



THE GUIDE TO COMPLIANCE

FIRST EDITION

Editors

Johanna Walsh, Alejandra Montenegro Almonte
and Alison Pople QC

Guide to Compliance

First Edition

Editors

Johanna Walsh

Alejandra Montenegro Almonte

Alison Pople QC

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2022
For further information please contact insight@globalinvestigationsreview.com

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK
© 2022 Law Business Research Ltd
www.globalinvestigationsreview.com

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of July 2022, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-83862-868-0

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Ankura Consulting Group, LLC

Baker McKenzie

Beccar Varela

Cloth Fair Chambers

Davis Polk & Wardwell LLP

Debevoise & Plimpton LLP

Demarest Advogados

Freshfields Bruckhaus Deringer

Galicia Abogados, SC

Herbert Smith Freehills

Jenner & Block LLP

Miller & Chevalier Chartered

Mishcon de Reya LLP

Ropes & Gray International LLP/R&G Insights Lab

Publisher's Note

The Guide to Compliance is published by Global Investigations Review (GIR) – the online home for everyone who specialises in investigating and resolving suspected corporate wrongdoing. We tell our readers everything they need to know about all that matters in their chosen professional niche.

Thanks to GIR's position at the heart of the investigations community, we sometimes become aware of gaps in the literature before others. *The Guide to Compliance* is a good example. For, although there has been significant growth in the availability of guidance on compliance worldwide – and in particular what amounts to a successful compliance programme (nobody makes a mistake on purpose but that does not mean we should not try harder to avoid making them) – to date, there has been no systematic guide to how exactly compliance fits into the enforcement equation. This book aims to solve that.

It combines a systematic *tour d'horizon* of the rules in place around the world with specific practical advice and a scan of the horizon in parts two and three. As such, it should swiftly earn a position in the front row of our readers' libraries.

The guide is part of GIR's steadily growing technical library. This began six years ago with the first appearance of the revered GIR *Practitioner's Guide to Global Investigations*. *The Practitioner's Guide* tracks the life cycle of any internal investigation, from discovery of a potential problem to its resolution, telling the reader what to do or think about at every stage. Since then, we have published a series of volumes that go into more detail than is possible in *The Practitioner's Guide* about some of the specifics, including guides to sanctions and to monitorships. I urge you to seek out all of them.

If you are a GIR subscriber, you will have received a copy already, gratis, as part of your subscription. If you are not, you can read an e-version at www.globalinvestigationsreview.com.

Last, I would like to thank the editors of *The Guide to Compliance* for bringing us this idea and for shaping our vision, and the authors and my colleagues for the clan with which it has been brought to life.

We hope you find the book enjoyable and useful. And we welcome all suggestions on how to make it better. Please write to us at insight@globalinvestigationsreview.com.

David Samuels

Publisher, GIR

July 2022

Contents

Introduction.....1
Johanna Walsh, Alejandra Montenegro Almonte and Alison Pople QC

PART I: GLOBAL COMPLIANCE REQUIREMENTS AND ENFORCEMENT

1 UK Compliance Requirements.....9
Niki Stephens, Alison Geary, Min Weaving and Elizabeth Hope

2 UK Compliance Enforcement.....25
Alison Pople QC and Kathryn Arnot Drummond

3 US Compliance Requirements.....43
Alejandra Montenegro Almonte, Ann K Sultan and FeiFei (Andrea) Ren

4 US Compliance Enforcement.....57
Kara Brockmeyer, Ivona Josipovic, Andreas A Glimenakis
and Berk Guler

5 Asia-Pacific Compliance Requirements75
Kyle Wombolt, Pamela Kiesselbach, Valerie Tao and Antony Crockett

6 Asia-Pacific Compliance Enforcement94
Mini vandePol, Christine Cuthbert, Gerald Lam, Andrea Kan
and Yuki Yung

7 Latin America Compliance Requirements.....114
Daniel S Kahn

8 Latin America Compliance Enforcement: Argentina, Brazil and Mexico	132
Maximiliano D'Auro, Rodrigo Allende, Eloy Rizzo, Andre Luis Leme, Victoria Teles Manhães Barreto Arcos, Carlos Chávez and Marianela Romero	

PART II: COMPLIANCE ISSUES IN PRACTICE

9 Navigating Global Compliance Issues.....	151
Ali Sallaway, Zara Merali, Daniel Travers and Xin Liu	
10 Compliance Issues in Corporate Transactions	168
Georgie Farrant, Gareth Austin, Michelle Rae Heisner and Andrew Martin	
11 The Role of Audit and Monitoring in Compliance	184
Sara Shaner, Shelly Mady and Jean-Michel Ferat	

PART III: EMERGING COMPLIANCE FIELDS

12 Compliance Issues in Cryptocurrency	201
Kayvan B Sadeghi and Lawrence W McMahon	
13 Compliance Issues in Environmental, Social and Governance Matters	213
Matthew Ewens, Charlotte Wilson and Christopher Gribbin	
14 Understanding and Shaping Organisational Culture to Disrupt the Cycle of Misconduct.....	224
Zachary Coseglia, Amanda Raad, Caitlin Handron, Leah Dowd, Jeffrey Irwin and Karina Thomas	
Appendix 1: About the Authors.....	239
Appendix 2: Contributors' Contact Details	263

Introduction

Johanna Walsh, Alejandra Montenegro Almonte and Alison Pople QC¹

We are delighted to publish the first edition of the *GIR Guide to Compliance*, which brings together compliance guidance and criminal enforcement trends relating to financial crimes and misconduct.

