessity of evolving regulation to facilitate the development of "fintech".

Fintech is becoming a priority for many asset management firms. It has the potential to revolutionize their business models, bringing greater efficiency to financial transactions, for example, and helping firms and regulators meet the increasing demands for data.

In the main, regulators recognize the benefits of new technologies and are seeking to accommodate them. But they are also concerned about existing risks that could be heightened by the new forms of services.

They are also evolving regulation to become more fit-for-purpose in a digital age. "Big data", robo-advice, crowdfunding and cryptocurrencies are all in the regulators' sights.

The sprint for fintech supremacy

The **European** Commission has made provisions for the use of fintech in existing legislation, including in MiFID II[1], the Payment Services Directive and in European Market Infrastructure Regulation. In 2017, it issued a consultation paper on the development of its policy approach towards technological innovation in financial services. It is seeking "a genuine technology-enabled single market for retail financial services".

In March 2018, the Commission launched its FinTech Action Plan. The plan outlines 19 steps to enable innovative business models to scale up, to support the uptake of new technologies, and to increase cybersecurity and the integrity of the financial system.

The steps include setting out a "blueprint" with best practices on regulatory sandboxes and work on a common standard for distributed ledger technology (DLT) to enable connectivity between different networks. The Commission also plans to create a Europe-wide financial technology laboratory, where policymakers can discuss regulatory approaches to new technology in the finance sector.

The Commission believes an EU-wide fintech platform for regulators could address the problems of regulatory divergence across Europe. Several national regulators, including in the **UK, France** and the **Netherlands**, have already set up regulatory laboratories, giving rise to a potential slew of different rules across the EU. In **Ireland**, the CBI[2] announced in April 2018, that it intends to establish an 'innovation hub' for firms, both start-ups and incumbents, to engage directly with the CBI on innovation and FinTech.

The **UK**'s FCA[3] indicated it would open up its financial technology innovation lab to international regulators. The UK regulator has been operating a regulatory sandbox since 2016 and says it has received a number of membership enquiries from firms outside the UK.

Indeed, in February 2018, the FCA and the **US** Commodity Futures Trading Commission signed a fintech co-operation agreement. The agreement focuses on information sharing on fintech market developments, and pools insights from innovation competitions and sandbox projects. It will allow UK and US fintech players to enter each other's markets without red tape.

Also in February 2018, the FCA proposed a "full multilateral sandbox", structured as an "international college of regulators" already operating their own sandboxes. This would enable firms to conduct tests in different jurisdictions at the same time, and allow regulators to solve common cross-border regulatory problems, said the FCA.

Similarly, MAS[4] in **Singapore** has signed agreements with authorities in other jurisdictions to foster collaboration in the development of fintech ecosystems and to encourage greater innovation. Bilateral agreements were signed with Egypt and Lithuania in 2018. Other jurisdictions include Denmark, the Philippines, Poland, Malaysia, Thailand, France, Hong Kong and Japan. In addition, MAS launched a SGD 27 million grant to promote the further use of artificial intelligence and data analytics in the financial services market.

Most countries are, for the moment, developing fintech-related regulation at a purely local level. These include **Switzerland**, where FINMA[5] reviewed its ordinances and circulars, and found them to be largely technology-neutral. It issued a circular to facilitate client onboarding via digital channels (video identification), which came into force in March 2016, and the regulator said it aimed to further a fintech-friendly environment, having launched a regulatory sandbox.

The **French** AMF[6] said that it will continue to support innovative projects, notably via its dedicated FinTech, Innovation and Competitiveness division, created in 2016, and to discuss changes in the regulatory framework due to new types of offer, in particular Initial Coin Offerings (ICOs). However, it is not keen to adopt a sandbox approach to deal with innovations within Europe and believes that a level-playing field – which might include some element of proportionality – should apply to all players, be they new entrants relying on technology or established players.

In **Bahrain**, the CBB[7] similarly introduced a regulatory sandbox for fintech. To be eligible to participate, firms must show the CBB that they have an innovative product of tangible benefit to customers and a well-developed regulatory testing plan. Firms must also submit a sandbox exit strategy that demonstrates their intention and ability to deploy the proposed solution in Bahrain. Bahrain currently has six approved fintech firms in the sandbox.

