Tech REG CHRONICLE™

FINTECH

MAY 2022

CPI COMPETITION POLICY INTERNATIONAL™

Competition Policy International, a What's Next Media and Analytics Company

LETTER FROM THE EDITOR

Dear Readers,

Financial Technology (or, more snappily, "FinTech") has been on the rise in recent years. Financial markets are subject to multiple legal regimes, which act in parallel to ensure that consumers and investors can have faith and security in the integrity of the financial system. FinTech raises certain novel concerns that regulators (including antitrust authorities) are currently grappling with.

FinTech is a broad term, but, at its essence, it refers to new technology that seeks to improve and/or automate the delivery and use of financial services. Initially, the term FinTech was used to refer primarily to innovations employed at the so-called "back-end" systems of established financial institutions. Increasingly, however, new technology has been deployed to refer to consumer-focused services encompassing education, retail banking, fundraising and nonprofit sectors, and investment management, to name but a few.

Perhaps the most prominent example of FinTech disrupting existing financial markets has been the rise of cryptocurrencies (though despite their meteoric success, for now, the bulk of regulation remains focused on governing the established financial institutions, in light of their sheer market power). The articles in this Chronicle run the gamut of the FinTech space, with a specific focus on antitrust rules (and how they interact with existing regulatory regimes).

Marcel Haag opens with a timely piece querying what the the regulatory approach to FinTech should be in the EU? Should the existing set of regulatory regimes apply (with the caveat that certain parts that fail the existing criteria should be banned)? Or is there a need for a new, bespoke regulatory regime (or set of regimes) for novel financial services? The European Commission has embraced a forward-looking policy towards digital finance; spanning the domains of both Fintech and so-called "BigTech." The article focuses in particular on

two proposed legislative frameworks in the pipeline: the proposal for a Distributed Ledger Technology pilot regime and the proposal for a Regulation on Markets in Crypto-Assets.

In turn, Michael McKee & Marina Troullinou discuss developments in the UK. The Financial Conduct Authority ("FCA") – the UK's regulator for financial services – has a specific role in promoting effective competition financial services for the benefit of consumers. The so-called "regulatory sandbox" is one of the FCA's main tools in this regard. It allows innovators to test new products in a live market environment in close collaboration with the FCA. In addition to being a testing platform for firms, it is also a forum to foster cooperation between the FCA and market innovators. The article explores how the sandbox has evolved since its introduction in 2016; and offers insights on how it has worked in practice.

Andrew Godwin discusses the challenges for regulatory design in the area of cryptocurrencies. The article focuses on the likely direction of reform in Australia and examines the challenges inherent to the area (not least in reference to the definition of what crypto assets even are). In terms of possible reform, the article suggests, inter alia, a move away from a prescriptive, rules-based approach in favor of a principles-based approach, and the conferral of greater powers and flexibility on regulators to adapt to challenges brought about by technology.

Christopher B. Leach focuses on how the U.S. Federal Trade Commission ("FTC") has shown itself to be among the industry's most active regulators. The agency enforces not only the broad prohibition on unfair and deceptive acts and practices, but also a range of laws, including ECOA, TILA, and the FCRA, among many others. Indeed, the article brings out the fact that FinTech regulation is the archetypal "alphabet soup" of multiple laws and regulators; due in no small part to its novel nature. In particular, the article focuses on the agenda of the newly-minted chair of the FTC (Lina Khan) and her likely moves in this rapidly-evolving space.

Susan Joseph addresses calls for a comprehensive federal scheme that would recognize privacy as a fundamental right. Specifically, these calls call for solutions that would be architecturally developed from the individual privacy point of view. Such so-called "trust frameworks" will need to mesh with new laws that support privacy as a fundamental right.

Finally, Lee Reiners focuses on issues related to the regulation of cryptocurrencies as potential commodities. Should crypto assets be regulated by analogy with assets that are currently regarded as commodities, or be subject to a bespoke regime? This is a question that legislators and other policymakers will face for years to come.

As always, many thanks to our great panel of authors.

Sincerely,
CPI Team

TABLE OF CONTENTS

CPI COMPETITION POLICY™ INTERNATIONAL

FINTECH

MAY 2022

SUMMARIES

FINTECH REGULATION – THE EU APPROACH
By Marcel Haag

What should be the regulatory approach to FinTech? Should it be about bringing FinTech under the roof of the current regulatory regime and possibly banning any parts that cannot fit? Should it be about leaving FinTech alone and unregulated? Do we need a bespoke regulatory regime? Should disruptive innovation be encouraged or held back? This article presents the emerging EU regulatory approach to FinTech in relation to financial services. The European Commission has embraced a forward-looking policy towards digital finance aiming to regulate innovation in and not out, while at the same time addressing and monitoring the potential risks and challenges resulting from FinTech and BigTech. The article focuses in particular on two examples of innovative legislative frameworks currently in the pipeline: the recently agreed proposal for a Distributed Ledger Technology pilot regime and the proposal for a Regulation on Markets in Crypto-Assets. Both are examples of new innovative frameworks directed at FinTech. Together, they have the potential to spur innovation in the field of financial services and to help bringing them to the next technological level.

INNOVATION: THE EVOLUTION OF THE FCA SANDBOX
By Michael McKee & Marina Troullinou

Promoting innovation in financial services has been at the top of the UK's regulatory agenda over the last years. The UK's "pro-innovation" regulatory environment for financial services is considered by many as a key driver of continuing growth of the UK's fintech sector and a necessary element for ensuring that the UK remains a leading global fintech hub. The Financial Conduct Authority ("FCA") – which is the UK's conduct regulator for financial services – has a specific mandate to promote effective competition in the financial services sector for the benefit of consumers. The regulatory sandbox is one of the FCA's main tools to support innovation and thereby fulfil its competition mandate. The regulatory sandbox allows innovators to test new products in a live market environment in close collaboration with the regulator. In addition to being a valuable testing platform for firms, the sandbox is also a unique forum which fosters cooperation between the FCA and market participants to support innovation. This article explores how the regulatory sandbox has evolved since its introduction in 2016 and offers insights on how it has worked in practice.

CRYPTO ASSETS AND THE CHALLENGES FOR REGULATORY DESIGN
By Andrew Godwin

This article discusses the challenges for regulatory design in the area of crypto assets and suggests the likely direction of reform in Australia. It examines the challenges by reference to the definition of crypto assets, questions that are relevant to the regulation of crypto assets, the current regulatory framework for crypto assets in Australia, and the likely direction of reform in Australia. In terms of the likely direction of reform, the article suggests a move away from a prescriptive, rules-based approach to regulation in favour of a more principles-based approach, the expansion in the regulatory net to include providers of crypto-asset services, and the conferral of greater powers and flexibility on regulators to adapt to challenges brought about by technology.

A PROPOSAL FOR OVERSIGHT OF DIGITAL ASSET SPOT MARKETS IN THE U.S.
By Lee Reiners

Recent turmoil in the digital asset market has renewed calls for greater oversight of the sector. Unfortunately, the uncertain legal status of digital assets in the U.S. complicates efforts to more vigorously regulate them. The Commodity Futures Trading Commission ("CFTC") has classified Bitcoin and Ether – and by extension other cryptocurrencies that are similarly structured – as commodities (courts have also upheld this classification). While the CFTC regulates commodity derivatives, they do not regulate commodity spot markets, although they do have enforcement authority for fraud and manipulation in commodity spot markets. The practical effect of this structure is that cryptocurrency exchanges in the U.S. are not regulated at the federal level (they are required to register with the Financial Crimes Enforcement Network and obtain state money transmitter licenses). This article explores potential options for addressing the gap in digital asset spot market regulation and recommends that Congress grant the Securities Exchange Commission exclusive authority over all facets of the digital asset market, from spot to derivatives, by creating a special definition of security under the securities laws that would incorporate digital assets.

PRIVACY IN A TECHNOLOGICAL AGE

By Susan Joseph

In our data-driven society, privacy as a fundamental right should be recognized and upheld. We must adopt strong legal and technological protections that preserve our autonomy. Legally speaking we must establish a comprehensive federal scheme that recognizes privacy as a fundamental right. Technologically speaking, solutions that are architecturally developed from the individual privacy point of view should be deployed. These trust frameworks will need to mesh with new laws that support privacy as a fundamental right. New types of decentralized/blockchain identity systems are coming online and evolving which support privacy rights and restore the balance of power between the individual and service provider. These systems are disruptive, potentially very profitable, and will impact status quo business models. Tensions between the old and new will have to be resolved. With legal and technological means working together, we can protect our right to be left alone. Privacy is possible in the digital age.

FINTECH & THE FEDERAL TRADE COMMISSION

By Christopher B. Leach

As the fintech industry has evolved over the past decade, the Federal Trade Commission has proved to be among the industry's most active regulators. Acting through a multi-member, bipartisan structure, the agency enforces not only the broad prohibition on unfair and deceptive acts and practices, but also a range of proscriptive laws, including ECOA, TILA, and the FCRA, among many others. As a result, the FTC has broad experience in the fintech space, dealing with issues related to lead generation, B2B payments, digital assets and payment processors (again, among many others). Companies should expect increased scrutiny with Lina Khan now leading the FTC as its Chair, given her ambitious rulemaking and enforcement agenda. Some of her appeared to have stalled for several months due to a democratic vacancy on the FTC, leaving the FTC with a 2-2 democrat-republican split. But with the confirmation of the third democratic commissioner, Alvaro Bedoya, Chair Khan now should have a voting majority to pursue her agenda. In this article, Christopher Leach, a partner with Mayer Brown and a former attorney with the Federal Trade Commission, explains the FTC's enforcement trends for in the fintech space and where Chair Khan may take the agency during her term.

FINTECH REGULATION – **THE EU APPROACH**

BY
MARCEL HAAG

Director for Horizontal Policies at DG FISMA – European Commission.

FinTech (short for financial technology) is a term that refers to the integration of technology into offerings by financial companies to enhance the use and quality of financial services and their delivery to consumers. Until recently, FinTech was considered to be an emerging, still marginal phenomenon. However, technological advances and recent events such as the global pandemic have accelerated the increase in offerings of and demand for FinTech solutions in financial services and other sectors to an extent that by now FinTech has irreversibly altered the way we perceive the provision of financial services across all fields of financial activity.

FinTech companies come in all shapes and sizes. They can be micro startups, SMEs, es-

tablished financial institutions that wish to develop internally their own FinTech solutions as part of their business model, or even large technology companies (the so-called "BigTech" companies) trying to enter the market and replace or enhance the usage of financial services provided by existing financial companies. With recent technological developments and the increased availability of FinTech solutions, more companies are able to enter the market and provide financial services. BigTech companies in particular often act as intermediaries, bundling their services and products with associated financial services. These companies can scale up their services quickly, given their large number of users. This has the potential to radically change market structures.

Digital technologies have made it possible for firms to specialize in a particular link of the value chain. Thus, technology is contributing to breaking up previously integrated value chains for certain financial services. This can increase competition and improve efficiency. However, it also makes value chains more complex, making it harder for supervisors to have an overview of the related risks. If some actors in the value chain are not regulated entities, the supervisory authority may lack full information of or control over the whole structure. The new business models need to be examined and analyzed carefully to understand the risks and opportunities associated with them and to propose the right policy solutions.

Financial regulation needs to adjust to technological developments and the new types of companies that emerge and provide services. It needs to address associated risks for consumers, counterparts, and the financial system. The European Commission has committed to adapt, where necessary, the existing conduct and prudential EU legal frameworks to safeguard financial stability and market integrity and to protect consumers.

> ***Financial regulation needs to adjust to technological developments and the new types of companies that emerge and provide services***

FinTech is often not about an entirely new product or a new service or a new type of service provider. It is frequently about new technology that may enable already existing products or services to be offered in a different and more efficient way, reaching a greater number of potential users. When developing policy on FinTech, therefore, the issue is not so much about devising a new tailormade framework to regulate the new technology, but rather about finding ways to allow this new technology to be used by existing products, market infrastructures and service providers, while addressing any additional risks that this technology might pose, in particular to consumers.

The European Commission has opted for a forward-looking approach to digital finance aiming to regulate innovation in and not out, while at the same time addressing and monitoring the potential risks and challenges resulting from FinTech and BigTech. It has realized early on that if Europe is to reap the benefits of innovations such as distributed ledger technology, artificial intelligence, and cloud computing, it has to maximize the European single market's potential so that companies can scale up across borders. This is how efficiency gains can be made and consumers can get more choice and access to cutting-edge digital tech, with better products and services at lower prices. This is essential if European companies are to compete with their peers, for example from Asia or the United States.

The Digital Finance Strategy[2] set out the Commission's intention to review the existing financial services legislative frameworks to protect consumers and safeguard financial stability, protect the integrity of the EU financial sectors, and ensure a level playing field. It highlighted that faster, more open, and collaborative innovation cycles call for regular examination of and adjustments to EU financial services legislation and supervisory practices, to ensure that they support digital innovation and remain appropriate and relevant in evolving market environments. Rapid and disruptive change based on technological progress is testing regulation and supervision in many fields, but it is particularly challenging in the area of FinTech.

The strategy points to risks for the financial ecosystem and for financial services value chains. Technology companies – large and small – are increasingly entering financial services markets. For example, several of these companies already provide payment services but responses to the Commission's public consultation suggest that they are likely to expand into other financial services as well.

The European Commission has embraced FinTech as a development that can potentially bring great opportunities and has adopted a number of proposals aimed at regulating several key elements of FinTech, which are related to technology and to activities linked to crypto-assets. This article focuses on two examples of innovative legislative frameworks currently in the pipeline: the recently agreed Distributed Ledger Technology pilot regime and the proposal for a Regulation on Markets in Crypto-Assets which is still being negotiated.

2 COM (2020) 591) adopted in September 2020.

As part of its Digital Finance Strategy, the Commission proposed the Markets in Crypto-Assets Regulation ("MiCA"), which seeks to promote responsible innovation within crypto-asset markets and ensure that market integrity, consumer and investor protection and financial stability are preserved. The EU has been ahead of other jurisdictions in proposing a comprehensive regulatory framework and aims to set the benchmark in crypto-assets regulation. The proposal was necessary because existing EU law did not cover adequately the dimension of crypto-assets as a major FinTech development.

The proposed MiCA framework addresses the issuance of crypto-assets, the requirements for crypto-asset service providers and the supervision of issuers and service providers for crypto-assets. It covers crypto-assets not qualifying as financial instruments and distinguishes between asset referenced tokens ("ARTs"), electronic money tokens ("EMTs"), and those crypto-assets that fall into neither of these two categories. Asset referenced tokens are those types of crypto-assets that aim to maintain a stable value by referencing one or several fiat currencies that are legal tender, one or several commodities, one or several crypto-assets or a combination of these. Electronic money tokens (or e-money tokens) are those types of crypto-assets that are intended to be used as a means of exchange and that aim to maintain a stable value by referencing the value of an official currency of a country. Both ARTs and EMTs are also generally known as stablecoins. Any other digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology is considered to be a crypto-asset.