While laws prohibiting and punishing financial crimes and misconduct have long existed, during the past 20 years or so, governments have steadily increased efforts to enforce these laws and to prosecute those who violate them. In parallel with (and often embedded) in those enforcement efforts, many governments have issued compliance guidance and, in many instances, codified that guidance in regulatory or legal obligations. Compliance now lies firmly at the heart of prevention and enforcement of financial crimes and misconduct, and the developments in this area demonstrate a firm commitment from global legislators, policymakers and law enforcement to continue in this approach.

For instance, in June 2022, the United Kingdom published the Law Commission Options paper for reform to corporate criminal liability. Among the options under consideration is a new corporate criminal offence in the United Kingdom of ‘failure to prevent fraud by an associated person’. If accepted and brought onto the statute books in the United Kingdom, the consequences for corporate compliance programmes will be highly significant. In October 2021, US Deputy Attorney General Lisa Monaco issued a memorandum announcing ‘initial revisions’ to the Department of Justice’s (DOJ) corporate criminal enforcement policies and announcing the creation of a Corporate Crime Advisory Group with the DOJ. The Group will have a ‘broad mandate’ to update the DOJ’s

¹ Johanna Walsh is a partner at Mishcon de Reya LLP, Alejandra Montenegro Almonte is a member and vice chair of the international department at Miller & Chevalier Chartered and Alison Pople QC is a barrister at Cloth Fair Chambers.

approach to ‘cooperation credit, corporate recidivism, and the factors bearing on the determination of whether a corporate case should be resolved through a deferred prosecution agreement (DPA), non-prosecution agreement (NPA), or plea agreement’, among other topics.

In the Asia-Pacific (APAC) region, a number of jurisdictions are moving into a compliance-based approach in relation to corporate bribery issues. In June 2020, Malaysia introduced corporate liability on a failure-to-prevent basis and the Malaysian Anti-Corruption Commission charged a company and its director under this new corporate liability regime for the first time in March 2021. Elsewhere in the region, Australia is awaiting the enactment of a corporate offence of failure to prevent bribery by an associate, while Singapore is also reviewing its foreign bribery laws.

The prominence of environmental, social and governance (ESG) issues in recent years exemplifies the global policy shift to a compliance-based approach to corporate good conduct. ESG topics are deeply interwoven into financial misconduct issues. Supply chain issues represent an obvious example, as they can be highly complex and often extremely difficult to navigate for a corporate.

The rapid increase in the use and evolution of cryptocurrency in the past decade has posed challenges for governments as they consider whether and how to regulate the use of digital assets. Although the United States has opted, at federal level, to rely on existing regulatory and compliance regimes, other jurisdictions, such as Singapore and Switzerland, have recently introduced specific laws aimed at promoting themselves as ‘crypto-friendly’ environments.

For many global and multinational corporations, evaluating enforcement risk and navigating the patchwork of compliance expectations can be a challenge. Hence, the idea for this *Guide to Compliance* was born.

Overview of the Guide

This Guide undertakes to capture enforcement and compliance trends across the globe. Specifically, the Guide aims to:

- bring together an overview of the compliance regimes in respect of economic crime and misconduct in different jurisdictions in terms of both requirements and enforcement;
- provide practical assistance to practitioners tackling the challenges created by multi-faceted and multi-jurisdictional global compliance issues; and
- provide insight and guidance on key emerging areas in respect of compliance in economic misconduct.

The challenge of summarising an entire body of enforcement and compliance trends is not a simple one. Each of the chapters included in this Guide seeks to summarise the trends that best capture the current state of enforcement and compliance in the relevant region or subject matter. We look forward to continuing to build on and deepen these summaries in future editions.

Part I: Global Compliance Requirements and Enforcement

- **UK Compliance Requirements:** The focus of this chapter is on those areas of criminal risk and regulatory risk arising from compliance failures. In terms of criminal risk, the authors consider bribery, tax evasion and money laundering and set out the relevant legislative framework together with the guidance issued by the authorities in respect of each. From a regulatory risk perspective, the authors expand on the approaches to compliance failures taken by the Financial Conduct Authority and the Gambling Commission.
- **UK Compliance Enforcement:** This chapter builds on the first chapter and sets out the main areas of enforcement activity in the United Kingdom, drawing on lessons that can be derived from previous enforcement outcomes together with statements of policy from the various UK enforcement agencies. As with the UK Compliance Requirements chapter, the authors divide the chapter between criminal enforcement and regulatory enforcement.
- **US Compliance Requirements:** This chapter discusses the four main sources of documents on compliance requirements issued by the DOJ. The chapter specifically sets forth the elements of an effective compliance programme and DOJ expectations with regard to each.
- **US Compliance Enforcement:** Building on the chapter on US Compliance Requirements, the authors explain how US authorities incorporate compliance factors into white-collar enforcement. They describe key considerations that companies should bear in mind when evaluating potential enforcement risks and when embarking on the reporting and settlement process with US authorities.
- **Asia-Pacific Compliance Requirements:** There are unique challenges in covering the APAC region from a compliance perspective owing to the diversity of government regimes, cultures and economies. The authors have risen to the challenge and provide a valuable overview covering issues in a thematic way in respect of key areas of risk such as bribery and money laundering.