[1] Markets in Financial Instruments Directive, revised
[2] Central Bank of Ireland
[3] Financial Conduct Authority
[4] Monetary Authority of Singapore
[5] Financial Market Supervisory Authority
[6] Autorité des Marchés Financiers
[7] Central Bank of Bahrain

In addition, the Bahrain Economic Development Board launched the Bahrain Fintech Bay, which it said is the largest dedicated fintech hub in the Middle East and Africa. The new hub aims to further the development and acceleration of fintech firms as well as the interaction between investors, entrepreneurs, government bodies and financial institutions.

In the **UAE**, the Dubai International Finance Centre has undertaken considerable regional advertising for its own fintech sandbox, accompanied with conferences and other events. Meanwhile, the Abu Dhabi Global Market opened what it billed as the first "RegLab" in the region, a tailored regulatory regime for fintech participants.

In **Japan**, the "Online Transactions in FinTech era Research Group" was jointly established by the FinTech Association, Japan Association of New Economy and the JFSA[8].

In addition, a "FinTech Demonstration Experiment Hub" was set up as part of Japan's "In the Future Investment Strategy 2017". Thematic teams are formed in the hub to address topics such as compliance and oversight risks and practical issues on legal interpretations. A bill to establish a regulatory sandbox was also passed.

In **Canada**, the Ontario Securities Exchange (OSC) created LaunchPad, a dedicated regulatory team which supports fintech businesses; and in **Indonesia**, the regulator's strategic priorities for 2018 include supporting fintech.

The **Guernsey** regulator has established an Innovation Soundbox and the **Jersey** regulator has a Regulatory Sandbox for prospective clients and service providers, where existing or future licensees can discuss and test ideas, innovations or future applications. The Innovation Soundbox has already been used successfully, for example with the recent launch of the world's first private pquity blockchain in Guernsey.

DLT attracting plenty of attention

DLT is a potential fintech game changer. It has huge potential implications for settlement of financial transactions, and for firms' back and middle offices. The technology aims to prevent fraud by using a public digital database that is continuously maintained and verified by the other computers in a chain of transactions.

In **Europe**, ESMA[9] identified possible benefits in clearing and settlement, record of ownership and safekeeping of assets, reporting and oversight, reduction of counterparty risk, efficient collateral management, continuous availability, security and resilience, and cost reduction. DLT might also be used to enhance pre-trade information and the matching of buyers and sellers.

The European Commission, in early 2018, announced it would invest up to EUR 340 million over the next two years to identify regulatory risks and business opportunities linked to "blockchain" technology. The proposed EU Blockchain Observatory and Forum, launched with the support of the European Parliament, will highlight key developments of DLT, promote European firms and reinforce European engagement with multiple stakeholders involved in DLT activities.

The Commission wants the EU to become a leading world region in the technology. It has been funding projects through the EU's research programs, FP7 and Horizon 2020, since 2013.

The Commission seeks to build on existing DLT initiatives, ensure that they work across borders, consolidate expertise and address challenges, such as disintermediation, trust, security and traceability. It will enable cross-border co-operation on practical use cases, bringing together Europe's various experts and stakeholders, including public authorities, regulators and supervisors.

In **France**, securities not traded via a central securities depository or a securities settlement system can now be represented and transmitted using DLT. The securities covered by the French initiative are equities, debt securities, short-term debt securities and units of collective investment undertakings. The regulatory and legal framework is under construction: the Blockchain Ordinance sets the framework and provides for the use of the technology. It will become applicable by 1 July 2018.

In response, the central securities depositary has proposed new fund distribution standards, including encouraging the use of DLT in the sales process, as part of efforts to make French funds more attractive to international investors.

In **Switzerland**, FINMA has been supporting efforts in developing and implementing DLT solutions in the Swiss finance industry for several years. And in **Ireland**, the Department of Finance published a discussion paper on virtual currencies and blockchain technology, and announced the subsequent creation of an internal working group to monitor further developments in this area.

[8] Japanese Financial Services Agency
[9] European Securities and Markets Authority

Regulators won't give fintech a free ride though

Despite the potential benefits, innovation is causing regulators to question whether current rules and supervisory approaches for fintech are fit for purpose.

Caution is increasingly being expressed about the need to address risks in the new technologies. In early 2017, the FSB[10] chair, Mark Carney, warned that some innovations could generate systemic risks through increased interconnectedness and complexity, greater herding and liquidity risks, more intense operational risk and opportunities for regulatory arbitrage. However, in its mid-term review, in July 2017, the FSB concluded that there were "currently no compelling financial stability risks from emerging Fintech innovations".