The MiCA framework seeks to provide legal certainty for innovators to allow them to navigate financial legislation and scale across the EU. It builds on three main principles:

· Preserving market integrity;

· Ensuring consumer and investor protection;

· Securing financial stability – if and when crypto-assets acquire a market presence that could trigger stability issues.

MiCA implements international recommendations from the Financial Stability Board ("FSB") as regards stablecoins and also from the Financial Action Task Force ("FATF"), ensuring that together with the updated AML framework, all AML/CFT risks are appropriately mitigated.

From early on, the EU has been promoting international coordination in the area of crypto-assets and in particular of stablecoins and has been actively participating in all relevant fora such as the G7, FSB and FATF. These innovations present the biggest opportunities but also the biggest risks, where their use across borders offers global efficiency gains, and the EU will continue and step up their work with international partners to promote cooperation and supervisory convergence based on common principles and standards.

By the time the Commission presented its MICA proposal there were already signs of fragmentation in the EU, with some Member States establishing rules for crypto-assets. The need to comply with multiple and sometimes conflicting rules puts an additional burden on companies operating in this space and hampers their ability to develop and scale up across the internal market. An EU-wide harmonized framework will replace existing national rules, reduce complexity and administrative burden, provide legal clarity, and facilitate crossborder activities. It will mean that a crypto-asset service provider authorized in a Member State will benefit from an EU passport and be able to operate across the entire EU single market.

A concern that is frequently raised in the context of FinTech is that crypto-assets could offer opportunities for illicit activities like money laundering or terrorist financing. The notion of "virtual currencies" is defined under the existing EU Anti Money Laundering Directive. Providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers are considered to be "obliged entities" for the purpose of anti-money laundering rules and as such, are required to follow anti money laundering checks and procedures. The objective of the Anti-Money Laundering Directive regarding virtual currencies was to control the "gatekeepers," i.e. the providers of services to EU consumers which makes the link between the virtual sphere and the real world.

A concern that is frequently raised in the context of FinTech is that crypto-assets could offer opportunities for illicit activities like money laundering or terrorist financing

However, the crypto-assets area is evolving very fast and compared to the Financial Action Task Force's Recommendation adopted in June 2019, the Commission has identified some gaps that need to be closed: The notions of "virtual asset" and "virtual asset service provider" as included in the FATF's recommendation are broader than the notions of "virtual currency" and the above-mentioned services providers covered in the current Anti Money Laundering Directive. The MiCA proposal therefore uses the terms "crypto-assets" and "crypto-asset service providers" that are in line with the FATF Recommendations.

The overhauled AML framework proposed in July 2021, cross-refers to MiCA, bringing in scope a range of new crypto-asset service providers as obliged entities. At the same time, the proposed update of the Transfer of Funds Regulation has also included information requirements for transfers of crypto-assets. This will lead to the implementation of the so-called "travel rule" from the FATF.

A second cause of concern regarding FinTech in general and crypto-assets in particular relates to the environmental footprint that is caused by the mining of certain crypto-assets. This concern refers to the environmental impact and high energy needs of DLT, notably for certain crypto-assets. As set out in the European Commission's strategy for financing the transition to a sustainable economy,[3] this is an area where the EU will need to assess the sustainability impact of digital finance technologies. The Commission argues that the EU should take the lead in making these infrastructures climate neutral and energy efficient by 2030. For this purpose, it can build on previous initiatives to promote sustainable data centers.

A further, equally important framework related to FinTech is the Commission proposal for a Distributed Ledger Technology Pilot Regime Regulation ("DLT Pilot") on which a political agreement was reached in November 2021. It will soon become part of the legislative framework and will apply from next year. Distributed ledger technology is a technology that supports the distributed recording of encrypted data. It is a way of keeping records of transactions and is shared across a network whereby these transactions are validated and stored and can be traced when needed. It is an important innovation because where previously transactions were created and stored only by intermediaries, DLT can run without third party involvement and is also highly transparent, secure, and tamper-proof.

The overhauled AML framework proposed in July 2021, cross-refers to MiCA, bringing in scope a range of new crypto-asset service providers as obliged entities

In the area of trading and settlement of financial instruments DLT can bring a number of benefits, notably in terms of efficiency, security, and transparency. However, the current rules have not been written with this technology in mind and may hamper the wider use of this technology the trading and post-trading areas. While the use of DLT has the potential to improve efficiency more information is needed before legislation can be overhauled. The DLT pilot regime aims to achieve just that, by allowing for some limited and temporary exemptions from existing rules where they could pose technical obstacles to achieve the full benefits of using DLT. The DLT pilot will enable market participants to safely experiment with DLT to issue, trade and settle securities in a controlled setting.

The pilot will run for five years and will be reviewed at the end of this period in order to determine whether to make it permanent, amend it or abandon it. It means that DLT is currently tested in a 'sandbox'. The experience gained will inform future policymaking and could potentially lead to more wide-ranging changes. This framework is a first of its kind in the EU and will enable the EU to move the forefront of innovation in this field. The experience gained can also be useful to develop general principles for the implementation of regulatory sandboxes in other fields.

Also in data driven finance, work is progressing in the Commission on the creation of an open finance framework to allow the access to and the reuse of business-to-business and business-to-consumer data with customer consent across a wide range of financial services. This framework will be developed in a bottom-up approach, building on a close cooperation with experts and stakeholders. For that purpose, an expert group is analyzing different use cases and assessing issues of data availability and data accessibility in finance. An open finance framework will build on the Commission's broader European Data, which aims at the creation of an internal market for data through cross-sectoral rules on data use that are, in principle, also applicable in the financial sector.

Ensuring fair competition and a level playing field, including with technology firms, within an open data space is an essential aspect in this context. Due consideration will also have to be given to the opportunities and the risks in light of the lessons learnt from the implementation of the second Payment Services Directive ("PSD2"),[4] which led to new players entering the payments market, offering new and innovative solutions previously unavailable. Open finance will mean to give more control to the users of financial services, be it consumers or firms, when it comes to the way their data is used and to who can access the data. It is a FinTech innovation with the potential to significantly improve the consumer and user experience in financial services.

What is then the EU's approach to FinTech? It is about recognizing the potential of FinTech and improving the regulatory environment to be more conducive to innovation

3 COM (2021) 390, July 6, 2021.

4 COM (2020) 66, February 19, 2020.

while minimizing its risks. It is about enabling the scaling up of FinTech services across an EU-wide internal market and beyond. And it is about staying ahead of the game and embracing technological change where it increases efficiency and is beneficial to consumers and companies and to society at large. Responsible innovation in FinTech can and will improve the products and services offered, and the European Commission will be there to help see it through.

> *Ensuring fair competition and a level playing field, including with technology firms, within an open data space is an essential aspect in this context*

INNOVATION: THE EVOLUTION OF THE FCA SANDBOX

BY MICHAEL MCKEE

& MARINA TROULLINOU

Partner & Associate, DLA Piper UK LLP, respectively.

01 INTRODUCTION

Promoting innovation in financial services has been at the top of the UK's regulatory agenda over the last years. The UK's "pro-innovation" regulatory environment for financial services is considered by many as a key driver of con-

tinuing growth of the UK's fintech sector and a necessary element for ensuring that the UK remains a leading global fintech hub. The Financial Conduct Authority ("FCA") – which is the UK's regulator for financial services – has a specific mandate to promote effective competition in the financial services sector for the benefit of consumers.

The regulatory sandbox is one of the FCA's main tools to support innovation and thereby fulfil its competition mandate. The regulatory sandbox allows innovators to test new products in a live market environment in close collaboration with the regulator. In addition to being a valuable testing platform for firms, the sandbox is also a unique forum which fosters cooperation between the FCA and market participants to support innovation. This article explores how the regulatory sandbox has evolved since its introduction in 2016 and offers insights on how it has worked in practice.

02

WHAT IS THE REGULATORY SANDBOX AND HOW DOES IT WORK?

One of the key objectives of the FCA includes promoting effective competition in consumers' interests. The FCA sees innovation as an essential element of its competition mandate. Innovation enables new entrants to challenge incumbent institutions, deliver inventive products and services for consumers and potentially reduce operating costs in financial services.[2]

In this context, in 2014, the FCA launched a dedicated Innovation division (formerly known as "Project Innovate") with a specific focus on promoting innovation and competition in the financial services sector.[3] The regulatory sandbox forms part of Project Innovate's offering. The initiative was first introduced in November 2015, with the first slot (known as a "cohort") opening for applications in June 2016.

The regulatory sandbox allows businesses to test innovative propositions in a live – but yet "controlled" – market environment with real customers. It was initially divided into two cohorts per year, each running for a six-month testing period. From August 2021, the sandbox is permanently open for applications throughout the year.

A. Not Just for Start-ups

The sandbox is addressed to a broad range of firms with a business model which is relevant to financial services. The FCA encourages participation from innovative firms from all backgrounds, with a view to accelerating "*the change needed to promote more diverse and inclusive practices across FinTech*."[4] Since its launch, the FCA has received over 500 applications from firms wishing to participate in the sandbox.[5]

The sandbox is not dedicated exclusively to authorized firms, or firms that require a regulatory license to operate in the UK. Rather, the sandbox is also open to firms with business models that generally fall outside the regulatory perimeter, but nevertheless wish to develop products and services which can support the financial services industry. A typical example includes technology providers that are looking to deliver solutions for the financial services market.

> ***In this context, in 2014, the FCA launched a dedicated Innovation division (formerly known as "Project Innovate") with a specific focus on promoting innovation and competition in the financial services sector***

The sandbox is not exclusively addressed to the start-up fintech crowd. A number of incumbents have tested their own applications in the context of the sandbox, ranging from large banks (such as Barclays, Natwest, Standard Chartered Bank, Nationwide, and Experian) to market infrastructure service providers (the London Stock Exchange Group). Even the UK Post Office has participated in the

2 Supporting innovation in financial services: the digital sandbox pilot, April 2021.

3 https://www.fca.org.uk/publication/research/the-impact-and-effectiveness-of-innovate.pdf.

4 https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

5 https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms.

sandbox to test an app relating to digital identities.[6] Law firms have also joined the innovation arena – for example, international law firm DLA Piper tested its own RegTech application which allows firms to digitally manage regulatory compliance to support digitalized issuance processes.[7]

Firms that are interested to participate must submit an application explaining how they satisfy the FCA eligibility criteria, including setting out what makes their proposition "genuinely innovative" and how it is anticipated to benefit consumers, businesses or financial markets more generally.[8]

Products and services admitted for testing range from blockchain-based payment services, platforms which tokenize issuance of financial instruments to RegTech propositions, financial education platforms and sustainable finance investment platforms.

In 2018, Deloitte in collaboration with Innovate Finance (which is an industry body representing the UK FinTech sector) undertook a survey[9] interviewing several sandbox participants from the first four cohorts. According to the report findings, "the unequivocal message" was that sandbox experience was a valuable one for participants who benefited in a variety of ways, from receiving regulatory guidance to helping them "kicking the tires" on the risks involved in their business model.[10] The report also found that the sandbox also resulted in certain "unexpected benefits" for firms, noting in particular that:

> "While the FCA has emphasised strongly that it does not "pick winners"[11], the feedback from our interviews is that being accepted into the sandbox, and proving the underlying technology in a live environment, increased the credibility of firms with both investors and customers alike."[12]

B. What Should Firms Expect from Participating in the Sandbox?

The sandbox provides firms with access to regulatory expertise and facilitates testing through a variety of available "tools." Firms admitted in the sandbox are assigned a dedicated FCA case officer, who is responsible for supporting the firm in their sandbox journey. This includes helping them navigate the various regulatory requirements, getting clarity around their test parameters and objectives and ensuring that the test is undertaken effectively.[13] The case officer can also act as a link between the firm and other departments within the FCA, which may be relevant for the particular test in question.

"The sandbox provides firms with access to regulatory expertise and facilitates testing through a variety of available "tools."

Generally speaking, undertaking regulated activities in the UK requires authorization or registration, unless an exemption applies. This means that a number of businesses operating in the financial services space will require authorization just to be able to test their application with real customers. This can be a significant barrier to entry, particularly for smaller firms with limited resources to access legal support. A tool available to sandbox firms is that they can apply for "restricted authorization." This is a fast-track process which allows firms to obtain authorization quickly in order to test their Minimum Viable Product ("MVP"), but subject to specific parameters and limitations tailored around the test (for example limitations around the types and number of customers they can take on or volume of

6 https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms.

7 https://www.dlapiperintelligence.com/investmentrules/blog/articles/2020/two-of-our-projects-accepted-into-the-fca-sandbox.html.

8 https://www.fca.org.uk/firms/innovation/regulatory-sandbox/eligibility-criteria.

9 https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-fca-regulatory-sandbox-project-innovate-finance-journey.pdf.

10 https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-fca-regulatory-sandbox-project-innovate-finance-journey.pdf.

11 https://www.fca.org.uk/news/speeches/uk-fintech-regulating-innovation.

12 https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-fca-regulatory-sandbox-project-innovate-finance-journey.pdf.

13 https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf.

transaction they are allowed to undertake). Firms can then decide, based on the outcome of the test, if they wish to go for full authorization.

Other firms may be providing services which are at the fringes of the regulatory perimeter and may require guidance on how to avoid triggering any regulatory requirements. For example, this may apply to technology firms that want to know whether they act as a simple (unregulated) technology provider or whether their business model means that they require authorization to operate in the UK. Equally, a proposition may push the boundaries of the regulatory perimeter in novel ways and may, therefore, not fit squarely within existing regulations and guidance. In those cases, there are tools available that aim to help firms navigate the various FCA rules. For example, this ranges from helping firms identify the rules and guidance that may be applicable to their business model (known as "signposting") to providing "informal steers" on potential regulatory implications of the proposed project. In certain cases, it may even involve providing individual guidance, setting out how the FCA would interpret the requirements in that particular case.

The FCA is given extensive powers under the sandbox, including the ability to waive or modify certain of its rules for the purposes of a test, if deemed to be unduly burdensome, or even issuing a "no enforcement action" letter for the duration of the test.

03
BEYOND THE UK: THE GLOBAL SANDBOX

The Global Financial Innovation Network ("GFIN") – an international network of financial services regulators and relevant organizations – was launched in January 2019, building on the FCA's earlier proposal for the creation of a "global sandbox."[14] The GFIN is led by the FCA, which also acts as chair.