- **Asia-Pacific Compliance Enforcement:** The authors cover enforcement priorities, outcomes and trends by reference to key jurisdictions in the region – Australia, China, Hong Kong, Japan and Singapore – while also providing a commentary on emerging trends and key compliance issues for corporates in the APAC region.
- **Latin America Compliance Requirements:** During the past decade, compliance has increased in importance in Latin America. In this chapter, the authors provide an overview of the guiding compliance principles applicable to the region and lay out best practices for designing, implementing and maintaining an effective corporate anti-corruption compliance programme that complies with such requirements and principles, helps companies avoid and identify misconduct, and mitigates liability where a violation occurs.
- **Latin America Compliance Enforcement:** Latin America as a region continues to evolve in its enforcement efforts with each individual country being at a different stage in that evolution. In this chapter, the authors focus on enforcement trends in some of the more developed jurisdictions – Argentina, Brazil and Mexico.

Part II: Compliance Issues in Practice

- **Navigating Global Compliance Issues:** The authors provide guidance for in-house counsel and compliance teams in multinational businesses on how to navigate global compliance issues, taking into account particular risk vulnerabilities, including in different jurisdictions, sectors and emerging risks, together with how to put in place an effective compliance framework to mitigate these risks. The chapter includes a checklist for managing a crisis should one arise.
- **Compliance Issues in Corporate Transactions:** Identifying compliance risks in corporate transactions is essential not just to avoid the risk of a purchaser making a bad buy but also to avoid any risk of successor liability or future civil claims for historic or ongoing compliance issues. The authors identify the key compliance areas in due diligence and how to conduct an effective assessment of compliance policies and procedures or issues in third-party dealings. Finally, the authors consider how best to remediate any compliance issues identified in the course of the due diligence process.
- **The Role of Audit and Monitoring in Compliance:** Periodic risk-based audits and ongoing monitoring are emblematic of a maturing compliance programme. In this chapter, the authors discuss regulators' expectations with respect to the role of audits and monitoring, the differences between the two exercises and the critical role of data and enterprise resource planning systems. Recognising

the inherent challenges in developing and implementing effective monitoring and auditing programmes, the authors provide practical guidance on how to action such programmes.

Part III: Emerging Compliance Fields

- **Compliance Issues in Cryptocurrency:** The advent of digital assets has presented a number of unique regulatory and compliance challenges. In this chapter, the authors provide overviews both of those challenges and the current regulatory landscape, primarily in the United States but also in a number of other jurisdictions where the regulatory landscape and compliance regimes are evolving to address those challenges.
- **Compliance Issues in Environmental, Social and Governance Matters:** The authors have focused on two fundamental areas of risk for corporates in the ESG arena: supply chain issues and specific reporting requirements. They also examine the emerging issue of voluntary reporting in respect of ESG matters and consider issues of practical importance, such as investigation and remediation.
- **Understanding and Shaping Organisational Culture to Disrupt the Cycle of Misconduct:** The importance of a company's culture on the effectiveness of its compliance programme cannot be understated. This chapter considers how corporates can use behavioural science to enhance their compliance culture, introducing the concept of the 'culture cycle' and using examples to demonstrate how deficient corporate culture can enable misconduct. The authors look at ways to measure and assess corporate culture and the changes that can be made to foster a stronger culture of ethics and compliance.

Our thanks

We are extremely grateful to our wonderful contributors. Their deep expertise and thoughtful insight are demonstrated and shared in the chapters that follow. It has been a great pleasure to work with them in bringing this project to fruition, and we will look forward to continuing to work with them in future editions of this GIR Guide. We also extend our thanks to Celia Marr, managing associate at Mishcon de Reya LLP, for her assistance with preparing chapter outlines.

Mahnaz Arta, Hannah Higgins and Georgia Goldberg, at Law Business Research, have honed to a fine art the skill of herding busy practitioners to make these GIR Guide publications possible and we are extremely grateful that they do so, and that they do it with such professionalism, patience and good humour.

Part III

Emerging Compliance Fields

CHAPTER 12

Compliance Issues in Cryptocurrency

Kayvan B Sadeghi and Lawrence W McMahon¹

More than 10 years have passed since Satoshi Nakamoto introduced the first blockchain network and associated digital asset, Bitcoin. In that time, the blockchain industry has grown into a trillion-dollar ecosystem attracting the attention of consumers, investors, enterprises and governments around the world. Blockchain technology and the associated digital assets raise exciting prospects of new forms of economic development but also present a serious challenge to existing regulatory and compliance regimes. This chapter provides an overview of those challenges and of the current regulatory landscape, primarily in the United States but also in a number of jurisdictions² where the regulatory landscape and compliance regimes are evolving to address these challenges.