Nevertheless, fintech is largely untested and this worries regulators. The **European** Central Bank's committee on payments and market infrastructures, believes DLT, for instance could pose new risks to the financial system, including uncertainty about operational and security issues. Its report cited potential legal and operational obstacles: "Having many nodes in an arrangement creates additional points of entry for malicious actors to compromise the confidentiality, integrity and availability of the ledger".

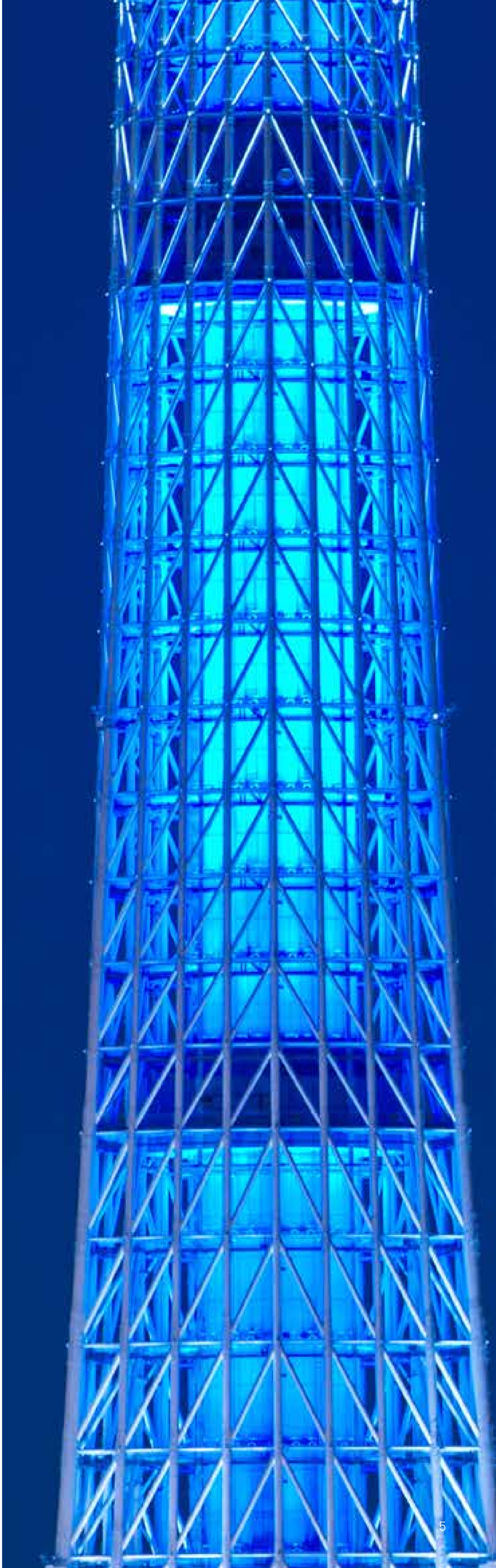
ESMA examines DLT

ESMA has also consulted on the application of DLT, aiming to identify its benefits, risks and challenges in securities markets, and ways of addressing the risks. Before DLT is applied for larger-scale purposes, ESMA is concerned that its legal certainty and broader legal issues – such as corporate, contract, solvency and competition laws – need to be considered and clarified. Key risks identified by ESMA are cyber, fraud, money laundering, operational, herding behavior (increased market volatility) and unfair competition.

The **UK** financial regulator, on the other hand, is worried that DLT could lead to a lack of individual accountability at firms. In a paper on distributed ledgers, published in December 2017, the FCA warned that the collaborative nature of the technology meant it might be difficult to tell who is responsible for decisions.

It said that the use of the technology "might affect how individual responsibility and accountability is allocated". The regulator said this could be the case even if a firm used a permissioned blockchain, where the number of parties were restricted.

[10] Financial Stability Board



The FCA said firms will have to set out clearly each manager's personal responsibilities, in line with the SMCR[11].

Big data is worrying regulators too. The FSB in late 2017 highlighted the potential risks associated with the growing use of artificial intelligence (AI) and machine learning and warned they must be monitored by regulators. The Basel-based regulator warned that "the lack of interpretability or auditability of AI and machine learning methods could become a macro-level risk", with a "widespread use of opaque models" potentially resulting in unintended consequences.