Among other things, a key objective of GFIN is to facilitate cross-border testing of innovative solutions with an international element, and in particular *"to provide a more efficient way for innovative firms to interact with regulators, helping them navigate between countries as they look to scale new ideas,"* including "*the ability to conduct a cross-border test – a solution for firms wishing to test innovative products, services or business models across more than one jurisdiction*."[15]

The idea of a global testing platform appears as a natural continuation of national sandbox initiatives, particularly in the context of markets which are inherently global. In practice, however, its implementation has not been without its challenges. Following the first testing pilot phase in 2019, GFIN published a lessons learned report reflecting on the pilot outcomes and feedback.[16]

"The idea of a global testing platform appears as a natural continuation of national sandbox initiatives, particularly in the context of markets which are inherently global. In practice, however, its implementation has not been without its challenges

Even though the concept of "cross-border testing" appeared to be "self-explanatory" for participating regulators, the report found that firms had varying interpretations of what constituted a cross-border test.[17] This meant that GFIN received applications which did not necessarily have "inherent" cross-border characteristics as originally expected. Rather it appeared that a number of firms were hoping to use the global sandbox as an opportunity to be introduced by one national regulator to another national regulator, with a view to exploring market entry opportunities in the relevant jurisdiction.[18] The result was that firms applied to more jurisdictions than originally anticipated. Coupled with the fact that firms were expected to submit applications in all jurisdictions where they were interested to undertake testing, in prac-

14 https://www.fca.org.uk/firms/innovation/global-financial-innovation-network.

15 https://www.fca.org.uk/firms/innovation/global-financial-innovation-network.

16 https://www.thegfin.com/s/GFIN-CBT-Pilot-lessons-Learned-publication-09012020-FINAL-8247.pdf.

17 https://www.thegfin.com/s/GFIN-CBT-Pilot-lessons-Learned-publication-09012020-FINAL-8247.pdf.

18 https://www.thegfin.com/s/GFIN-CBT-Pilot-lessons-Learned-publication-09012020-FINAL-8247.pdf.

tice this meant that, in certain cases, firms submitted up to 14 applications for the same test (with most firms filing 4 to 6 applications on average).[19]

In addition, according to the report, although GFIN expected to receive more interest from larger and international institutions with cross-border operations, there was "a noticeable lack of applications" from this type of firms. This may have been due to the short application window (which was only one month), but it may also indicate that the value of participating in the global sandbox was not made sufficiently clear for firms.

Overall, among 44 applicants, only eight firms were initially admitted for cross-border testing as part of the pilot. However, following six months of working with the respective national regulators to set out joint testing plans, only two firms managed to proceed to the actual testing phase.[20] The remaining six were not ready to meet all the relevant regulators' expectations. This was partly due to the fact that, in some jurisdictions, firms cannot be admitted in the sandbox unless they are already authorized to provide financial services or have partnered with an authorized firm for the purposes of the sandbox. This meant that some firms could not appropriate local partners in time.

04

THE POWER OF DATA: THE DIGITAL SANDBOX

As the UK financial services sector is becoming increasingly more digital, the FCA has seen heightened demand for support services focusing on data and data access.[21] The emergence of new market participants, on the one hand, coupled with extensive digital transformation efforts among incumbent institutions, on the other hand, means that data is playing an increasingly more prominent in financial services. At the same time, market participants, and especially new market entrants, require access to more comprehensive consumer and market data in order to develop innovative technological solutions.[22]

Against this backdrop, in 2021, the FCA in collaboration with the City of London Corporation ("CoLC") launched a pilot of the "Digital Sandbox" – a digital testing environment for technology solutions.

This initiative aims, among other things, to fill a gap in the early-stage "proof of concept" phase of product development by providing participants with access to synthetic and publicly available data in order to facilitate testing of prototype technology solutions. In addition, the Digital Sandbox pilot aims to support innovators by offering a "market-place" for application programming interface ("API") solutions, where digital service providers can list and grant access to services using APIs, as well as a coding development environment. It is also intended to operate as a collaboration platform between sandbox participants and mentors and an "observation deck" for regulators to "observe in-flight testing at a technical level" and "inform policy thinking" in a controlled environment.[23]

> ***"As the UK financial services sector is becoming increasingly more digital, the FCA has seen heightened demand for support services focusing on data and data access***

The pilot was focused on three areas – preventing scams and fraud, supporting vulnerable consumers and promoting SME financing. Feedback[24] on the pilot suggested that the Digital Sandbox generally delivered value for firms and overall helped them accelerate product development. That being said, however, ensuring sufficient data quality across numerous topics proved more challenging than expected. In particular, the pilot evaluation report noted that:

19 https://www.thegfin.com/s/GFIN-CBT-Pilot-lessons-Learned-publication-09012020-FINAL-8247.pdf.

20 https://www.thegfin.com/s/GFIN-CBT-Pilot-lessons-Learned-publication-09012020-FINAL-8247.pdf.

21 https://www.fca.org.uk/firms/innovation/digital-sandbox.

22 https://www.fca.org.uk/publication/corporate/digital-sandbox-joint-report.pdf.

23 https://www.fca.org.uk/firms/innovation/digital-sandbox.

24 https://www.fca.org.uk/publication/corporate/digital-sandbox-joint-report.pdf.

"It is important to recognise that synthetic data is a nascent and enormously complex field. Even with world-leading expertise contributed by the Turing Institute, the Working Group was unable to create the required richness across so many data sets."

The second phase of the Digital Sandbox, which was launched in November 2021, was dedicated exclusively to the topic of environmental, social, and governance ("ESG") data and disclosure and associated new products and services.[25] In an effort to keep the scope narrow, and thereby ensure sufficient data quality, this "sustainability cohort" was focused on addressing specific market challenges in the chosen subject area. This included, for example, exploring how technology can be used in order to promote transparency in disclosure and reporting in relation to sustainability and how technological solutions can increase consumer understanding around the ESG features of products and providers and provide visibility around potential alternative solutions which may be more aligned with their needs and preferences.[26]

"The second phase of the Digital Sandbox, which was launched in November 2021, was dedicated exclusively to the topic of environmental, social, and governance ("ESG") data and disclosure and associated new products and services

05
THE FUTURE OF THE SANDBOX

As part of the 2020 Budget, the Chancellor asked Ron Kalifa OBE to undertake an independent review regarding the development of the UK fintech sector in the years ahead. This is commonly known as the "Kalifa Review."[27] The Kalifa Review "*sets out a series of proposals for how the UK can build on its existing strengths, create the right framework for continued innovation, and support UK firms to scale*," in order to support fintech growth and "*extend the UK's competitive edge over other leading fintech hubs*."[28]

Interestingly, the review's findings suggest that *"FCA's regulatory sandbox is already the busiest sandbox facility in the world."*[29] With a view to ensuring, among other things, that the UK retains its competitive edge in fintech, the Kalifa Review explores how sandbox initiatives can help to further promote the UK fintech sector and what steps must be taken to "enhance" the regulatory sandbox going forward. This includes, for example, making the regulatory sandbox permanently open for applications (rather than operating on a cohort basis), creating a dedicated space for identified "priority fintech areas" and introducing a "scalebox" to support fintech companies at the growth stage. In addition, the Kalifa Review recommended that the digital sandbox should be made permanent and that, in the longer term, it may be housed with an independent, non-regulatory body, with the participation of the FCA.

25 https://www.fca.org.uk/firms/innovation/digital-sandbox.

26 https://www.fca.org.uk/firms/innovation/digital-sandbox.

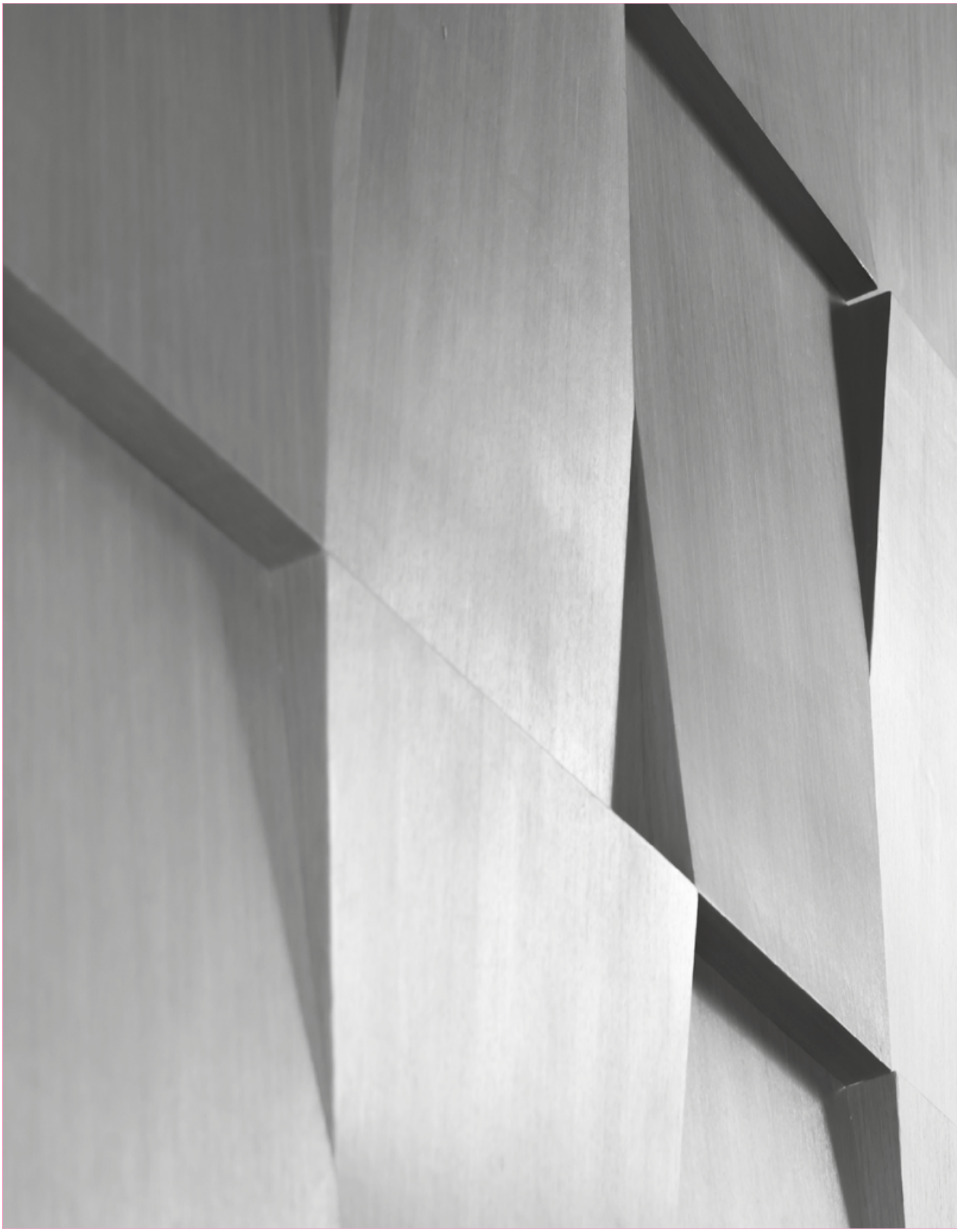
27 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978396/KalifaReviewofUKFintech01.pdf.

28 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978396/KalifaReviewofUKFintech01.pdf.

29 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978396/KalifaReviewofUKFintech01.pdf.

Overall, this demonstrates the UK's commitment to further develop and support sandbox initiatives going forward, with a view to fostering competition and innovation in the financial services sector and promoting the UK as a global hub for fintech. It also shows that this form of collaboration between public sector bodies and market participants can deliver value for both the regulator and firms, by enhancing the understanding of emerging regulatory issues and providing a hub to explore how technology and innovation can help build more inclusive, progressive and potentially safer financial markets.

> ***Interestingly, the review's findings suggest that "FCA's regulatory sandbox is already the busiest sandbox facility in the world.***



CRYPTO ASSETS AND THE CHALLENGES FOR REGULATORY DESIGN

BY
ANDREW GODWIN

Dr Andrew Godwin is Principal Fellow at Melbourne Law School, the University of Melbourne, and Special Counsel assisting the Australian Law Reform Commission in its current Review of the Legislative Framework for Corporations and Financial Services Regulation. This article is adapted from "The Australian Reform Agenda," presentation delivered by the author at the "Regulating Digital and Crypto-finance: A Conversation Across Borders" webinar hosted by the UCL Centre for Ethics and Law on March 22, 2022. For a recording of the webinar, see https://www.ucl.ac.uk/laws/events/2022/mar/online-regulating-digital-and-crypto-finance-conversation-across-borders.

01 INTRODUCTION

The past decade has seen extraordinary growth in technological innovation. The emergence of blockchain technology (and distributed ledger technology more broadly) has led to a range of innovations in area such as financial services. These innovations include new ways of raising finance, such as initial coin offerings ("ICOs"), new means of exchange for payment purposes, such as cryptocurrencies, and new asset classes, such as crypto assets (which include cryptocurrencies and tokens more broadly); and new forms of business, such as decentralized autonomous organizations ("DAOs"). The new terminologies and taxonomies that have emerged alongside these innovations have presented challenges for both regulators and

regulatory design. This article discusses the challenges for regulatory design in the area of crypto assets and suggests the likely direction of reform in Australia.

02
WHAT ARE CRYPTO ASSETS?

Crypto assets have been defined in a number of different ways. A recent consultation paper issued by the Department of the Treasury in Australia defined a "crypto asset" as follows:

"A crypto asset is a digital representation of value that can be transferred, stored, or traded electronically. Crypto assets use cryptography and distributed ledger technology."[2]

The above definition is similar to that adopted by financial regulators in Australia, including the market conduct regulator, the Australian Securities and Investments Commission ("ASIC"),[3] and Australia's central bank and payment systems regulator, the Reserve Bank of Australia ("RBA").[4] ASIC has noted that crypto assets "may also be commonly referred to as digital assets, virtual assets, tokens or coins," and that ASIC is "not aware of a universally accepted name for, or definition of, "crypto-asset."[5]

> ***Crypto assets have been defined in a number of different ways***

A legislative definition of "digital currency" appears in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), which is similar to the definition published by the Financial Action Task Force.[6] Singapore has adopted a legislative definition of "digital payment token" for the purposes of its payment services legislation.[7]

As noted by ASIC, crypto assets "are not a homogenous asset class."[8] The UK Government has stated that the main types of crypto asset including the following:

· **Exchange Tokens**. Exchange tokens are intended to be used as a means of payment and are also becoming increasingly popular as an investment due to potential increases in value. The most well-known token, bitcoin, is an example of an exchange token.

· **Utility Tokens**. Utility tokens provide the holder with access to particular goods or services on a platform, usually using [distributed ledger technology]. A business or group of businesses will normally issue the tokens and commit to accepting the tokens as payment for the particular goods or services in question. In addition, utility tokens may be traded on exchanges or in peer-to-peer transactions in [the] same way as exchange tokens.

· **Security Tokens**. Security tokens provide the holder of a security token particular rights or interests in a business, such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits.