Regulatory challenges of digital assets

Digital assets present unique regulatory challenges for a number of reasons. Many of those challenges stem from the core innovation of blockchain: to enable peer-to-peer transfer of value with less need for trusted intermediaries. First, unlike many other technological innovations, blockchain networks disrupt highly regulated financial markets. Second, the core disruption is to reduce the need for intermediaries, but many existing regulatory frameworks are built around regulating those intermediaries. Third, blockchain technology enables myriad new forms of assets that do not fit neatly within the categories of financial instruments addressed by existing regulations, even though they may trade in markets

1 Kayvan B Sadeghi is a partner and Lawrence W McMahon is an associate at Jenner & Block LLP.

2 The United Kingdom, the European Union, Switzerland, Singapore and Dubai.

resembling conventional financial markets. Fourth, the technology and resulting markets are global, thus requiring some measure of coordination and limiting the efficacy of efforts to regulate in any one jurisdiction.

As a result, the extensive global infrastructure of financial regulation is confronting fundamental questions of what existing regulations apply and to whom, and how to enforce them, in a rapidly evolving blockchain ecosystem that continues to adapt and raise new questions faster than the law can evolve to provide answers.

Broadly, there are two primary approaches taken by governments, in varying combinations: (1) seek to fit digital assets into existing regulatory and compliance regimes (the approach primarily relied on at the federal level in the United States to date); and (2) create new laws or amend existing laws specifically to address digital assets (as is evident in jurisdictions such as Switzerland and Dubai, and certain states in the United States such as New York).

This chapter offers a high-level overview of the relevant laws in selected jurisdictions that will be relevant for compliance concerns. Although approaches differ, a few recurring themes emerge. First, most jurisdictions recognise that digital assets are at times used as an investment vehicle and, thus, may implicate the laws and regulations governing securities markets, largely with an investor protection objective. Second, governments recognise that digital assets could be used as a tool for money laundering, sanctions avoidance or other illicit transactions and, therefore, seek to apply know-your-client or anti-money laundering regulations (or both), either by fitting certain digital asset transactions within existing laws or by crafting new laws to make these obligations explicit for digital assets.

Current regulatory landscape for digital assets

United States

There are a number of US regulators with overlapping authority over digital assets at both the federal and state levels. Unlike other jurisdictions, there is no overarching digital asset regulatory regime to which a participant can look for compliance obligations. Instead, businesses must consider distinct areas of US federal law – and, in some instances, state law – that may be relevant to any given digital-asset activity.

Although it is not an exhaustive list, prominent areas of regulatory and compliance obligations include federal and state securities and commodities laws, and federal and state banking laws governing money services businesses. Furthermore, a presidential Executive Order on digital assets issued by the Biden administration called on the Consumer Financial Protection Bureau, the Federal Trade Commission and other agencies to attend inter-agency meetings on digital

asset regulatory questions, each of which has its own regulatory ambit that may be implicated by certain digital asset activities.³ On 7 July 2022, the Secretary of the Treasury, in coordination with the heads of other relevant agencies, delivered to President Biden a framework for international engagement on digital assets, which emphasises active engagement with international partners through standard-setting bodies such as the Financial Stability Board, the Financial Action Task Force and others.⁴ Certain states also have developed digital asset regulations, including the New York State Department of Financial Services BitLicense requirement for ‘virtual currency business activity’.⁵

The SEC and the Securities Laws

The securities laws of the United States are enforced primarily by the Securities and Exchange Commission (SEC). Anyone engaged in digital asset transactions must be mindful of whether the digital asset activity in question amounts to an offer or sale of securities, or whether the digital asset itself is a ‘security’ under the securities laws. If so, then a host of registration and reporting requirements under the securities laws may come into play,⁶ and an entity must further enquire as to whether it meets the definition of an ‘issuer’, an ‘exchange’, a ‘broker’ or a ‘dealer’.

The SEC’s focus on digital assets continues to grow. On 3 May 2022, it announced that it was nearly doubling the size of its Crypto Assets and Cyber Unit,⁷ with a continuing focus on investor protection as reflected in a statement from the SEC’s director of enforcement, who commented: ‘Crypto markets have exploded in recent years, with retail investors bearing the brunt of abuses in this space’.

3 ‘Executive Order on Ensuring Responsible Development of Digital Assets’ (9 March 2022), at <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> (last accessed 4 July 2022).

4 <https://home.treasury.gov/news/press-releases/jy0854> (last accessed 11 July 2022).

5 23 NYCRR § 200.

6 For example, an issuer of securities to the public generally must register those securities with the US Securities and Exchange Commission (SEC) and disclose detailed information about the financials, structure and management of their underlying business. See 15 U.S.C. § 78l. After registration, issuers are also subject to ongoing annual, quarterly and other reporting requirements. See 15 U.S.C. § 78m.