Another potential risk identified by the regulator is that the use of AI and machine learning could lead to a dependency on third-parties and create "the emergence of new systemically-important players that could fall outside the regulatory perimeter".

However, the FSB did state that more efficient processing of information would make the financial system more efficient.

In **Bahrain**, the CBB has brought the outsourcing cloud services within its regulatory purview. It has mandated certain minimum security measures that must be in place before a cloud outsourcing arrangement can be undertaken, including encryption of customer information, maintenance of a secure audit trail and that the release of customer data to foreign governments or courts is the sole responsibility of the licensee and subject to CBB approval.

Industry challenges				Solutions for a successful regulatory ecosystem
Inability to holistically evaluate adherence to local and global regulatory requirements	Unmanaged voluminous and complex regulatory data	Costly manual maintenance and inadequate monitoring of regulatory changes	Segmented and inefficient business models and operating procedures	A regulatory ecosystem's regulatory horizon scanning should address an institution's ability to: • Source laws and rules at a domestic and global scale that allows for easy consumption and identification of impacted relevant data • Seamlessly monitor new and changed regulations and trends • Quickly prioritize regulatory changes to quickly determine impact of the change across the entire firm
Failure to properly respond to changes with flexibility due to lack of enterprise wide framework	Incapability to convert regulatory text into business obligations	Lack of workflow and case management to properly monitor changes	Inadequate collection and mapping of key data elements needed to provide an end-to-end view	A regulatory ecosystem's risk and compliance mapping and assessment allows for the ability to: • Comply with regulations by integrating a suite of automated and cognitive tools in an enterprise-wide technology framework • Provide a comprehensive view of mapped data elements, enabling the support for change management and compliance • Efficiently and effectively convert regulatory text and requirements into business obligations and workflow items to owners for compliance evaluation
Incapability to address functionality and operational gaps	Inability to develop action plans and testing programs	Inability to associate obligations to testing programs to monitor and test	Absence of innovative technology to efficiently accelerate tests, results, and rule automation	A regulatory ecosystem's compliance monitoring and testing allows for the ability to: • Derive testing programs across multiple business data elements to automate testing • Enhance monitoring and testing by evaluating operating and control effectiveness and properly identifying and remediating gaps • Accelerate testing through machine learning
Fragmented reporting, inadequate data standards and management controls	Deficiency in meeting heightened reporting demands	Undefined global data model and lineage	Inadequate level of granularity to link obligations and processes	A regulatory ecosystem's customized analytics, reporting, and data management allows for the ability to: • Provide comprehensive view of how the organization has met compliance to the requirements • Standardize testing methodology and reporting that easily provides analytics for predictive forecasting and identification of touch points for regulatory change • Globally manage regulatory and test data and identify lineage

[11] Senior Managers Certification Regime

Cybersecurity remains a top priority

Cybersecurity is another essential component of the regulatory view of fintech.

In **Singapore** in September 2017, MAS established a cybersecurity advisory panel, comprising thought leaders from around the world. The panel will advise on strategies to enhance the cyber resilience of the Singaporean financial sector. In November 2017, MAS and the Financial Services Information Sharing and Analysis Centre launched a pan-Asia Pacific initiative to share cyber threat information in a timely manner and to enable a rapid and co-ordinated response to emerging threats. And in February 2018, the government passed a Cybersecurity Bill with new powers for the Cyber Security Agency.

ESMA announced it would create a forum for senior supervisors in the **EU** during the course of 2018 to help develop common approaches to cyber security and cyber resilience. The move follows a call by the European Commission for regulators to examine cyber resilience, citing cyber-attacks as a key threat to financial stability.

In **Germany**, BaFin[12] said it would add rules and principles on cybersecurity to secure the roll-out of digital strategies of UCITS[13] and AIF[14] management companies.

The issue is taken seriously the world over. In **Bahrain**, the CBB has recently mandated that cyber security controls are periodically evaluated for adequacy, taking into account emerging cyber threats and establishing a credible benchmark of cyber-security controls.

The CBB also requires reporting to it any instances of cyberattacks, whether internal or external, which compromise customer information or disrupt critical services that affect firms' operations. The reporting should be accompanied by the root cause analysis of the cyber-attack and measures taken by them to ensure that events do not re-occur.