· **Stablecoins**. Stablecoins are another prominent type of cryptoasset. The premise is that these tokens minimize volatility as they may be pegged to something that is considered to have a stable value such as a fiat currency (government-backed, for example U.S. dollars) or precious metals such as gold.[9]

2 Department of the Treasury (Cth), *Crypto asset secondary service providers: Licensing and custody requirements* (Consultation Paper, March 21, 2022). A similar definition is adopted by the UK Government. See *HMRC internal manual - Cryptoassets Manual,* available at https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10100. See also Art. 3(1)(2-5) of the proposed EU Markets in Crypto-Assets Regulation (MiCAR).

3 See ASIC, *Crypto-assets as underlying assets for ETPs and other investment products* (Consultation Paper, CP 343, 30 June 2021) at 7-8.

4 See Reserve Bank of Australia, "What are Cryptocurrencies?," available at https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html.

5 ASIC, *supra* note 3 at 8.

6 Financial Action Task Force, *Report: Virtual Currencies – Key Definitions and Potential AML/CFT Risks* (2014).

7 *Payment Services Act 2019 (No. 2 of 2019)* (Singapore).

8 ASIC, *supra* note 3 at 8.

9 UK Government, *supra* note 2.

The taxonomy for crypto assets in the proposed EU Markets in Crypto-Assets Regulation ("MiCAR") adopts a slightly different taxonomy for crypto assets. If enacted, MiCAR would regulate the following:

· "asset-referenced tokens," which includes stablecoins;

· "e-money tokens," which are a type of crypto asset whose main purpose is to be used as a means of exchange aimed at stabilizing their value by referencing only one fiat currency; and

· "crypto-assets other than asset-referenced tokens or e-money tokens," which include utility tokens that are issued for non-financial purposes and may include cryptocurrencies such as bitcoin.

MiCAR does not apply to security tokens, which are regulated as a "financial instrument" under the Directive on Markets in Financial Instruments, commonly known as MiFID2.[10] In addition, central bank digital currencies are exempted from MiCAR if they are issued by central banks acting in their monetary authority capacity or by other public authorities.

It is relevant to note that crypto assets, such as cryptocurrencies and tokens more broadly, are often created and issued by ICOs. The regulation of ICOs has also been the subject of examination and debate in many jurisdictions.

03

WHAT QUESTIONS ARE RELEVANT TO THE REGULATION OF CRYPTO ASSETS?

There are a number of questions that are relevant to the regulation of crypto assets. These are questions that all jurisdictions need to consider.

· **First**, should the regulatory framework in respect of crypto assets – particularly private cryptocurrencies – be prohibitive or permissive? In September 2021, the People's Bank of China declared that trading in cryptocurrencies was illegal and banned related activities, including fundraising through ICOs.[11] In South Korea, a ban on ICOs has also been in place since 2017. However, the government is reported to be considering removing the ban and bringing ICOs within the regulatory framework.[12] In India, the central bank, the Reserve Bank of India, issued a circular in 2018 prohibiting banks from providing services in connection with cryptocurrencies. This ban was later set aside by the Supreme Court in 2020. In November 2021, the Indian Government introduced the Cryptocurrency and Regulation of Official Digital Currency Bill into the Parliament. If enacted, the legislation would provide a framework for the creation of a central bank digital currency and prohibit all private cryptocurrencies in India, subject to certain exceptions "to promote the underlying technology of cryptocurrency and its uses." It is uncertain what the prohibition and its exceptions would mean for the development of DAOs and ICOs in India.

Jurisdictions in the region that are permissive in nature include Australia, Singapore, and the Hong Kong Special Administrative Region, all of which regulate tokens and ICOs by reference to the existing regulatory framework, and Japan, which began to develop a bespoke regulatory framework for cryptocurrencies in 2014 and is developing specific guidelines for ICOs.

· **Second**, how should tokens or crypto assets be classified and what taxonomy should be used for this purpose? This is a fundamental question as it is difficult to know how to regulate something if it is difficult to classify it for regulatory purposes. The taxonomical challenges have become greater as a result of the pace of change that has been brought about by technological innovation and also the extent to which new asset classes have come to be defined more by technology than by traditional concepts or labels. Some jurisdictions have undertaken token mapping

10 Directive 2014/65/EU.

11 China has, however, started to trial its central bank digital currency, the digital yuan.

12 See Timothy Craig, "ICOs Could Be Returning to South Korea," *Crypto Briefing* (January 19, 2022), available at https://cryptobriefing.com/icos-could-be-returning-to-south-korea/.

exercises to determine the best way to characterize the different types of token.[13]

· **Third**, who or what should be the target of regulation? A particularly important related question is who should bear responsibility if things go wrong. Given that it is very difficult, if not impossible, in a practical sense to regulate technology itself, the focus inevitably shifts to those who utilize the technology or provide services, such as distributed ledger technology services or "crypto-asset services" as referred to in MiCAR. There have been proposals in Australia to widen the regulatory net to include service providers.[14]

· **Fourth**, what regulatory style or method should be adopted for the regulation of crypto assets? For example, should jurisdictions favor a principles-based approach, over a prescriptive, rules-based approach? An example of a jurisdiction that has adopted a principles-based approach to the regulation of distributed ledger technology (DLT) providers is Gibraltar, where a DLT provider is required at all times to comply with specified regulatory principles. The principles include the requirement for a licensed DLT provider to "conduct its business with honesty and integrity"; "pay due regard to the interests and needs of each and all its customers and communicate with them in a way that is fair, clear and not misleading"; "have effective arrangements in place for the protection of customer assets and money when it is responsible for them"; and "have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing."[15]

Should jurisdictions favor a principles-based approach, over a prescriptive, rules-based approach?

· **Fifth**, should crypto assets be subject to bespoke (i.e. separate) regulation or instead be incorporated into an integrated regulatory framework? As noted above, some jurisdictions have regulated crypto assets within their existing regulatory framework and by analogy with the regulation of existing products and concepts. In these jurisdictions, crypto-specific provisions and definitions have appeared in legislation dealing with anti-money laundering (e.g. in Australia) and in payments legislation in order to attract the relevant licensing and other requirements (e.g. Singapore and the UK). By contrast, jurisdictions such as Gibraltar have adopted bespoke regulations, as outlined above. Many jurisdictions have also adopted a regulatory sandbox to provide an opportunity for technology-based products and services to be tested under controlled conditions outside the formal regulatory framework. In all contexts, a key concern is consumer protection.

· **Sixth**, what is the impact of the applicable regulatory model in the relevant jurisdiction? This question often has greater relevance than is recognized. A related question is whether there is a single market conduct and consumer protection regulator and a single rule book for this purpose, or multiple regulators and different rulebooks for different sectors or industries. The Twin Peaks regulatory model, under which regulation is objectives-based and functionally split between a market conduct regulator and a prudential regulator, has been recognized as being conducive to technological innovation. As noted by Professor Howell Jackson of Harvard University,

> …one of the advantages of Twin Peaks systems is that they are better suited to reach beyond traditional sectors to areas such as finance companies (New Zealand) or Fintech innovations (Hong Kong). With the rise of Big Tech and the ever-rising importance of various flavors of shadow banking, the comparative advantages of Twin Peaks structures should continue to grow. Objectives-based supervision may just be a better fit for the Twenty-First Century economy.[16]

· **Seventh**, what are the regulatory objectives, principles or philosophy that guide a jurisdiction in its reg-

13 See Department of the Treasury (Cth), *supra* note 2 at 3: "Consistent with the Government's response to the Senate Report, a token mapping process will be completed as a separate piece of work and finalised by the end of year," and, at 12, "the token mapping exercise to be completed by end of 2022 will provide further clarity as to how crypto assets are classified on a risk-based and technology agnostic basis."

14 See Department of the Treasury (Cth), *supra* note 2 at 3.

15 Financial Services (Distributed Ledger Technology Providers) Regulations 2017 (Gibraltar).

16 Andrew Godwin & Andrew Schmulow (eds), *The Cambridge Handbook of Twin Peaks Financial Regulation* (Cambridge University Press, 2021), Foreword at xix.

ulation of crypto assets? By way of example, since the late 1990s when the design of corporations and financial services legislation was significantly influenced by an inquiry called the Wallis Inquiry, Australia has subscribed to the principle that there should be "similar (or same) regulatory treatment for functionally equivalent products." This has been a guiding principle in relation to the development of regulation in this area for the past 25 years. A critical challenge with a functional approach, however, is how to define and assess functional equivalence.

The UK, by comparison, has been guided by the principle of "same risk, same regulatory outcome." A risk-based approach has some attractiveness, but there is a challenge in determining how to measure risk as it is applied to products and activities.

Under its Digital Finance Strategy, the EU has adopted an approach to financial stability, based on the principle of "same activity, same risk, same rules." This is similar to the approach in the UK, but appears to represent a more activities-based approach. This also has some attractiveness, but it requires clarity around the classification of crypto assets, which has been identified as a challenge under MiCAR.[17]

It is also important to consider the relevance of general regulatory principles, such as the need for regulation to be technology-neutral; in other words, not to favor one technology over another.[18]

04

WHAT IS THE CURRENT REGULATORY FRAMEWORK FOR CRYPTO ASSETS IN AUSTRALIA?

To date, Australia has regulated crypto assets by reference to the existing legal and regulatory framework and has not enacted bespoke laws or legal provisions. To some extent, a holistic approach to the regulation of crypto assets is predestined as a result of Australia's functional approach to regulating financial products, and also the functional nature of the Twin Peaks regulatory model, involving a single market conduct and consumer protection regulator in financial services in the form of ASIC and a separate prudential regulator in the form of the Australian Prudential Regulation Authority ("APRA"). The functional approach to regulating financial products and to financial supervision creates a certain path dependency that favors a holistic approach to reform.

Adopting the functional approach, section 763A of the *Corporations Act 2001* (Cth) provides that a financial product is a "facility"[19] "through which, or through the acquisition of which, a person does one or more of the following":

- "makes a financial investment";
- "manages financial risk"; or
- "makes noncash payments."

The functional approach to the definition of "financial product" in the Corporations Act means that if crypto assets or tokens function as financial products under any of the three categories set out above, they will be regulated as such and will attract the relevant obligations, including those in respect of licensing and disclosure. One of the benefits of the functional approach is that it recognizes the challenges in designing regulation by reference to labels as distinct from the function of a particular product or activity.

By contrast, many other jurisdictions rely on exhaustive lists of financial products or services to regulate securities, financial products, or investment products. Australia appears to be unique in relying on a broad, functional definition of "financial product" – a point that was noted and explored in some detail in the first Interim Report issued by the Australian Law Reform Commission in its review into the simplification of corporations and financial services regulation in Australia.[20] Similarly, the United States adopts a functional test – the Howey Test – to determine whether a transaction is an "investment contract."[21] This test, however, is relevant

17 A key issue that is subject to debate is the difficulty in drawing lines between the different types of token and the challenges that this may create in terms of regulatory arbitrage. See Dirk A. Zetzsche, Filippo Annunziata, Douglas W. Arner & Ross P. Buckley, "The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy" (2021) 16(2) *Capital Markets Law Journal* 203.

18 See Department of the Treasury (Cth), *supra* note 2 at 6: "The Government identifies the following objectives for the proposed regulatory regime: ensuring that regulation is fit for purpose, technology neutral and risk-focussed…"

19 The term "facility" is defined in s 762C.

20 Australian Law Reform Commission, *Interim Report A: Financial Services Legislation* (ALRC Report 137, November 2021) at 287 [7.66].

21 As decided in *Securities and Exchange Commission v. W. J. Howey Co., 328 U.S. 293* (1946), an investment contract is "a contract, transaction or scheme whereby a person invests [their] money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party."

to determining what qualifies as a "security," and thereby attracts the disclosure and registration requirements, and does not cover financial or investment products more broadly.[22]

Although the functional approach in Australia appears attractive, ASIC has noted that it "can cause uncertainty for investors and consumers as well as issuers and distributors of these assets" and that "[i]t is a policy matter for government whether or not there should be clarity on this issue."[23] Of course, a key issue is how regulatory clarity might be provided. The next section examines the likely direction of reform in Australia.

05

WHAT IS THE LIKELY DIRECTION OF REFORM IN AUSTRALIA?

Although the timetable for law reform in Australia is uncertain, the Federal Government acknowledged the need to modernize the regulatory architecture in its response to various inquiries and reviews, including an inquiry by the Senate,[24] the Review of the Australian Payments System;[25] and the Parliamentary Joint Committee Inquiry into Mobile Payments and Digital Wallets, and noted the following:[26]

> The reviews found new technologies and services are testing our current regulatory definitions, perimeter, and powers, and exposing regulatory gaps which could contribute to increased risks of consumer and business harm, possible future systemic instability and impeding private sector investment in innovative products and services.
>
> Failure to modernize our regulatory framework will mean Australian businesses and consumers are increasingly engaging with unregulated parties and the rules governing our systems could be increasingly determined by foreign governments and large multinational companies.[27]

Included in the recommendations of the Payments System Review Report were the following:

> · that powers be given to the responsible minister, the Treasurer, to designate payment systems and participants for regulatory purposes and to direct regulators to develop regulatory rules accordingly;
>
> · that a functional approach be adopted in terms of the regulation of payments;
>
> · that coordination between the regulators, particularly the RBA and AUSTRAC, which is the AML regulator, be strengthened.

Included in the recommendations of the Senate Select Committee were the following:

> · that a market licensing regime for Digital Currency Exchanges be established;
>
> · that a custody or depository regime for digital assets with minimum standards be established;
>
> · that a token mapping exercise be conducted to determine the best way to characterize the various types of digital asset tokens in Australia;

22 The regulatory classification of cryptocurrencies was complicated when, in 2015, the Commodity Futures Trading Commission defined bitcoin and other cryptocurrencies as commodities under the U.S. Commodity Exchange Act.

23 The Senate (Australia), Select Committee on Australia as a Technology and Financial Centre, *Second Interim Report* (April 2021) at [5.56], citing ASIC's answers to questions on notice.

24 Senate (Australia), Select Committee on Australia as a Technology and Financial Centre, Final Report (October 2021). This report focussed on reforms in Australia's technology, finance and digital asset industries, including reforms in the regulation of cryptocurrencies and digital assets. For details of this inquiry and copies of the reports, see https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/FinancialRegulatoryTech.

25 Australian Government, *Payments system review – From system to ecosystem* (June 2021). This review focussed on the payments system and how it should be reformed to accommodate new technologies, business models, participants, and new forms of money. For details of this review, see https://treasury.gov.au/review/review-australian-payments-system.

26 For details of this inquiry, see https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Corporations_and_Financial_Services/Mobileanddigitalwallet.

27 Australian Government, *Transforming Australia's Payments System* (December 8, 2021), available at https://treasury.gov.au/publication/p2021-231824 at 4.