7 <https://www.sec.gov/news/press-release/2022-78> (last accessed 4 July 2022).

'Securities' under US federal law

The Securities Act of 1933 and the Securities Exchange Act of 1934 list a number of enumerated categories of instruments that fall within the definition of a 'security', including stocks, bonds, debentures, notes, investment contracts and many others.⁸ The category 'investment contract' functions as a catch-all for numerous investment transactions or schemes not otherwise captured in the statutory definitions, and it is the category into which the SEC places many digital asset transactions. The seminal test for what constitutes an investment contract was set forth in the Supreme Court case, *SEC v. Howey*. As the Court stated and the SEC maintains today, the term 'investment contract', as used to define a security, 'embodies a flexible rather than static principle, . . . capable of adaptation to . . . countless and variable schemes'.⁹ *Howey* creates a four-part test that the SEC has used to determine whether a digital asset offering is a securities offering. Although there are slightly different articulations of the test, for a transaction or scheme to constitute a securities offering, it must generally involve (1) an investment of money (2) in a common enterprise (3) with a reasonable expectation of profits, (4) derived from the effort of others.

Although, to date, the SEC has not issued any rule-making or definitive guidance on the application of securities laws to digital assets, the *Howey* test has guided the SEC's thinking as its position on digital assets has evolved across a series of reports, enforcement actions and public speeches.¹⁰ In 2019, the SEC released a 'Framework for "Investment Contract" Analysis of Digital Assets',¹¹ which spelled out how the agency's staff are likely to approach digital assets under *Howey*, though it is careful to state that it is not a binding standard.

8 See 15 U.S.C. § 77b(a)(1).

9 *SEC v. Howey*, 328 U.S. 293, 299 (1946).

10 The SEC's first substantial action relating to cryptocurrencies was its July 2017 'Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO' (see <https://www.sec.gov/litigation/investreport/34-81207.pdf> (last accessed 11 July 2022)), in which the SEC staff made clear that they viewed the sale of DAO tokens as a securities offering. In June 2018, the director of the SEC's Division of Corporations gave prepared remarks at a cryptocurrency summit, in a speech titled 'Digital Asset Transactions: When Howey Met Gary (Plastic)', which was interpreted as conveying the SEC's staff's position at the time – see <https://www.sec.gov/news/speech/speech-hinman-061418> (last accessed 11 July 2022). The SEC also has brought dozens of enforcement actions, a list of which is maintained at <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions> (last accessed 11 July 2022).

11 <https://www.sec.gov/files/dlt-framework.pdf> (last accessed 4 July 2022).

An additional area in which the application of US securities laws to digital assets continues to evolve is in the distinction between a ‘securities offering’ and a ‘security’. Although the SEC maintains the position that initial coin offerings (ICOs) are securities offerings, it is a separate question whether the digital assets themselves are securities and must be regulated as such. For example, selling a token in a fundraising scheme may constitute a securities offering, but the token itself may not be a security if it carries no rights to any ownership or future payments.

Where compliance currently stands under US securities laws
To date, SEC officials have stated that the agency does not consider Bitcoin to be a security, and ETH may not be a security.¹² However, the SEC has viewed most ICOs as securities offerings. Therefore, any activity that involves issuance and distribution of a new digital asset may constitute a securities offering under US law and trigger a variety of compliance obligations.

Compliance obligations fall on multiple sets of constituents under US securities law. In an offering such as an ICO, the offeror will be an issuer. An ‘issuer’ includes ‘every person who issues or proposes to issue any security’.¹³ An entity engaging in issuing a new digital asset that has the essential characteristics of an investment will likely be considered by the SEC to be an issuer subject to the full registration requirements as applicable to any other issuer of securities.

Separate from issuance, any business that effects digital asset transactions on behalf of others, or that engages in a business of buying and selling digital assets, should consider whether the requirements for brokers or dealers may apply. ‘Brokers’ are those who effect securities transactions ‘for the account of others’. A ‘dealer’ is any person buying or selling securities for that person’s own account, but there is a ‘trader exception’ when the buying or selling is ‘not part of a regular business’.

12 <https://www.sec.gov/news/speech/speech-hinman-061418> (last accessed 4 July 2022) (William Hinman, Director of the SEC Division of Corporate Finance, explains that, in his view, ‘current offers and sales of Ether are not securities transactions’ as is also the case with Bitcoin); but see <https://decrypt.co/103926/sec-chair-gensler-bitcoin-not-security-what-about-ethereum> (last accessed 14 July 2022) (quoting and linking to a video of an interview on 27 June 2022 with SEC Chairman Gary Gensler, in which he identifies Bitcoin as a commodity but makes clear that Bitcoin is the ‘only one’ for which he is willing to make that statement).

13 15 U.S.C. § 77b(a)(4).