The **UK**'s FCA has proposed a requirement for independent directors of fund management company boards to address the "under-reporting" of cyberattacks. Megan Butler, the FCA's director of supervision for investment, wholesale and specialists, said during a speech in late 2017 that the UK regulator expects "candour" from financial firms, particularly on cyberattacks. She said: "Our suspicion is that there's currently a material under-reporting of successful cyberattacks in the financial sector."

In **Australia**, APRA[15] has published a consultation on a prudential standard on information security to address the growing threat of cyberattacks. The proposed standard includes requirements on governance, capability, controls and detection mechanisms. It also includes assurance over the cyber capabilities of third parties, such as service providers, and improving entities' ability to respond to and recover from cyber incidents.

In April 2018, the three **European** Supervisory Authorities (ESAs) issued a report on risks and vulnerabilities in the financial sector. Cyber risks have become a "significant and highly escalating threat to investor protection, the financial markets and their stability worldwide," they said. They called on financial institutions to improve their IT systems and explore risks to information security, connectivity and outsourcing.

Big data continues to attract the interest of regulators

It seems that no discussion of technology is complete without reference to "big data". The ESAs believe the phenomenon has the potential to grow and that a firm's capacity to use big data may be a key determinant of its future competitive advantage. Having consulted in early 2017, the ESAs issued their final report in March 2018.

The ESAs define big data as the collection, processing and use of high volumes of different types of data from various sources, using IT tools, in order to generate ideas and solutions or to predict certain events or behaviors. They observe the increase in the use of big data, albeit to varying extents across the sectors and across the EU. They recognize that its use could transform the way products and services are provided, which could provide benefits for consumers and financial institutions.

However, there are attendant risks. The potential for errors could lead to incorrect decisions taken by financial services providers, for example, and the increasing segmentation of the customer base is influencing market and product access. The ESAs note that consumers should be made aware of the risks.

Taking into account the benefits and the risks associated with the use of big data, the ESAs have concluded that any legislative intervention at this point would be premature. They note that existing legislation should mitigate many of the risks identified (see the discussion in Chapter 3 on new data protection rules, for example). They will, however, continue to monitor developments and invite financial firms to develop and implement good practices on the use of big data.

[12] Bundesanstalt für Finanzdienstleistungsaufsicht
[13] Undertaking for Collective Investments in Transferable Securities
[14] alternative investment fund
[15] Australian Prudential Regulatory Authority

Robo-advice comes under regulatory scrutiny

Robo-advice is being scrutinized by regulators across the globe as the numbers of platforms and users increases. The key regulatory concern is that consumers should receive appropriate advice, the same as in the traditional face-to-face advice business model. The use of technology raises the added concern that, if there is an error in the programming or technological process, it may not be picked up without human intervention. Also, consumers may presume that their inputs and the computer must be right without question or double-checking.

Most regulators believe their existing rules are adequate. A number, though, are seeking to clarify the difference between general information, generic advice and personal recommendations, and are requiring regulated firms clearly to disclose the type of service they are offering and its limitations. Some regulators acknowledge that their supervisory techniques must evolve.

Singapore, for example, recognizes the gaining popularity of digital advisory services and welcomes such offerings to complement existing advisory channels. MAS has proposed amendments to regulations to address the unique characteristics and risks of such services. It is concerned with the minimum standard of client care, governance and management oversight, and that the methodology should be sufficiently tested and robust.

In **Europe**, EFAMA[16] has urged ESMA not to impose more onerous rules for an investment service "that is quite similar [to face-to-face advice], though provided through digital means".

EFAMA highlighted a resolution adopted by the European Parliament's Economic and Monetary Affairs Committee in 2017 that said: "the same consumer protection requirements should apply to robo-advice as to face-to-face advice". It disagrees with ESMA's recommendation that robo-advice firms need to focus on providing sufficient information to clients given the "limited" – or even non-existent – human interaction these firms have with end-investors.

ESMA recommends that robo-advisers provide information on the algorithm they use, an explanation of the degree of human involvement in the service, and how the firm will use suitability information to develop a solution for the end-investor. But EFAMA warned that further disclosures for robo-advice companies may have an adverse effect, leading to information overload.

In **Germany**, the BVI said that the implementation of the additional requirements would require firms to carry out "an extensive re-modelling of existing websites and client onboarding". According to the BVI, one of its members estimated that such a process would cost about EUR 3.5 million and take up to a year to undertake.