· that a new Decentralized Autonomous Organization company structure be established;[28] and

· that Treasury lead a policy review of the viability of a retail Central Bank Digital Currency in Australia (Recommendation 8)

The Government stated its in-principle agreement to the above recommendations[29] and has commenced consultations in relation to crypto asset secondary service providers.[30]

Treasury's recent consultation paper in relation to crypto asset secondary service providers acknowledged the "evolving question about whether [providers] who deal in all crypto assets should be included in the regulatory perimeter, or whether the types of applicable crypto assets should be more narrowly defined."[31] It identified two options for regulating providers. The first option would bring all crypto assets into the existing financial services regime by defining crypto assets as financial products under section 764A of the Corporations Act. Under this option, the government (or ASIC as the regulator) "could be provided with powers to exempt or "carve out" particular crypto assets which do not warrant regulation under the financial services regime in a risk-based manner."[32]

This would be consistent with submission to the Senate Committee that advocated including a definition of a "digital asset" in the Corporations Act on the basis that this would expressly attract the disclosure and other consumer protection regimes and allow ASIC to administer the Australian financial services licensing regime in respect of financial services relating to digital assets. Other submissions advocated a bespoke approach.

The alternative option would involve self-regulation by the crypto industry in the form of codes of conduct for crypto asset services. This approach, Treasury suggested, would be "closer to the U.S. and UK, who do not specifically regulate crypto assets (excluding for AML/CTF) unless they are securities or financial products."[33]

What does all of this suggest in terms of the direction of reform? First, it is likely that the impact of technology will result in a move away from a prescriptive, rules-based approach to regulation in favor of a more principles-based approach, one that is supported by clear outcomes. Secondly, the regulatory net is likely to expand to include a broader range of parties than was traditional the case, including providers of crypto-asset services. This was previously recognized in the Payments System Review Report in Australia in relation to providers of payment facilitation services.

Thirdly, it appears inevitable that regulators will need to be given greater powers and flexibility to adapt to challenges brought about by technology and will also need greater regulatory discretion in order to achieve adequate consumer protection without stifling innovation.

"Treasury's recent consultation paper in relation to crypto asset secondary service providers acknowledged the "evolving question about whether [providers] who deal in all crypto assets should be included in the regulatory perimeter, or whether the types of applicable crypto assets should be more narrowly defined

28 It is relevant to note that Treasury agreed to commence consultation on an "appropriate regulatory structure" for Decentralized Autonomous Organizations, leaving open the possibility that an alternative to the company structure is adopted.

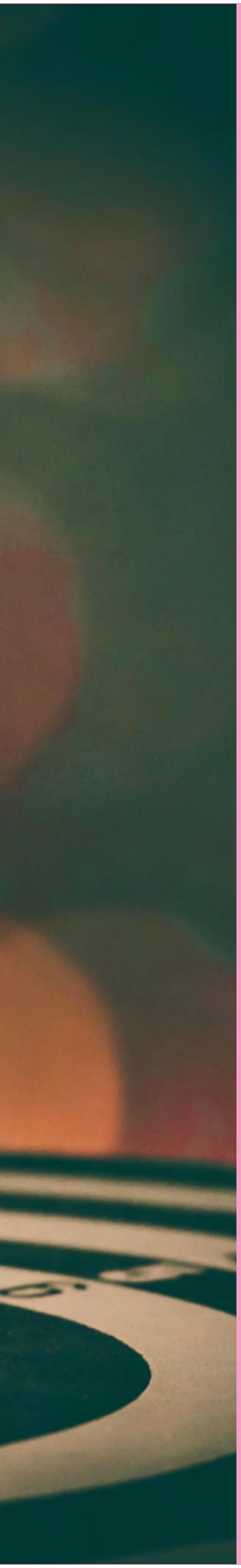
29 Australian Government, Transforming Australia's Payments System (December 8, 2021), available at https://treasury.gov.au/publication/p2021-231824.

30 Department of the Treasury (Cth), *supra* note 2.

31 *Ibid.* at 5.

32 *Ibid.* at 18.

33 *Ibid.* at 19.



A PROPOSAL FOR OVERSIGHT OF DIGITAL ASSET SPOT MARKETS IN THE U.S.

BY

LEE REINERS

Lecturing Fellow and Executive Director at Global Financial Markets Center, Duke University School of Law.

01 INTRODUCTION

Recent turmoil in the digital asset market has renewed calls for greater oversight of the sector.[2] The good news is that the digital asset selloff has not – thus far – spilled into the traditional financial sector. The absence of contagion should only reinforce the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation's policy of requiring supervised banking institutions to re-

2 See Lily Jamali, *Crypto asset meltdown prompts calls for regulation*, Marketplace, May 13, 2022, https://www.marketplace.org/2022/05/13/crypto-asset-meltdown-prompts-calls-for-regulation/.

quest, and receive, approval before engaging in activities involving or relating to digital assets.[3] The bad news is that digital asset markets are not static, and what is true today will almost certainly not be true a year from now.

Unfortunately, the uncertain legal status of digital assets complicates efforts to more vigorously regulate them. The Commodity Futures Trading Commission ("CFTC") has classified Bitcoin and Ether – and by extension other cryptocurrencies that are similarly structured – as commodities (courts have also upheld this classification). While the CFTC regulates commodity derivatives, they do not regulate commodity spot markets, although they do have enforcement authority for fraud and manipulation in commodity spot markets. The practical effect of this structure is that cryptocurrency exchanges in the U.S. are not regulated at the federal level (they are required to register with the Financial Crimes Enforcement Network ("FinCEN") and obtain state money transmitter licenses). This fact recently came into stark relief when the largest cryptocurrency exchange in the U.S., Coinbase, acknowledged in an SEC filing that in the event they file for bankruptcy, crypto assets they hold in custody on behalf of customers "could be subject to bankruptcy proceedings, and such customers could be treated as our general unsecured creditors."[4] In contrast, the Securities Investors Protection Corporation ("SIPC") "protects against the loss of cash and securities – such as stocks and bonds – held by a customer at a financially-troubled SIPC-member brokerage firm" up to $500,000.[5]

This gap in digital asset spot market regulation, and the need to address it, has been acknowledged by Securities and Exchange Commission ("SEC") Chair Gensler,[6] CFTC Chair Behnam,[7] the digital asset industry, and members of Congress. The threshold question however, is which agency should be given oversight of digital asset spot markets, and what should be the extent of their authority? Here, there are no shortage of proposals, however, a consensus has yet to emerge.

02
KEY PRINCIPLES

It is important to have clearly defined principles when developing and assessing regulatory proposals. In short: What are the policy objectives a comprehensive digital assets regulatory bill should achieve? The Executive Order on digital assets offers six objectives that serve as a natural starting point: protect consumers, investors, and businesses; protect United States and global financial stability and mitigate systemic risk; mitigate the illicit finance and national security risks; reinforce United States leadership in the global financial system and in technological and economic competitiveness; promote access to safe and affordable financial services; and support technological advances that promote responsible development and use of digital assets.[8] I consider each of these objectives in order of priority.

To accomplish these objectives, any comprehensive regulatory framework for digital assets must have the following features:

1. One dedicated regulatory agency with exclusive oversight over digital asset trading markets.

The fact that some digital assets are commodities while others are securities has led to unnecessary confusion within the private and public sector. It has also prevented meaningful regulatory action to address clear consumer and investor abuse. For example, in a recent speech, SEC Chair Gensler noted that the trading venues the SEC currently oversees solely trade securities, but that some "crypto platforms currently list both crypto commodity tokens and crypto security tokens, including crypto tokens that

3 See *Notification of Engaging in Crypto-Related Activities*, Fed. Deposit Ins. Corp., Apr. 7, 2022, https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html; *Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank*, Off. of the Comptroller of the Currency, Nov. 18, 2021, https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1179.pdf.

4 Paul Kiernan, *Coinbase Says Users' Crypto Assets Lack Bankruptcy Protections*, Wall St. Journal, May 12, 2022, https://www.wsj.com/articles/coinbase-says-users-crypto-assets-lack-bankruptcy-protections-11652294103.

5 *What SIPC Protects*, SIPC, https://www.sipc.org/for-investors/what-sipc-protects, last visited May 17, 2022.

6 See Gary Gensler, *Remarks Before the Aspen Security Forum*, U.S. Sec. & Exch. Comm'n, Aug. 3, 2021, https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03.

7 See *Testimony of Chairman Rostin Behnam Regarding "Examining Digital Assets: Risks, Regulation, and Innovation*," Commodity Futures Trading Comm'n, Feb. 09, 2022, https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam20.

8 Executive Order on Ensuring Responsible Development of Digital Assets, Exec. Order No. 14067, 87 Fed. Reg. 14143, Mar. 14, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

are investment contracts and/or notes."[9] Gensler goes on to note that SEC staff is working with the CFTC to address joint regulation of such platforms, but history suggests that this type of interagency collaboration does not yield meaningful results (interagency turf battles are far more common). The bifurcation of digital assets as commodities or securities has also contributed to strange outcomes in trading markets. For example, the CFTC permitted the listing of cryptocurrency futures contracts, and the SEC subsequently authorized an exchange-traded fund ("ETF") tracking cryptocurrency futures, but the SEC has yet to authorize a spot cryptocurrency ETF. A spot cryptocurrency ETF and cash-settled cryptocurrency futures both provide exposure to cryptocurrency without requiring investors to ever take possession of cryptocurrency. The fact that we have one without the other makes little sense.

2. Recognition in federal law of digital assets as a new asset class.

The confusion around whether a given digital asset is a commodity, security, or something else must be addressed if one agency is to have sole authority over digital asset markets. Gensler recently noted that "Congress painted with a broad brush the definition of a security" and that the Supreme Court's 1946 *Howey* Test – saying an investment contract exists when there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others – further clarified when an investment contract exits.[10] Were it not for the "efforts of others" prong of the *Howey* Test, the majority of digital assets would qualify as investment contracts.

The Commodity Exchange Act is more prescriptive in defining a commodity but the definition also includes "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in." In essence, this means that the moment there is a derivative on an underlying asset, that asset is considered a commodity, unless it meets the definition of a security.

While a principles-based approach to securities regulation has served our capital markets – and the investors and issuers within them – well, digital assets do challenge definitional boundaries and contribute to legal gray areas. For example, can a token issued by a decentralized autonomous organization ("DAO") be considered an investment contract if there truly is no central party, or parties, essential to the DAO's performance? The only way to address this uncertainty is by statutorily recognizing and defining digital assets in federal law. Of course, most financial assets are digital these days, so the definition of digital assets must be precise enough to exclude existing securities, like stocks and bonds, yet broad enough to incorporate cryptocurrency as well as current and future cryptocurrency offshoots (DAOs, non-fungible tokens ("NFTs"), etc.). One potential definition is found in the Infrastructure Investment and Jobs Act: "'digital asset' means any digital representation of value which is recorded on a cryptographically secured distributed ledger…"[11]

3. The agency responsible for regulating digital assets must have broad rulemaking authority to address a rapidly evolving market.

The digital asset market is constantly evolving, which is why Congress must not be overly prescriptive when drafting regulatory proposals. The rise of decentralized finance ("DeFi"), DAOs, stablecoins, and NFTs demonstrates the need for the principal regulatory agency to have the statutory authority to address the risks associated with the latest developments in the digital asset market.

03 PROPOSALS

With these objectives and features in mind, I now turn to considering, at a high level, several proposals for regulating the digital asset market that have emerged recently.

1. Establish a self-regulatory organization ("SRO") to establish and enforce standards of conduct.

This is the preferred solution for many digital asset firms, including Coinbase.[12] While there is precedent in the financial sector for an SRO (FINRA, FICC, etc.), this model

9 Gary Gensler, *Prepared Remarks of Gary Gensler On Crypto Markets, Penn Law Capital Markets Association Annual Conference*, U.S. Sec. & Exch. Comm'n, Apr. 4, 2022, https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422.

10 *Id.*

11 Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429, https://www.congress.gov/bill/117th-congress/house-bill/3684/text.

12 Faryar Shirzad, *Digital Asset Policy Proposal: Safeguarding America's Financial Leadership*, The Coinbase Blog, Oct. 14, 2021, https://blog.coinbase.com/digital-asset-policy-proposal-safeguarding-americas-financial-leadership-ce569c27d86c.

suffers from several challenges. As Professor Ryan Clements notes, these challenges include "classic economic problems like organizing 'the commons' and dealing with free-riders, as well as practical and legal considerations like ensuring [SRO] accountability, enforcing non-compliance penalties, facilitating government oversight, creating suitable member incentives to participate, and ensuring a high cost of expulsion."[13] If an SRO is to be pursued, it would be better to assign FINRA the task of regulating digital asset trading rather than to create an entirely new SRO.

2. Give the CFTC authority to regulate digital asset spot markets.

CFTC Chair Behnam recently argued for this during a Senate Agriculture Committee meeting,[14] and it makes intuitive sense, given the CFTC's role in overseeing digital asset derivatives and the agency's existing digital asset capacities. This solution has also been advocated by some digital asset firms and CEOs, including Sam Bankman Fried of FTX, because the CFTC has historically acted favorably towards digital assets – going back to the 2017 self-certification of bitcoin futures and the embrace of former CFTC Chair Giancarlo as "Crypto Dad."[15] However, the CFTC does not have an investor protection mandate, which is one reason for its permissive approach to digital assets, and the agency is chronically underfunded. In addition, the CFTC has used its fraud and manipulation enforcement authority sparingly when it comes to digital assets. In short, the CFTC has been uncritical in its review of digital asset proposals and does not have the resources to sufficiently regulate digital asset spot markets. Furthermore, as noted by Behnam, digital assets are fundamentally different from other commodities in that more retail investors invest in them and international markets affect them directly, to say nothing of the fact that commodities tend to be tangible.[16] For these reasons, the CFTC should not be given digital asset spot market authority.

3. A completely new digital assets regulatory agency.

Many argue that digital assets are fundamentally new kinds of assets that do not fit neatly into established regulatory categories; therefore, a new regulatory agency is needed to focus exclusively on digital assets. I reject this argument due to the complexities, inefficiencies, and political challenges associated with establishing a new agency. It is also not needed. Markets and the instruments that trade in them have always evolved, and regulatory agencies typically adapt (sometimes with Congress' help). Furthermore, a new agency could be captured by the digital assets industry in short order.

4. Carve out digital assets from the definition of commodity in the Commodity Exchange Act and recognize digital assets as securities under a special definition to the securities laws.

This would give the SEC exclusive authority to regulate all aspects of the digital assets industry and is the preferred option, given the SEC's statutory mission to protect investors and its long track record of capable expertise in regulating securities markets. The proposal would impose the same requirements on digital asset issuers and intermediaries as the current securities laws – principally the Securities Act of 1933, the Securities Exchange Act of 1934 ('34 Act), and the Investment Company Act of 1940 – impose on the securities industry. And it would also unite under a single agency regulation of all aspects of the digital asset market: spot markets, initial coin offerings, derivatives, and investment funds (including ETFs).