Besides token sales and exchanges, the SEC is also seeking to regulate accounts that offer interest or similar rewards on token balances. In February 2022, the SEC announced a settled enforcement against BlockFi, in which it found that BlockFi's cryptocurrency-based interest accounts were unregistered securities offerings and that BlockFi operated as an unregistered investment company. BlockFi paid a total US\$100 million in penalties to the SEC and state-level securities enforcers, and embarked on a process to register its interest accounts with the SEC as securities.¹⁴

In addition, each of the 50 states has its own securities laws. Compliance with state securities laws is often accomplished by registering with the SEC, but where a product or business is not registered with the SEC, it may be subject to registration requirements in one or more states.

The Commodities Futures Trading Commission and the Commodity Exchange Act

Although the SEC may view some digital assets as securities, many are also likely be commodities according to the Commodities Futures Trading Commission (CFTC), the agency that enforces the Commodity Exchange Act (as passed in 1936 and subsequently amended (CEA)). Furthermore, just because one digital asset is part of a securities transaction does not necessarily mean that it cannot also be a commodity, thereby creating the potential for overlapping regulation.

The CFTC does not have general regulatory jurisdiction over the 'spot' market in digital assets. Rather, the Commission regulates futures and other derivatives of commodities and the marketplaces or exchanges on which commodities trade. The CFTC also asserts jurisdiction over fraud within the spot market for commodities in which futures are traded.

Those engaged in any type of activity concerning swaps, futures or other derivatives of digital assets are likely to fall under the regulatory authority of the CFTC, which pursues enforcement against organisations that fail to register as swap execution facilities or future commission merchants.¹⁵ Likewise, if an organisation is a commodity trading adviser or commodity pool operator, the CFTC requires registration, record-keeping and disclosure. Beyond the regulatory requirements of certain business models under the CEA, organisations and individuals must comply with the CEA's anti-fraud and anti-manipulation mandates,

14 <https://www.sec.gov/news/press-release/2022-26> (last accessed 4 July 2022).

15 See, e.g., <https://www.cftc.gov/PressRoom/PressReleases/8433-21> (last accessed 4 July 2022).

which are wide in scope. For example, the CFTC pursues enforcement action against a variety of potentially deceptive trading practices, such as ‘spoofing’, in which market participants place orders they do not intend to complete, and manipulation of commodity or foreign-currency benchmark prices.¹⁶

Money services businesses and money transmitters under the Bank Secrecy Act

The Financial Crimes Enforcement Network (FinCEN), an enforcement body under the United States Treasury Department, has established regulation and compliance requirements for companies that move money as a business, such as currency dealers or cheque cashers. Money services businesses and money transmitters must register with FinCEN, and those businesses must ensure compliance with anti-money laundering regulations under the Bank Secrecy Act of 1970.

FinCEN has released specific guidance stating that money transmitter regulation applies equally to the national currencies of sovereign states and to cryptocurrencies.¹⁷ Guidance issued in 2019 by FinCEN¹⁸ analysed various virtual currency business models and concluded that many of them would qualify as money transmitters and thus fall under the registration and other requirements. Cryptocurrency businesses that transmit value between persons or entities are likely to be subject to FinCEN regulation.

Additionally, most states have their own registration requirements for money transmitters, thus requiring money services businesses to register in each state in which they do business (with some exceptions).

New York's virtual currency business activity licence (BitLicense)

A handful of states have introduced cryptocurrency-specific legislation, including Wyoming, which has exempted cryptocurrency from money transmitter regulation and property tax. The most restrictive state in the digital-asset regulator space is New York.

16 See, e.g., <https://www.cftc.gov/PressRoom/PressReleases/8534-22> (last accessed 11 July 2022); <https://www.cftc.gov/PressRoom/PressReleases/7181-15> (last accessed 11 July 2022).

17 <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (last accessed 4 July 2022).

18 <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> (last accessed 11 July 2022).

Organisations that operate in New York are required to maintain a licence, known colloquially as a ‘BitLicense’, if they engage in ‘virtual currency business activity’. This includes receiving or transmitting virtual currency, holding custody of virtual currency on behalf of others, buying and selling virtual currency as a customer business, performing exchange services as a customer business, or administering or issuing virtual currency.¹⁹ In essence, New York creates an *ex ante* licensing requirement before cryptocurrency-based business activities can be undertaken. Although this is the same approach as taken in some other jurisdictions, such as Dubai, it is a notable departure from the prevailing regulatory norm in the United States, in which regulatory agencies exercise discretion to engage in *ex post* enforcement activities rather than creating up-front requirements to enter the market.

The United Kingdom

The primary regulator of note in the United Kingdom is the Financial Conduct Authority (FCA), which regulates financial services firms and the British financial markets. The FCA divides digital assets into regulated tokens and unregulated tokens.²⁰ The two types of regulated tokens are security tokens, which provide the functional equivalent of equity or debt rights, and e-money tokens, which fall under the Electronic Money Regulations 2011²¹ but do not include cryptocurrencies such as Bitcoin, which are sometimes referred to in UK guidance as ‘exchange tokens’.²²

Exchange tokens are considered to be unregulated by the FCA, but since January 2020, they are subject to the UK’s Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.²³ Therefore, despite the lack of specific regulatory classification for many of the most common digital assets, compliance with anti-money laundering rules means that businesses exchanging or providing custodian services must register with the FCA, a process that requires disclosure of business plans, internal systems and controls, anti-money laundering risk assessment and other information.²⁴

19 See 23 NYCRR § 200.3(c).

20 <https://www.fca.org.uk/firms/cryptoassets> (last accessed 4 July 2022).