In the **Netherlands**, the regulator found major shortcomings in the way robo-advisers onboard new clients. It warned that some robo-advisers are placing too much responsibility on clients by requiring them to determine their own risk profiles. "Many businesses simply use a digital version of their hard copy question list to determine their client's investment goals and risk appetite", said the regulator. "Failing to accommodate for the differences between physical and online advice, such as the absence of human contact, generally doesn't produce sound advice."

Bitcoin encounters skepticism

Unsurprisingly given their volatility, bitcoin and other cryptocurrencies have encountered considerable skepticism in the investment industry. The **US** has pointedly refused to give the green light to funds based on cryptocurrencies. Dalia Blass, a director at the SEC[17] sent a letter in February 2018 to two firms, containing more than 30 questions that needed to be resolved before the SEC would allow the launch of mutual funds and ETFs[18] that invest in cryptocurrencies.

Ms. Blass's letter was a response to numerous applications from ETF providers to launch funds tracking cryptocurrencies. In December 2017, two exchange operators, CBOE Global Markets and CME Group, launched bitcoin futures markets, spurring a handful of ETF providers to submit new applications.

The US regulator also raised concerns over the potential lack of liquidity if investors rushed to redeem their shares if bitcoin remained volatile.

In **Japan**, the Coincheck hack in January 2018 has triggered considerable regulatory scrutiny. Hackers stole more than USD 500 million in virtual currency from Coincheck, a cryptocurrency exchange. In the wake of the attack, Japanese regulators announced on-site inspections at all unlicensed cryptocurrency exchanges.

However, official regulatory moves were supplanted by swift self-regulation. Just a few weeks after the hack, 16 exchanges had put together a self-regulatory regime, which governs exchanges previously registered with the JFSA. The new regime replaced an earlier plan to merge two bodies – the Japan Cryptocurrency Business Association and the Japan Blockchain Association.

[16] European Fund and Asset Management Association
[17] Securities and Exchanges Commission
[18] exchange-traded fund

The ICO market has come under regulatory scrutiny as the source of all potential cryptocurrency funds.

In view of the development of fundraising based on the use of crypto assets and DLT, and the risks associated with these transactions, the **French** AMF consulted on three possible supervisory options for a specific legal framework for ICOs:

1. Promote a best practice guide without changing existing legislation
2. Extend the scope of existing texts to treat ICOs as public offerings of securities
3. Propose new legislation adapted to ICOs

Option 3 received the strongest support, attracting nearly two-thirds of responses. In addition, there was unanimous support for an information document for buyers of tokens, which should include, at a minimum, information on: the project related to the ICO and its advancement; the rights conferred by the tokens; and the accounting treatment of funds raised during the ICO.

The AMF continues to work on the design of a flexible and tailored framework for ICOs, which could take the form of an optional authorization regime together with the delivery or not of a visa from the regulator.

Switzerland’s FINMA is relatively positive on ICOs. In late 2017, it issued guidance stating that ICOs may be subject to financial market laws depending on the characteristics of the ICO on a case-by-case basis. Potential links to collective investment schemes legislation may arise where the assets collected as part of the ICO are managed externally. New guidance from FINMA regarding ICOs and tokens was published in March 2018. Among other pronouncements, the guidance established that tokens qualify as securities if they are “standardized and suitable for mass trading”. However, FINMA added that the issuance and trading of tokens will be analyzed on a case-by-case basis.

In the Channel Islands, the **Jersey** Commission also sought to clarify the regulatory treatment of ICOs. A Jersey company issuing digital coins or tokens in Jersey now needs to obtain a consent from the Commission prior to setting up the operation. For consent to be given, the Commission considers the marketing material, which must contain clear consumer warnings highlighting that the ICO is unregulated and may result in substantial risks.

In **Guernsey**, the regulator has noted that “virtual or cryptocurrencies could interact with our regulatory laws in a number of ways and therefore any application would need to be assessed on its individual merits.”

European Commission Vice President Valdis Dombrovskis in December 2017 warned retail investors against buying bitcoins.

Meanwhile, **Germany** and **France** called for international scrutiny into digital currencies amid concerns that a "lack of clarity for investors … can only fuel speculation". The two countries issued their call in a letter to the G20.