04
EXTENT OF AUTHORITY

The SEC simply has more expertise, more resources (although, to be clear, additional funding would be required), and more appetite for enforcement in the digital assets area than the CFTC does. It is worth noting that even former CFTC Chairman Timothy Massad agrees that the SEC should be given oversight over digital asset spot markets: "Despite my personal affection for the CFTC, the SEC may be better suited to the task because it is more focused on

13 Ryan Clements, *Can a Cryptocurrency self-regulatory organization work? Assessing its Promise and Likely Challenges*, The FinReg Blog, June 21, 2018, https://sites.law.duke.edu/thefinregblog/2018/06/21/can-a-cryptocurrency-self-regulatory-organization-work-assessing-its-promise-and-likely-challenges/.

14 See *Testimony of Chairman Rostin Behnam Regarding "Examining Digital Assets: Risks, Regulation, and Innovation*," *supra* note 7.

15 See Robert Schmidt & Allyson Versprille, *Crypto Platforms Ask for Rules But Have a Favorite Watchdog*, Bloomberg, Mar. 31, 2022, https://www.bloomberg.com/news/articles/2022-03-31/crypto-exchanges-want-say-in-rules-under-biden-administration.

16 See Rostin Behnam, *Commodity Futures Trading Commission Respond to Letter on Digital Assets*, Senate Comm. on Agric., Nutrition, & Forestry, Feb. 8, 2022, https://www.agriculture.senate.gov/imo/media/doc/2022%2002%2008%20Ag%20committees%20digital%20asset%20response%20letter.pdf.

retail investors and cash markets."[17] In authorizing legislation, Congress should make clear that the SEC is expected to implement rules around investor protection, disclosure, pre-trade and post-trade transparency, uniform settlement standards, data reporting, recording keeping, anti-money laundering/know your customer, conflicts of interest, trading practices, client custody, operational risk, governance, and net capital. It will then be up to the SEC to determine if existing rules governing the offering, distribution, and trading of securities are sufficient to cover the risks associated with digital assets or if new rules are needed. Bringing digital assets within the securities laws will also allow investors to avail themselves of Rule 10b-5 of the '34 Act, which provides an additional measure of investor protection by making it illegal for any person to defraud or deceive someone, including through the misrepresentation of material information, with respect to the sale or purchase of a security.[18]

05
CONCLUSION

This proposal would address the primary gap in digital asset regulation by having Congress grant the SEC exclusive authority over all facets of the digital asset market, from spot to derivatives. It would do so by creating a special definition of security under the securities laws that would incorporate digital assets. Importantly, this proposal does not preclude Congress from regulating stablecoins, as the Supreme Court's *Marine Bank v. Weaver* decision held that "deposits" are "securities" for purposes of the federal securities laws unless those deposits are accepted either by Federal Deposit Insurance Corporation ("FDIC")-insured U.S. banks or by foreign banks that are governed by regulatory regimes providing comparable protections to their depositors.[19] Thus, as professor Arthur Wilmarth has noted, it is possible for stablecoins to be regulated as both "deposits" and "securities" unless Congress decides to bring stablecoins into the banking system and protect them with FDIC insurance.[20]

Should political realities make it untenable for the SEC to be given spot market authority, then the next best option would be to give the CFTC oversight over digital asset spot markets. Indeed, there appears to be growing bipartisan momentum for this approach. At the end of April, four members of the U.S. House of Representatives (two Democrats and two Republicans) introduced the Digital Commodity Exchange Act of 2022 ("DCEA").[21] The bill introduces a new term, "digital commodity," to the Commodity Exchange Act, and defines it as: "any form of fungible intangible personal property that can be exclusively possessed and transferred person to person without necessary reliance on an intermediary."[22] Digital commodity trading venues would then be subject to federal registration and regulation by the CFTC as an alternative to multistate transmitter licenses.

In addition to spot market regulation, a comprehensive digital asset regulatory bill would address issues around tax, national security, state jurisdiction, and stablecoins. The latter is particularly salient given the recent collapse in the algorithmic stablecoin, TerraUSD.[23] But time is of the essence, and the digital asset market will continue to evolve with remarkable speed and in unexpected ways. Congress should act quickly to close the regulatory gap in digital asset spot markets and provide the SEC with the tools it needs to protect investors.

> ***"The DGA-draft is intended to represent a first approach to the creation of an EU single market for data***

17 Timothy G. Massad, *It's Time to Strengthen the Regulation of Crypto-Assets*, The Brookings Institution, Mar. 2019, https://www.brookings.edu/wp-content/uploads/2019/03/Economis-Studies-Timothy-Massad-Cryptocurrency-Paper.pdf.

18 17 C.F.R. § 240.10b-5 (1951), https://www.law.cornell.edu/cfr/text/17/240.10b-5.

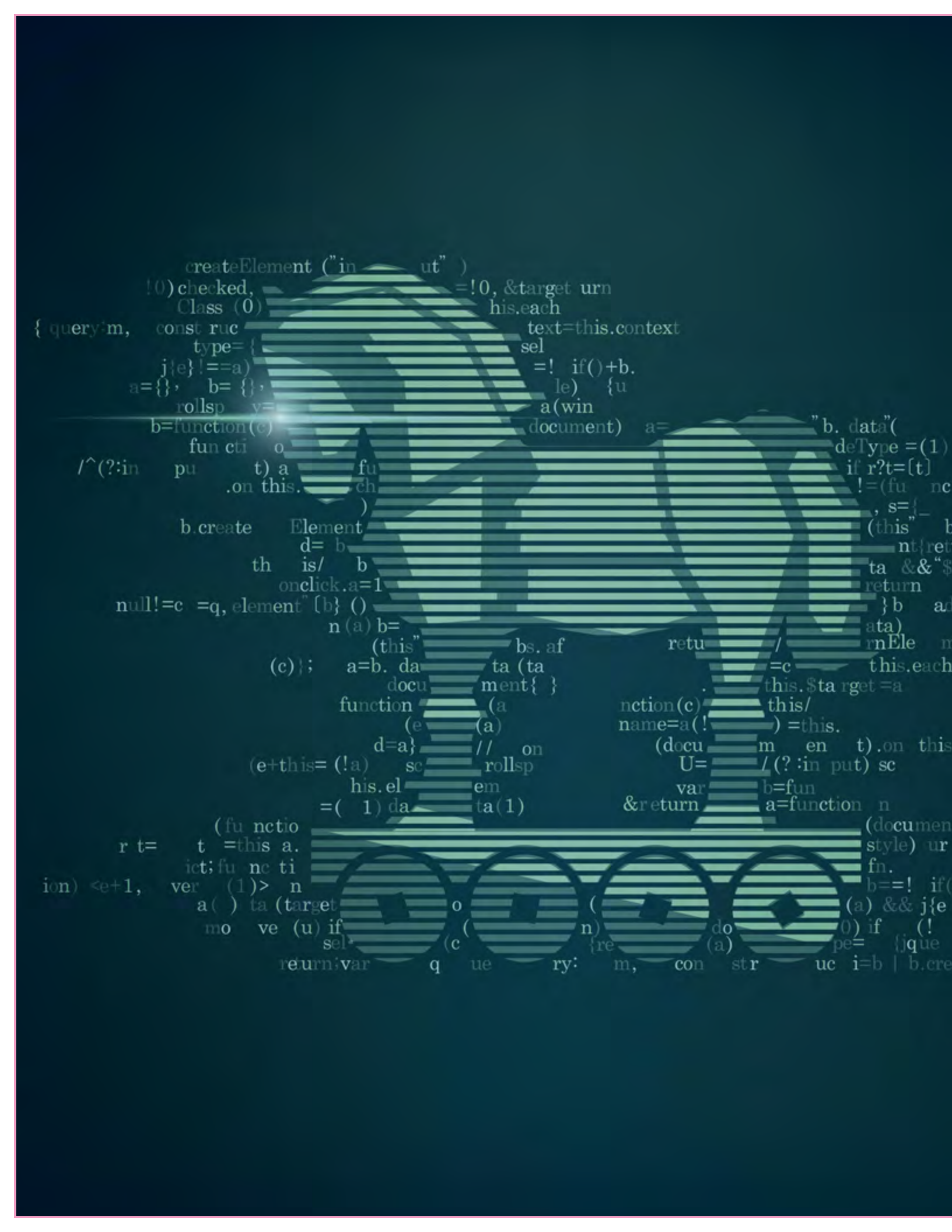
19 *Marine Bank v. Weaver*, 455 U.S. 551, 551-52 (1982).

20 Arthur E. Wilmarth, *It's Time to Regulate Stablecoins as Deposits and Require Their Issuers to Be FDIC-Insured Banks*, 41 Banking & Financial Services Policy Report No. 2 (Feb. 2022), at 1-20, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4000795.

21 Digital Commodity Exchange Act of 2022, H.R. 7614, 117 the Cong. (2022), https://republicans-agriculture.house.gov/uploadedfiles/digital_commodity_exchange_act_of_2022.pdf.

22 *Id.*

23 See Marco Quiroz-Gutierrez & Taylor Locke, *A 'stable' coin lost its peg over the weekend and pledged $1.5 billion in Bitcoin trying to stabilize. Here's how the algorithmic stablecoin was supposed to work—and didn't*, Fortune, May 10, 2022, https://fortune.com/2022/05/10/what-is-algorithmic-stablecoin-terrausd-bitcoin-crash/.



PRIVACY IN A TECHNOLOGICAL AGE

BY
SUSAN JOSEPH

Executive Director of Cornell FinTech Initiative, Cornell University, SC Johnson College of Business, CEO/CoFounder HealthTrends.AI, CEO, SusanJosephLLC- JD/MBA blockchain consulting, Executive Director, Diversity in Blockchain (nfp).

01 INTRODUCTION: PRIVACY RIGHTS IN OUR DATA-DRIVEN ECONOMY

What does privacy as a fundamental right mean? How does that right fare in a data-driven society? How can we protect privacy through both legal and technological measures? Answers to these questions will define how we will be able to live our lives as they are increasingly intertwined with, and influenced by, existing and emerging technologies.

02

WHAT DOES PRIVACY AS A FUNDAMENTAL RIGHT MEAN?

The right to privacy is one of the foundational precepts on which our stated constitutionally protected rights rely. Our right to autonomy and dignity is presupposed by the First (right to be an independent person), Fourth (right to be secure) and Fifth Amendments (right to refuse to self-incriminate). However, our Constitution does not explicitly enumerate a right to privacy.

In 1890, soon-to-be Supreme Court Justice, Louis Brandeis famously defined the right to privacy in a Harvard Law Review article as "a right to be left alone." Our technologically connected world did not exist back then, but the law certainly contemplates the protection of the person which extends to and covers his digital self as a representation of his personhood. In a digitally intermeshed world, are we able to be both connected and left alone? This question, and Justice Brandeis' definition take on new importance as privacy is continuously under attack in today's data-driven world.

Laws must evolve in response to technologies and societal changes. For instance, copyright law was created long ago in response to the introduction of the then revolutionary technology, the printing press. Today's digitally connected world requires a federal explicitly enumerated right of privacy to carry out the Declaration of Independence's fundamental assertions that we have an inalienable "right to life, liberty, and the pursuit of happiness." Congress and industry have taken note, and there are privacy bills under consideration. It is time to envision a comprehensive baseline federal law that imposes a strong duty of care with both remedial and significant penalties and consequences together with a Digital Bill of Rights.

03

OUR DIGITAL STORIES ARE SHARED BUSINESS

A. What Data is Collected?

It is often said that the collective "we" is the product, in this age of "surveillance capitalism." Every aspect of our lives can be captured and exploited for commercial gain by tech companies and others through collected data — data that should be protected under federal privacy laws. Some examples of data routinely collected by private businesses include our face prints, iris scans, location, purchase habits, sleeping habits, photos, voice recordings, fingerprints, the way we drive, how we exercise, what we read, what information we search for, who we know, how we use appliances and lights within our homes, etc. This information can be stored indefinitely, retrieved immediately, sold to many, and used to devise targeted marketing and profiling.

B. How is Our Personal Data Generated and Who Collects It?

Data is generated through a variety of online and mobile activities. A 2020 estimate calculates that 2.5 quintillion bytes (number with 18 zeros) of data are generated daily. This dizzying pace gets more impressive, when you consider that the bulk of the data generated in the world has occurred in the past two years. This data consists of both Personally Identifiable Information ("PII") which is defined as information that can be used to identify us and the broader spectrum of personal data, defined as information generally about us.

A sampling of the latest 2022 statistics show that in an internet minute, 231 million emails are sent, 5.9 million Google searches occur, 694 million songs are streamed, 16.2 million texts are sent and 2.1 million are active on Facebook (Meta). Much of our personal data is generated through internet searching. Google dominates the search arena by conducting ninety-five percent of all mobile searches and 90 percent of all desktop searches in the U.S.

Other companies also routinely collect and use our data to fuel applications and target us. Facebook is one such avid data collector and marketer. A leaked document from Facebook as reported in The Guardian states that Facebook collects trillions of data points daily. It is thought that the company tracks and collects 52,000 data points on every user observing us in many cases even after we leave the platform.

Data generated and collected through sensors in devices from appliances to cars to buildings is on the rise. Despite chip shortages and other supply chain disruptions in 2022, the number of connected devices (Internet of Things) is expected to grow to 14.4 billion and reach 27 billion by 2025. The amount of data coming online is almost incomprehensible.

Let's look at the seemingly straightforward example of smart light bulbs. Did you know that Amazon and Google collect data from these "smart home" implementations? They increasingly require that a light bulb controlled by a smart speaker continuously provide status reports to its hub. And the information acts as a tracker to our daily lives. As a re-

cent insurance journal article succinctly puts it: "Even light fixtures, in elaborate setups, are a map of home life: When do you get home? When does the light in your child's bedroom usually go off? What days do you burn the midnight oil?"

Or, look at the connected doorbells that have made their way into our lives. Ring's terms of service state that you grant them an unlimited, irrevocable and perpetual license to use the content which may include audio, images, video, or text. You may not want to consent to this automatic and passive method of collecting your data; and you may not even be aware of it.

04

YOUR HOME MAY BE YOUR CASTLE, BUT YOU HAVE ALLOWED IN A TROJAN HORSE OF ADVANCED HOME TECHNOLOGY AND SMART DEVICE PROVIDERS

A. What do Companies do with Our Data?

Companies make predictions from our data to select and nudge our behavior toward product and service purchases or to influence our relationships, associations, and voting choices. We are regularly micro and macro targeted. The applications that we use seem to fit us so well because they are created from and for us. And, they offer a carefully cultivated window to influence and shape our future. Some companies, like Facebook, feed millions of data points into algorithms which offer up six behavior predictions per second that can be marketed and deployed to advertisers who seek to influence our interactions. Facebook's approach is particularly powerful as it directs relatively personalized targeting to connected individuals subject to social influence.