21 SI 2011/99.

22 ‘Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3’ (July 2019), at 9, at <https://www.fca.org.uk/publication/policy/ps19-22.pdf> (last accessed 4 July 2022).

23 <https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime> (last accessed 4 July 2022).

24 <https://www.fca.org.uk/cryptoassets-aml-ctf-regime/register> (last accessed 11 July 2022).

The European Union

The European Union is in the process of adopting its Markets in Crypto-assets Regulation (MiCA), which will create a distinct regulatory regime for digital assets within the European Union. Previously, digital currencies were outside the scope of EU legislation.²⁵ The proposed MiCA has been under debate in the European Parliament since 2020, and it will create an EU-wide authorisation requirement for offerors of digital assets. Unlike the British approach, MiCA will create a specific set of regulatory categories specific to digital assets. The details of compliance requirements remain to be settled but on 31 May 2022, EU financial officials called for the forthcoming MiCA to emphasise anti-money laundering and advised that authorised digital asset exchanges should lose their licences for AML violations.²⁶

Switzerland

Switzerland has taken specific steps to hold itself out as a hospitable regulatory environment for cryptocurrency and digital assets. Unlike the United States, the Swiss approach involves delineating specific new regulatory categories for digital assets. Switzerland has presented itself as a hub for crypto innovation, and it has succeeded in making itself an important centre for ICOs.

Although the Swiss Financial Market Supervisory Authority (FINMA) takes the general approach that the same financial markets laws apply regardless of whether new technology underlies transactions, FINMA also issued its 2018 'ICO Guidelines', which create specific regulatory categories into which traditional cryptocurrencies, such as Bitcoin and other digital tokens, will fall.

The ICO guidelines recognise three types of tokens, though it emphasises that hybrids are possible, and, in the case of an ICO, a fact-specific, case-by-case inquiry may still be required to determine where a given token falls. The three enumerated categories are:

- payment tokens, which are synonymous with cryptocurrencies;
- utility tokens, which provide access to a digital application or service; and

25 <https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats> (last accessed 4 July 2022).

26 'Joint ESAs Report on the withdrawal of authorisation for serious breaches of AML/CFT rules', at 19–20, at https://www.esma.europa.eu/sites/default/files/library/joint_report_on_withdrawal_of_authorisation_aml_breaches.pdf (last accessed 4 July 2022).

- asset tokens, which represent rights in traditional assets and are analogous to equities, debt instruments, or derivatives.²⁷

FINMA has indicated that participants in the Swiss digital-asset space should prioritise their attention on Switzerland's securities regulations and anti-money laundering laws. Payment tokens require compliance with the Swiss Anti-Money Laundering Act but not Swiss securities laws. Conversely, asset tokens are regulated as full securities under Swiss law, including with a full prospectus requirement. Utility tokens are a more complex category. If a utility token at the time of its issuance solely confers digital access to some application or service, then it is not regulated as a security. But if a utility token has even a partial function as an investment, then FINMA treats it just like an asset token (i.e., as a security).

Separately, in August 2021, Switzerland implemented its Distributed Ledger Technology Act (the DLT Act), which formally recognises and creates a framework for rights to securities to be recorded on a blockchain ledger rather than traditional registration and certification processes. The DLT Act recognises blockchain-based digital assets as their own category and regulatory target with their own compliance needs that may overlap with, but also be distinct from, traditional financial regulations, such as those covering securities.

Singapore

Like Switzerland, Singapore has promoted itself as a crypto-friendly environment. It has been a successful hub of digital-asset activity, unlike many of its Asian neighbours (such as China, Indonesia and Thailand), which have at times restricted cryptocurrency trading or banned it outright. Singapore has taken the general approach that cryptocurrency businesses want to be regulated because they prefer to know what the rules are rather than to face uncertainties. To that end, cryptocurrency businesses operating in Singapore have long been regulated by the Monetary Authority of Singapore (MAS), and the Payment Services Act created a licensing regime for crypto activity.²⁸

Until recently, Singapore's approach was to regulate more lightly those cryptocurrency operators based in Singapore but who direct their services solely outside Singapore. In this way, Singaporean authorities aimed to adopt a

27 <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/> (last accessed 4 July 2022).

28 <https://www.mas.gov.sg/news/media-releases/2018/new-regulatory-framework-to-enhance-payment-services-in-singapore> (last accessed 4 July 2022).

‘consumer protection’ approach for their own citizens, while offering their city state as a hub for innovations aimed at the citizens of other countries. However, this has changed. On 5 April 2022, Singapore passed the Financial Services and Markets Bill,²⁹ under which digital-asset providers based in Singapore but conducting business in other countries must now abide by Singaporean anti-money laundering and anti-terrorism financing laws.³⁰ The Bill also introduces a licensing regime for Singaporean digital-asset service providers in compliance with Financial Action Task Force standards adopted in 2019 requiring licensing or registration in the jurisdiction where digital assets are created.³¹ Meanwhile, MAS reiterated its position, in January 2022, that cryptocurrency services should not be targeted at the general public of Singapore itself.³²

The current status of Singapore’s digital-asset regulatory approach has established an extraterritorial reach outside Singapore at the same time that activity within Singapore is being curtailed. The effect of Singapore’s increasing regulation remains to be seen.