BaFin outlines cryptocurrency risks

The German regulator views the key risks for investors as:

- Total loss
- Regulatory risks: up until now, most ICO issuers have not been regulated or supervised
- Lack of specific investor and consumer protection
- Information insufficiency: ICOs do not provide information for investors that is comparable to prospectuses or key investor information documents
- Opaqueness and complexity: being based on complex technological mechanisms, ICO structures remain opaque for most investors
- Volatility and liquidity risks: the value of coins is volatile and potentially illiquid as there are no secondary markets
- Operational risks: ICOs are prone to fraud, from wrongfully-drafted contracts, theft of private keys and abuse of program codes

BaFin supported a warning on ICOs by ESMA and issued several warnings of its own on consumer protection in relation to cryptocurrencies, in late 2017. It highlighted potential fund management impacts. It saw open issues around the qualification of coins and tokens as financial instruments or transferable securities, as well as the authorization requirements for fund management companies.

BaFin believes ICO risks may be mitigated by applying a robust regulatory environment on issuers of ICOs. It points to ESMA's consideration of whether ICO structures may qualify as AIFs. That would mean ICO issuers falling under the umbrella of the AIFMD. Alternatively, coins or tokens may qualify as financial instruments under MiFID II. This, in turn, could lead to them being eligible assets for UCITS.

Formal consultations on the regulatory environment of ICOs, cryptocurrencies and relevant derivative products have not yet been set by BaFin but are expected over the course of 2018. A clue to the direction of BaFin's thinking was provided, in April 2018, by its authorization of a fund investing in cryptocurrencies and blockchain technologies. Meanwhile, there is an increasing number of calls for ESMA to propose a pan-EU approach.

Crowdfunding gets its own rules

In **Singapore**, MAS simplified the rules for securities-based crowdfunding platforms to facilitate start-ups and small- and medium-sized enterprises. In particular, it simplified the pre-qualification checks that platforms must perform on investors and reduced the capital and operational risk requirements of the platform operators.

Under its FinTech Action Plan, the **European** Commission has issued a proposed regulation of crowdfunding. Crowdfunding improves access to funding, especially for start-ups and other small businesses, it says. A start-up can present its project on an online platform and call for support in the form of a loan (peer-to-peer lending) or equity. Investors receive a financial return for their investment.

The Commission observes that it is currently difficult for many platforms to expand into other EU countries. This is why crowdfunding in the EU is underdeveloped as compared to other major world economies, the Commission claims, with one of the biggest hurdles being the lack of common rules across the EU. This considerably raises compliance and operational costs and prevents crowdfunding platforms from expanding across borders.

Once adopted by the European Parliament and the Council, the proposed regulation will allow platforms to apply for an EU label based on a single set of rules, enabling them to offer their services across the EU. Investors on crowdfunding platforms will be protected by rules on information disclosures, governance and risk management, and by a coherent approach to supervision.

“...currently difficult for many platforms to expand into other EU countries”

Meanwhile, in February 2018, the **French** AMF published a position-recommendation on the marketing of security and mini-bond offers and the run-off management of platforms. It applies to crowdfunding investment advisors and investment services providers offering crowdfunding advice. It integrates the major principles already published by the AMF on marketing of financial products to retail clients and adapts them to the specific online nature of crowdfunding.

Technology by the regulators, for the regulators

It is perhaps natural that regulators seek to use technology to perform their role, similar to the firms they supervise. **Japan** is one of the jurisdictions leading the way in this regard.

In **Canada**, the OSC hosted the first regulatory "hackathon", in which fintech firms collaborated on finding solutions to everyday problems that impact the work of the OSC.

The **UK**'s FCA is another national regulator seeking views on how it can use new technologies to facilitate reporting to it by authorized firms. In its Call for Input, in February 2018, the FCA outlined how its "proof of concept" approach was developed at its TechSpring event in November 2017. It asked for views on how it can improve the process, seeking feedback on the role technology can play in regulatory reporting.

The consultation closes on 20 June 2018, and a statement summarizing the views received and the proposed next steps is due to be published in the following months.

Tom Brown
Global Head of Asset Management
KPMG International
T: +44 20 7694 2011
E: tom.brown@kpmg.co.uk

Julie Patterson
Head of Asset Management
Regulatory Change, Risk & Regulatory
Insight Centre, EMA
T: +44 20 73112201
E: julie.patterson@kpmg.co.uk

kpmg.com/eamr2018

Designed by Create Graphics | CRT094255A