The dark side of this bargain is that a David and Goliath style power imbalance favors very large technology service providers over consumers who have little choice to decline the surveillance and targeting because alternative products and services are not otherwise widely available. The "consent" to terms of service more similarly resembles a contract of adhesion than a level playing field. An individual is bound by thousands of words of obscurely written privacy policies and one-sided terms of service that he would have to weed through to determine if/how he could even take protective action. The reality, of course, is that almost no one has the time or expertise to read and understand these policies.

There have been some strong public repercussions for companies both collecting data and sending it to third parties to review. Tech companies now provide consumers with directions to turn off much of the data collection in many instances, but that is not a comprehensive or complete solution. And turning off the tracking options may not effectively protect your privacy. Google is currently being sued about its data gathering practices by the attorneys general of the District of Columbia, Texas, Washington, and Indiana who claim the company deceived consumers who revoked access to location data by continually surveilling them to obtain the data. When you consider that Google basically commands the data search market, the alleged overreach of data collection is staggering.

The end result is that our personal data is circulated and used both individually and in aggregate well beyond what we thought we permissioned, and we have custodied it with BigTech or other companies without adequate assurance of its safety and downstream transmission.

B. How Big of a Problem is Data Oversharing?

Many are familiar with Facebook's (now Meta) Cambridge Analytica and the misuse of our data that affected global elections. In that example, our dignity and very autonomy, not to mention our government, civil stability and well-being were targeted and manipulated. And just recently, The Wall Street Journal reported that Google, through its Project Nightingale, is collecting millions of medical data records from Ascension without patient or doctor consent to analyze for health care insights and patient care suggestions. That program has triggered a federal investigation.

Technology companies did not start out to control our every move. And we did not start out expecting to be controlled. Amazon, Google, and Facebook, for instance, sprouted a mere generation ago and brought technological innovation to the world with the goals of connection, information access, and convenience. Unfortunately, along the way, they morphed their business models. The online advertising industry grew with them, evolved, and largely eviscerated our privacy while they were looking, but we were not. It is time for us to seriously start looking.

05

COMPANIES HAVE NOT HONORED OUR TRUST

At the end of the day, we have to ask, at what cost is all of this convenience? We have come to expect that our data will be mishandled. Companies seem to have lost the ability to be good data stewards. The list of data breaches continues to grow. Once trust is broken, it is hard for a company to reclaim it. Several of the more egregious breaches from 2021, 2022, and recent years are listed below.

· **Misconfigurations of cloud services?** Names, email addresses, dates of birth, chat messages, location, gender, passwords, photos, payment information, phone numbers, and push notifications of more than 100 million Android users exposed.

· **Leaked database?** Emails and phone numbers of Facebook users from 106 countries, including more than 32 million records of U.S. users exposed.

· **Server breach?** Cash App (owned by Block) 8 million customers contacted about a hack of customer names, stock trading information, account numbers, portfolio values, and other sensitive financial information.

· **Plain text data storage risk?** See Equifax where an estimated 147mm people were affected and a recent FTC settlement of up to $700 million penalty was assessed.

· **Fingerprints and facial recognition potentially compromised?** See Suprema, which exposed 28 million records of over 1 million people worldwide.

06

LEGAL FRAMEWORKS CAN BE CREATED THAT PROTECT OUR PRIVACY

A. Strengthen the Right to Privacy

The Supreme Court in Griswold v. Connecticut in 1965 explicitly stated that guarantees in the Bill of Rights have penumbras which create zones of privacy. In other words, the right to privacy exists, is recognized, and protected — at least within certain bounds. Over the years, the implied right to privacy in the Constitution has been further expounded upon by the courts and legislatures. Specific statutory rights to privacy have also developed which limit access to PII such as HIPAA and others. However, no comprehensive federal law yet exists that creates a well-regulated and orderly scheme to protect our data and our privacy.

Our data is multifaceted. It has property-like characteristics. It is also an information flow that we necessarily must share in certain instances and keep to ourselves in other situations. Consider who actually owns my photo data when I share it with a social media site such as Facebook.

From an information flow perspective, suppose I post a group photo that includes me and other non-Facebook members. Is the photo owned by all, and must we all consent to its posting and posting afterlife? What if one of us wants to take down that photo posting? How does a non-Facebook member know the photo is posted or even ask for it to be deleted? Can I require that Facebook delete all information related to that photo posting including comments by others? What about the re-posts that have occurred? Does anyone have the right to take them down?

From a property rights perspective, if Facebook wants to monetize the use of my information, should I have the ability to be compensated? How are non-Facebook members who have not permissioned the use of their data compensated when their information is shared? What are the original poster's data ownership rights including compensation regarding the downstream sharing of posted information to third parties?

Simply treating data as property devalues the way data is used and respected in society. It is problematic to think of data as simply another piece of property. As a recent Brookings article states:

> "Treating personal information as property to be licensed or sold may induce people to trade away their privacy rights for very little value while injecting enormous friction into free flow of information. The better way to strengthen privacy is to ensure that individual privacy interests are respected as personal information flows to desirable uses, not to reduce personal data to a commodity."

07

CALL TO ADOPT A CONSTITUTIONALLY PROTECTED DIGITAL BILL OF RIGHTS

The most fundamental privacy protection is envisioned as a constitutionally protected right. A natural outflow of that protection is a Digital Bill of Rights clearly setting forth the rights and responsibilities of those who handle data.

An MIT Technology Review article outlined some general principles for a Data Bill of Rights. Those rights include:

· The right of the people to be secure against unreasonable surveillance shall not be violated.

· No person shall have his or her behavior surreptitiously manipulated.

· No person shall be unfairly discriminated against on the basis of data.

Federal law can draw from other legal frameworks that protect privacy. California has enacted privacy laws. Other states have enacted laws. However, a patchwork of state privacy laws that affect digital transmissions across state lines can very quickly become messy, hard to navigate, provide uneven protections, and be difficult to enforce. A more consistent approach would be to create strong federal protections.

Other governments have implemented proactive and protective privacy laws. The General Data Protection Regulation ("GDPR") enacted by the European Union is a good step toward accountability for companies who collect and use our personal data. It provides significant financial consequences for violators as well as remedial actions to protect individuals. It attempts to restore the balance of power from an asymmetric relationship to one that is fairer. These advancements sound encouraging. In addition to legal protection, technological solutions can help champion this right.

08

TECHNOLOGICAL SOLUTIONS CAN BE IMPLEMENTED THAT PROTECT PRIVACY

A. Data Minimization Principals Should be Followed

The principal of data minimization, collecting and retaining only that data that is necessary for the stated purpose, can be applied to protect privacy and identity. Since identity determines how you are counted and can transact, let's look at the components of digital identity.

B. Components of Digital Identity

· **Claims**: an identity claim is a statement made by the individual. One that contains two claims could be: 'My name is Mary, and my date of birth is June 28, 1979." This can also be thought of as an attestation.

· **Verifiable Credentials:** Documentation that provides evidence for the claim. These come in different formats, such as passports, birth certificates and drivers' licenses.

· **Proofs**: Showing that you hold the verifiable credential itself. This can be done by offering the verifiable credential such as a showing a driver's license. It can also be done by offering evidence that you have/hold a credential itself without showing the actual credential. This type of proof is referred to as "**zero knowledge proof**."

· **Verified Credentials:** A third party validates that according to their records, the claims are true.

· **Attester:** An issuer (which could be a third party such as a bank) issues a credential that says an individual has a bank account there. For instance, in the case of a bank account, the Bank agrees and issues a credential that "attests" to the fact that the bank account is there. The Bank would be the Attester. Or, an individual can issue a credential that "self-attests" to the fact asked to be proven. The individual would then be the Attester.

C. Credential Issues with Centralized Identity Systems

Frequently in real life you routinely cannot provide just the relevant data needed to prove your identity when presenting a credential. For instance, presenting a Driver's License to gain access to a building provides more information to a

security guard than simply you are who you say you are. By default, data is overshared and the building management's liability and risk increases as it has made itself a hacking target by holding this information.

D. Decentralized Identity is an Evolving Solution

In the near future, we can imagine a world where we have the technological, legal, and economic ability to reasonably share data for the services we want and recall further usage of it once the original shared purpose has been satisfied. In the above example, this would mean that only the data required to enter the building is shared, and that data is not allowed to be retained once you leave the building.

In all types of systems, we still have to accommodate the fact that traditional data on-boarding is necessary. Someone still has to collect and hold the data, offer it, and allow it to be used. But today's systems do not provide an automatic mechanism to protect shared data from further disclosure. Future decentralized systems can add that type of control which would be a vast improvement.

09

IF DATA SHARING CAN BE CHANGED TO FIT FOR ITS MOST NARROW PURPOSE, RESTORING DIGITAL TRUST AND REASONABLY ALLOCATING LIABILITY CAN OCCUR

It is exciting to see what is on the horizon. Approximately 86 major participants in the identity and technology space have joined together in a technologically focused consortium, the Decentralized Identity Foundation ("DIF"). Notably, FAANG and many smart device and financial service providers are not members. However, certain large technology and other enterprises such as Microsoft, IBM, Mastercard, Aetna, and Accenture are participating. DIF's mission is to develop the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interoperability. In short, decentralized identity technological solutions with concomitant standards are being built. To that end, the World Wide Web Consortium ("WC3") has a working group to address the standards for Decentralized Identifiers.

10

SELF-SOVEREIGN IDENTITY SYSTEMS MAY MINIMIZE DATA OVERSHARING

A. What is Self-Sovereign Identity?

In the self-sovereign identity vision, individuals and entities are enabled to create and manage their identifiers in a decentralized fashion, without relying on a third-party identity provider for validation. The system architecture is structurally set up to work from the perspective of the individual or the entity that is to be identified, and in the case of humans, is often anchored by unique biometric identifiers. It is unlike existing identity solutions that are structured from the perspective of the organization that provides an identifier and thus the law needs to be engineered to become more human-centered. Implicit in this vision is the idea that you show the minimum information needed to access products and services. This is closer to the way the offline world works.

Many of the proposed identity systems that are being developed incorporate blockchain technology. The protocols create frameworks for social trust. It is early days, but early days with promise. Last year, Microsoft launched its ION system for user controlled identities on the Bitcoin blockchain.

Late last year, Square released a Whitepaper describing a new decentralized protocol to enable trust using decentralized identity and verifiable credentials to "prove" the identity. It provided initial open-source code and will continue to release tools as the year progresses.

Practically speaking, these types of identity systems can work in the following way: your verifiable credentials are held by you on your phone or in your personal cloud. You, and not some third party, hold that data, and only you determine where it goes. You may offer up that data as proof to a third party to verify it, and you may put automated or manual rules in place that do not allow that third party to keep it.

11

GOVERNING PRINCIPALS OF IDENTITY

Some final words on Self-Sovereign Identity. Identity practitioners have suggested governing principals to reinforce that the individual is control of his identity. These include:

1. **Existence.** *Users must have an independent existence.*
2. **Control.** *Users must control their identities.*
3. **Access.** *Users must have access to their own data.*
4. **Transparency**. *Systems and algorithms must be transparent.* Note: To this end, the foundation of all technology solutions to enable SSI must be open source.
5. **Persistence.** *Identities must be long-lived.* Though note that newer proposals focus on single use or disposable identities. This principal is evolving.
6. **Portability.** *Information and services about identity must be transportable.*
7. **Interoperability.** *Identities should be as widely usable as possible.*
8. **Consent.** *Users must agree to the use of their identity.*
9. **Minimization.** *Data collection, use, and retention must be minimized.*
10. **Protection.** *The rights of users must be protected.*

12

SELF-SOVEREIGN IDENTITY HAS PLUSES AND MINUSES

Self-Sovereign Identity has both pluses and minuses for consumers and enterprise. Both legal and technological barriers exist today. The law would need to evolve in tandem with the technology and regulations would have to be enacted to empower this type of business process. With this type of identity system, control and responsibility are housed with the individual. Arguably, it places an extreme burden on the individual due to information, technological, and legal asymmetries.

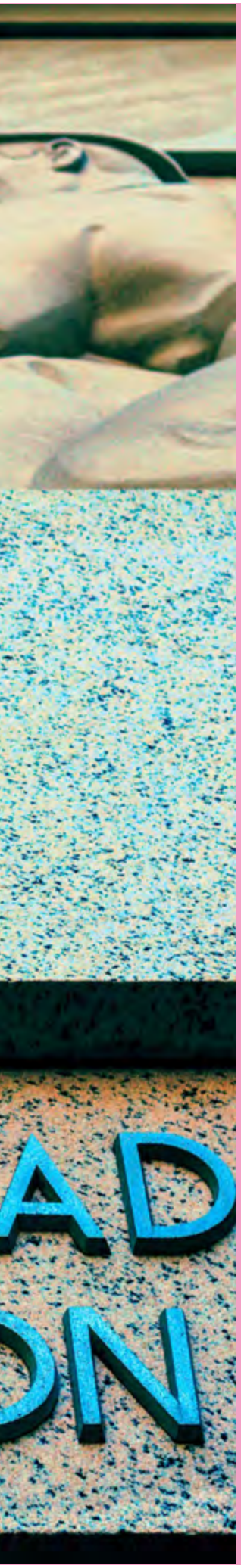
Creating this new environment of digital trust is disruptive and could initially threaten current data-driven business models such as social media which rely on harvesting our data to create products and services. However, it can also help de-risk and provide ease of compliance in ensuring our data is not trafficked downstream. New offerings that are privacy preserving could be more profitable and are up for grabs. The real winners will be individuals and society overall.

13

CONCLUSION: PROTECT PRIVACY THROUGH LEGAL AND TECHNOLOGICAL MEANS

In our increasingly data-driven world, we must adopt strong protections that preserve our autonomy. Such protections are derived from both legal and technological frameworks. Legal protections can be created by establishing a comprehensive federal scheme that recognizes privacy as a fundamental right. A Digital Bill of Rights with strong enforcement provisions should be created. Technological solutions that are architecturally developed from the individual privacy point of view should mesh with new laws that support privacy as a fundamental right. These trust frameworks and types of decentralized/blockchain identity systems are evolving. Tensions between these new identity systems, *status quo* business models, and existing privacy and data protection laws will have to be resolved. However, these types of systems that support privacy rights may encourage new and more profitable products and services while helping to restore a more equal balance of power between an individual and the service provider. Privacy is possible in the digital age. With legal and technological means working together, we can protect our right to be left alone.


EDERAL TR
COMMISSIO



FINTECH & THE FEDERAL TRADE COMMISSION

BY

CHRISTOPHER B. LEACH

Partner, Mayer Brown LLP; former attorney at Federal Trade Commission, Division of Financial Practices.

01 INTRODUCTION

When fintech lawyers think through the list of relevant regulators, what comes to mind? Within the alphabet soup of federal regulators — SEC, CFPB, FinCEN, and so on — companies sometimes have overlooked the Federal Trade Commission ("FTC"), to their peril. With more than 100 years of experience enforcing antitrust and consumer protection laws, the FTC has been an active player in the fintech space on a range of issues, using the agency's entire toolkit.