Dubai

In March 2022, the emirate approved the Dubai Virtual Asset Regulation Law, which establishes the Dubai Virtual Assets Regulatory Authority (VARA), a first-of-its-kind regulator dedicated to digital assets. The Law requires authorisation from VARA before a person may engage in any business activity relating to digital assets, including exchanging digital assets for national currency, exchanging digital assets for other digital assets, and the creation or maintenance of services facilitating or managing such exchanges.³³ The implementation of regulations remains in progress and VARA has not offered a timetable. However, the law

29 <https://www.mas.gov.sg/news/speeches/2022/financial-services-and-markets-bill-second-reading-speech-on-4-april-2022> (last accessed 4 July 2022).

30 <https://www.parliament.gov.sg/docs/default-source/default-document-library/financial-services-and-markets-bill-4-2022.pdf> (last accessed 4 July 2022); see <https://www.mas.gov.sg/news/speeches/2022/explanatory-brief-for-financial-services-and-markets-bill-2022> (last accessed 4 July 2022).

31 <https://www.mas.gov.sg/news/speeches/2022/explanatory-brief-for-financial-services-and-markets-bill-2022> (last accessed 11 July 2022).

32 <https://www.mas.gov.sg/news/media-releases/2022/mas-issues-guidelines-to-discourage-cryptocurrency-trading-by-general-public> (last accessed 4 July 2022).

33 <https://u.ae/en/about-the-uae/digital-uae/regulation-of-digital-properties> (last accessed 4 July 2022).

establishes that Dubai requires a licence to engage in a token offering, to operate a digital-asset platform, or to otherwise offer exchange, transfer, custody or portfolio services for digital assets.³⁴

Conclusion

Digital asset businesses operate in a regulatory environment that is uncertain and constantly evolving. In most jurisdictions, compliance will focus on securities, commodities and banking laws. Given the rapid evolution of technology and the law, and the likelihood of multiple overlapping compliance regimes, it is crucial to stay abreast of the regulatory developments and frequently re-evaluate compliance policies and procedures.

34 <https://mediaoffice.ae/en/news/2022/March/09-03/Mohammed-bin-Rashid-approves-Dubai-Virtual-Asset-Regulation-Law> (last accessed 11 July 2022).

APPENDIX 1

About the Authors

Kayvan B Sadeghi

Jenner & Block LLP

Kayvan Sadeghi is a partner in Jenner & Block's securities litigation and enforcement practice. He has nearly two decades of experience in complex commercial and securities litigation, investigations and enforcement proceedings.

Mr Sadeghi serves as lead counsel in complex commercial and securities litigation proceedings nationwide and regularly defends clients before the US Department of Justice, the Securities and Exchange Commission, state attorneys general and other government agencies. He also advises corporate boards and special committees in connection with internal investigations and corporate governance matters.

As a prominent member of the blockchain community, Mr Sadeghi represents leading blockchain projects, trading platforms and founders in high-stakes litigation and investigations, and advises numerous clients on crypto and fintech litigation, enforcement and related legal issues. He is a member of the Legal Working Group of the Wall Street Blockchain Alliance and has taught cryptocurrency litigation, enforcement and regulation for a graduate-level fintech course.

Lawrence W McMahon

Jenner & Block LLP

Lawrence McMahon is an associate in the firm's litigation department. Mr McMahon advises clients at all stages of litigation and investigations across a range of industries, with a focus on financial services. Additionally, Mr McMahon advises commodities and derivatives exchanges and market participants on regulatory risk and compliance under the securities and commodities laws, and he

advises international fintech platforms on compliance with US securities and banking regulation. Mr McMahon maintains an active pro bono practice, focusing on civil litigation in state and federal courts.

Mr McMahon earned his JD at Yale Law School, where he was an editor of the *Yale Law Journal*. During law school, he wrote portions of a Supreme Court amicus brief, and he worked on antitrust matters at the Maryland Office of the Attorney General. Previously, he served in the communications bureau of a non-profit organisation, and he taught Middle Eastern history at Georgetown University.

Jenner & Block LLP

353 N Clark Street

Chicago, IL 60654

United States

Tel: +1 312 222 9350

ksadeghi@jenner.com

lmcmahon@jenner.com

<https://jenner.com/>

The Guide to Compliance is the first volume to tackle the compliance side of the enforcement equation in a systematic way. It combines a *tour d'horizon* of the rules in place around the world with specific practical advice for corporations and their counsel, and scan of the horizon in parts two and three. It is part of the GIR technical library that has grown out of the *Practitioner's Guide to Global Investigations* and now includes guides to, among other things, monitorships and sanctions.

Visit globalinvestigationsreview.com
Follow @GIRalerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-868-0