The FTC's importance shifted up a notch with the appointment of Lina Khan as Chair of the agency. After making a name for herself with high-profile criticisms of tech platforms, Chair Khan has big plans for the FTC, including on issues related to fair lending, data privacy, information security, and focusing enforcement on the largest players in the market. Her progress had stalled in recent months while she awaited the confirmation of a third Democratic vote on the FTC. But with the third Commissioner now confirmed, companies should brace themselves for aggressive enforcement and new regulations.

02

REMIND ME, WHAT IS THE FTC?

For readers unfamiliar, the FTC is run collectively by 5 commissioners — traditionally two Democrats, two Republicans, and a chair appointed by the President. The Commission has two core mandates — consumer protection and competition — which are separated into distinct bureaus. Although under Chair Khan the agency has said the agency would take a more "interdisciplinary" approach and work across bureaus, investigations remain fairly siloed.

The FTC's primarily statutory tool is Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices in commerce ("UDAP" in compliance speak). To prove deception, the FTC must show that the company made a statement that was likely to mislead a reasonable person about a material fact. And to prove that a practice is unfair, the FTC must show that the practice did or was likely to cause substantial injury to consumers, that was not reasonably avoidable, and where the harm is not outweighed by countervailing benefits. Notably, the FTC Act doesn't require proof that any customers actually were deceived, or that any practice actually caused injury.

The FTC Act isn't the only statute that the FTC enforces relevant to fintechs. Among others, the agency enforces fair lending rules under the Equal Credit Opportunity Act, the disclosure requirements under the Truth in Lending Act, credit reporting issues under the Fair Credit Reporting Act, privacy and security under the Gramm Leach Bliley Act, and subscription rules under the Restore Online Shoppers' Confidence Act.

The FTC's authorizing statute provides some jurisdictional quirks relevant to a fintech firm. The FTC Act exempts banks from the FTC's jurisdiction; while the FTC can subpoena a bank for records, a bank cannot be the subject of an FTC enforcement action. But be careful, because that limitation does not apply to any non-bank entity that may work with a bank, for example non-bank fintechs that may offer Banking as a Service, or lead generators that may connect banks with prospective customers. The FTC also takes the view that "consumers" it can protect include small businesses (absent statutory definitions to the contrary), such that companies offering B2B solutions regularly are the subjects of FTC actions.

03

HOW DOES THE FTC USE THESE POWERS IN THE FINTECH SPACE?

Over the past decade, the agency has built up experience in a number of areas relevant to fintechs. Below are just a few:

- *Lead generation*. The FTC has long been interested in lead generators — the companies that acquire consumer information to provide leads on possible sales to other companies, including fintech lenders and other providers. Cases involving these entities often involve misrepresentations related to sharing data in ways that are at odds with representations to consumers when obtaining their consent. For example, the FTC has brought actions in which the lead generator told consumers that it would use the data only to connect consumers with lenders, but then used the data for other activities, including marketing. Similarly, the FTC looks skeptically at lead generators who represent that they connect consumers with "the best" lenders (think the "top 10" rankings) but that really connect with lenders who generate the most revenue for the lead generator. And liability has not ended with the client-facing lead generators themselves: the FTC also has brought cases against the companies and lenders that have purchased the leads, on the theory that the lead generators were acting as their agents.

- *Unauthorized fees.* One of the FTC's bread-and-butter actions involve unauthorized fees. These cases can run the gamut, from boiler-room frauds stealing from consumers, to cases where the agency alleges that companies hid fees or

failed to disclose fees adequately. Cases against fintechs have generally fallen into the latter category, with the primary takeaway being that the FTC has looked with great skepticism on fees disclosed only in terms and conditions, even if those practice would be sufficient to obligate customers under state-law contract principles.

- *Access to funds.* In cases as diverse as payments and neobanks, the FTC has brought cases where companies did not provide consumers with access to funds in a timely manner. These cases often are difficult for the FTC. While consumers frequently complain of transfer or withdrawal delays, there are not general rules regarding how long companies have to effect those transfers. For that reason, the FTC often has built these cases on deception theories — that the company promised transfers in a certain timeline, but did not deliver. For example, one payments company was sued because its promise of overnight access did not account for the company's KYC and other processes that might slow down transfers from in-app funds to a regular bank account.

- *Gig economy.* Like many regulators, the FTC is interested in companies in the gig economy. Because these companies operate in a two-sided market, issues can arise both from consumers who purchase goods or services, and also from the individuals who work using those platforms. Focusing on the platform users here, the FTC has brought a number of actions alleging that companies made deceptive earnings claims in advertising designed to recruit new users. Although these actions often are brought under Section 5 of the FTC Act directly, the FTC recently initiated a rulemaking on deceptive earnings claims, targeting the gig economy specifically. While in its early stages, the rulemaking appears poised to codify the FTC's existing practice, and possibly to provide specific guardrails regarding certain claims such as when companies use the word "up to" to qualify representations.

- *Subscriptions.* As part of the Restore Online Shoppers' Confidence Act, the FTC has authority to sue companies that take customer money through "negative option" products sold over the internet. In English, a "negative option" is nothing more than a recurring subscription, in which the consumer's inaction is taken as consent to continue charging the consumer until the consumer affirmatively cancels the subscription. The rules are straightforward: companies must disclose all material information prior to obtaining customers' billing information and provide an easy means of cancellation. But the FTC has focused on this statute — releasing an enforcement statement related to negative option marketing—in part because it authorizes the agency to collect civil penalties for first-time violators.

- *B2B lending & payments.* As indicated above, the FTC places pride in protecting small businesses, and has brought a number of actions against companies that provide credit to small businesses. For example, in 2020, the agency brought a pair of actions against companies that offer Merchant Cash Advances — a small business lending product structured as a purchase of future receivables, and thus often not subject to state laws governing credit, such as licensing and usury restrictions.

- *Digital assets.* The agency also has an important role in the digital asset space, most recently identified in President Biden's executive order on digital assets as a key agency related to consumer protection. Although the FTC does not take a side in the big regulatory disputes — e.g. "is it a security" — the agency has taken action publicly against companies involved in cryptocurrency. For example, the FTC sued a company operating a pyramid scheme that was offering the "potential" to make substantial sums in bitcoin, but the company's structure ensured that few ever made those amounts. Outside of the scam space, the agency has brought cases against companies that offer services adjacent to digital asset transactions, including a case against a company that sold bitcoin mining equipment for delays in sending equipment.

- *Payment processors.* While many of the same lessons above apply to companies that process payments, companies in this area also have been the subject of liability where they facilitate scams by processing payments between victims and perpetrators. These cases often are charged either as "unfair" practices under Section 5 of the FTC Act or, if the scams involved telemarketing, providing substantial assistance to violators under the Telemarketing Sales Rule. These cases are not based on strict liability. Rather, they generally require knowledge or conscious avoidance of knowledge by, for example, ignoring red flags.

> ***Over the past decade, the agency has built up experience in a number of areas relevant to fintechs***

04

SO, WHAT CAN THE FTC DO WHEN A COMPANY BREAKS THE LAW?

As a civil law enforcement entity, nobody will go to jail (although the agency regularly refers fraud cases to the Department of Justice for prosecution). The agency's primary tool for first-time offenders is conduct relief, either via a cease-and-desist order issued by the Commission through its administrative process, or via an injunction issued by a federal court. The provisions can range from the banal — a "sin no more" order prohibiting the company from violating the law in the same way again — to industry bans and material limitations on business practices. In recent years, the agency has been more creative in crafting injunctive relief, for example by requiring companies that have unlawfully collected user information to delete all the information and any algorithms that relied on that data, or by requiring multi-year cybersecurity audits if the violation involved inadequate or deceptive data security.

Notably, the FTC can sue not only the company, but also individuals who knew of the violation and had authority to control the conduct. This sort of liability is more obviously appropriate in smaller companies and boiler room operations where the owner also was actively engaged in a fraud. But the FTC also has brought cases against officers of large corporations, with Republican Commissioners often dissenting on that point.

Monetary sanctions are the agency's other tool, but this part is in flux. For the past four decades, the FTC relied on favorable court interpretations holding that Section 13(b) of the FTC Act — which allows the FTC to seek "injunctions" against UDAPs under Section 5 of the FTC Act — also allows courts to order companies to pay restitution. The Supreme Court rejected this practice unanimously in *AMG Capital Management v. FTC*, issued in April 2021. That decision left the FTC scrambling to find other ways to force companies to pay money in connection with enforcement actions. The agency retains a number of traditional ways to obtain monetary relief, including by enforcing laws that expressly authorize civil penalties or other monetary relief, or by enforcing rules that the FTC itself writes.

The agency also has attempted to stretch its existing authorities in questionable ways to obtain money from companies. For example, it recently succeeded in its first use of a broader application of Section 521(a) of the Gramm-Leach-Bliley Act, which authorizes the FTC to obtain money penalties. Originally understood to prohibit scammers from obtaining financial information under a false pretext, the FTC used the statute to allege a violation simply by dint of a misrepresentation in the course of a transaction where a consumer presents payment information. And then there are settlements where the FTC seems not to have any theory for money penalties, but nonetheless has convinced the target to pay as part of the resolution, even if a court could not order the relief.

05

WHAT SHOULD FINTECHS EXPECT FROM THE FTC?

For the past few months, the agency largely has not been executing on Chair Khan's agenda. From October 2021 until just this month (May 2021), the agency was operating only with 2 Democrats and 2 Republicans — Rohit Chopra's seat has been vacant since he left the FTC to lead the Consumer Financial Protection Bureau. For the months of the 2-2 commission, Chair Khan has not been able to push through her aggressive agenda. But that is set to change soon. Alvaro Bedoya, President Biden's pick to fill the third Democrat seat — whose nomination had stalled in the Senate Commerce Committee — was confirmed by the Senate on May 11, 2022 on a 51-50 vote (with Vice President Harris breaking the tie).

Now that Chair Khan has her voting majority, the fintech world should expect a number of changes that might affect their businesses. Based on her priorities and actions to date, here are three of the most prominent spaces to watch.

- *Fair lending enforcement.* Chair Khan has said that one of the FTC's priorities is to increase enforcement against practices that harm "marginalized communities," which of course includes fair lending issues. For companies that offer credit to consumers, that obviously means that the Equal Credit Opportunity Act may be in play in every investigation. But she also suggested expanding further. She and the other Democratic Commissioner issued a separate statement in an auto-lending settlement explaining that they also would have supported a count alleging that discriminatory conduct also should be pleaded as an "unfair" practice in violation of Section 5 of the FTC Act.

  The effect of adopting such a theory of liability could be to expand dramatically the FTC's role

in enforcing anti-discrimination laws or even potentially creating an "ability to repay" requirement. Whereas the Equal Credit Opportunity Act applies only to credit transactions, Section 5 of the FTC Act applies broadly to "commerce." The views from this joint statement come days after the Consumer Financial Protection Bureau similarly announced that it would interpret its own "unfairness" authority under the Dodd-Frank Act to prohibit discrimination outside of the credit context, unmoored from specific anti-discrimination statutes. Whether that theory holds up in court remains to be seen. But expect that there will soon be three democratic votes to transform the FTC into a main anti-discrimination enforcer.

- *Privacy rulemaking.* In December 2021 the agency announced that it might initiate a rulemaking starting in February 2022 on cybersecurity, data privacy, and algorithmic bias. But with only two Democratic commissioners to support the rule, that deadline has come and gone with no action. The rule's provision are not yet clear. If the agency follows the precedent from its other recent proposed rulemakings, this privacy rule likely will aim to codify the legal theories FTC has employed in prior enforcement actions. These certainly would include prohibitions on misrepresentations regarding cybersecurity protections or data collection/sharing practices, among many others. And in speeches, both Chair Khan and Sam Levine, the FTC's Director of the Bureau of Consumer Protection, have flagged their concern with the standard notice-and-consent process widely used in the market.

  The rule itself likely will not be final for some time. FTC rulemaking is more involved than the notice-and-comment process under the Administrative Procedure Act. In addition to a proposed and final rule, the FTC must issue an advanced notice of proposed rulemaking, prove that the practices at issue are "prevalent," and hold a hearing where concerned individuals can present their own evidence and, if necessary, cross-examine the FTC's evidence. And that is all before court challenges.

> ***Now that Chair Khan has her voting majority, the fintech world should expect a number of changes that might affect their businesses***

- *Enforcement against dominant platforms and intermediaries*. Another consistent theme in Chair Khan's speeches is a desire to re-focus enforcement into "dominant platforms" and key market intermediaries. Her reasons seem largely one of resource allocation — moving away from one-off whack-a-mole fraud cases to more complex matters where conduct relief can have a much larger effect on consumers across the market. While this shifting enforcement may not involve new legal theories, larger companies in this space should be aware that they are under increased scrutiny.

06 CONCLUSION

The FTC has a long history of enforcing its laws in the fintech space. This focus is likely to increase now that Chair Khan has her third Democratic vote to proceed on a more aggressive enforcement and regulatory agenda. How this ends will depend on how far the agency is willing to push, and whether companies are willing to test novel theories in court. I would stay tuned.

WHAT'S **NEXT**

For June 2022, we will feature a TechREG Chronicle focused on issues related to **Content Regulation**.

ANNOUNCEMENTS

CPI TechREG CHRONICLES July & August 2022

For July 2022, we will feature a TechREG Chronicle focused on issues related to the **Gig Economy**. And in August we will cover **Editorial Advisory Board**.

Contributions to the TechREG Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI TechREG Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "TechREG Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers in any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

ABOUT **US**

Since 2006, **Competition Policy International** ("CPI") has provided comprehensive resources and continuing education for the global antitrust and competition policy community. Created and managed by leaders in the competition policy community, CPI and CPI TV deliver timely commentary and analysis on antitrust and global competition policy matters through a variety of events, media, and applications.

As of October 2021, CPI forms part of **What's Next Media & Analytics Company** and has teamed up with **PYMNTS**, a global leader for data, news, and insights on innovation in payments and the platforms powering the connected economy.

This partnership will reinforce both CPI's and PYMNTS' coverage of technology regulation, as jurisdictions worldwide tackle the regulation of digital businesses across the connected economy, including questions pertaining to BigTech, FinTech, crypto, healthcare, social media, AI, privacy, and more.

Our partnership is timely. The antitrust world is evolving, and new, specific rules are being developed to regulate the so-called "digital economy." A new wave of regulation will increasingly displace traditional antitrust laws insofar as they apply to certain classes of businesses, including payments, online commerce, and the management of social media and search.

This insight is reflected in the launch of the **TechREG** Chronicle, which brings all these aspects together — combining the strengths and expertise of both CPI and PYMNTS.

Continue reading CPI as we expand the scope of analysis and discussions beyond antitrust-related issues to include Tech Reg news and information, and we are excited for you, our readers, to join us on this journey.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY™ INTERNATIONAL