International
Comparative
Legal Guides

Practical cross-border insights into anti-money laundering law

Anti-Money Laundering 2023

Sixth Edition

Contributing Editors:
Stephanie L. Brooker & M. Kendall Day
Gibson, Dunn & Crutcher LLP

sifma
ICLG.com

Industry Chapter

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

Anti-Money Laundering and Cryptocurrency: Legislative Reform and Enforcement


Kevin Roberts

Alix Prentice

Duncan Grieve

Charlotte Glaser

Cadwalader, Wickersham & Taft LLP

Introduction

Anti-money laundering (**AML**) is a top legislative and law enforcement priority in the UK, the U.S., and Europe. The current direction of travel is the culmination of a number of high-profile cases over the last decade, where major financial institutions and other financial market participants have failed to prevent criminal funds from being "laundered" through their accounts. At a political level, there is also a rising awareness within American, British and European governments that repositories of "black cash", concealed and dispersed through offshore financial systems and controlled by hostile state actors such as Russia, have been used in attempts to undermine democratic elections. Such awareness has only been heightened following Moscow's invasion of Ukraine, which has resulted in the imposition of unprecedented sanctions and calls for hyper-vigilance with respect to attempts by Russian state actors and oligarchs to use cryptoasset transactions to evade such sanctions.[1] The current crackdown on money laundering activity is evident in a number of significant active criminal and regulatory enforcement actions worldwide, and in legislative reform efforts aimed at expanding the regulated sphere by forcing participants in other vulnerable markets (particularly art, antiquities and jewellery) to implement AML controls.

The exponential rise of cryptocurrency and its increasing prominence and acceptance by mainstream market participants is further driving the expansion of this enforcement trend. As demand for digital assets, including Bitcoin, Ethereum and others continues, important questions arise regarding how the uptake of cryptocurrency can be made compatible with basic AML control, such as the requirements for regulated market participants to check the identity and legitimate source of funds of their customers. The spectacular failure of FTX highlights the need for comprehensive internal governance controls on crypto platforms, and seems highly likely to result in further targeted enforcement and regulation. This year again ushers in a number of developments in the U.S. and UK, where authorities have begun strengthening the regulatory framework, cracking down on perpetrators and implementing protections for investors.

Cryptocurrency assets such as Bitcoin present unique challenges to the existing regulatory system. Bitcoin can be thought of as "pseudonymous" (rather than truly anonymous) in the sense that the components of Bitcoin, such as addresses, private and public keys, and transactions are all read in text strings (for example, of a public address) that in no way directly link to anyone's personal identity. However, if an address is used on an exchange that implements the kind of basic identity checks used in the mainstream financial sector, such as Know Your Customer (**KYC**), then that address, in theory, can be linked back to a real-world identity. However, even where such resolutions can be applied to trace the identity of cryptocurrency holders, for example, cryptoassets continue to present bad actors with ample opportunity to launder the proceeds of crime.

This chapter explores some of the tensions and potential pitfalls inherent in cryptocurrencies' acceptance within the broader financial system, particularly the regulated financial sector and other regulated asset classes. Businesses are understandably interested in exploring opportunities brought about by broadening acceptance of these assets, but great care needs to be taken to manage the increasing risk of regulatory, and even criminal, sanctions under AML legislation.

Growth in Virtual Currencies and Supporting Infrastructure

In a little over a decade, cryptocurrencies have progressed from an idea many sophisticated investors dismissed as counterculture, to a mainstream financial phenomenon. With over US$41 billion worth of institutional capital flooding into the cryptocurrency space alone,[2] the financial, political and legislative establishment has had to embrace this emerging asset class of virtual currencies. Even with still very little practical use for cryptocurrency, major investors like BlackRock[3] have joined in with heavyweight corporate investors like Tesla, Inc., and large Wall Street banks in the move towards supporting digital assets. In 2021, other financial institutions took steps for more direct contact with the currency, including the Bank of New York Mellon, who joined State Street and a number of other banks in a consortium to publicly back cryptocurrency trading platform Pure Digital. A number of financial institutions are even recommending Bitcoin to retail investors, and many banks are becoming increasingly comfortable offering these services to clients.

Whilst no other similar coin has been offered since the launch of J.P. Morgan's JPM Coin, UK banks continue to keep a close eye on developments and spend R&D budget on keeping up with the trend, including National Westminster Bank Plc (**NatWest**), who last year launched a new digital team to expand the bank's use of blockchain technology within its capital markets business.[4] Even central banks are considering the introduction of digital currencies. Earlier this year, the Bank of England announced that there is likely to be a future need for a "digital pound".[5] However, any intention of further cryptocurrency-related investment continues to come with warnings from regulators and leading bodies about the dangers of the lack of regulation.

The cataclysmic failure of FTX and the collapse of the stablecoin TerraUSD, and its sister cryptocurrency Terra, last year, not only impacted the valuations of crypto assets globally, but also tempered investor appetite and shaken confidence in an

already volatile market. During the last two months of last year (2022), the flow of venture capital investment into cryptocurrency was the lowest it has ever been, and it is expected to continue to slow throughout this year.[6] Such events have also sharpened the focus of many global regulators and accelerated the pace of enforcement action in this area. In March this year, the co-founder and CEO of the parent company of TerraUSD and Terra, Do Kwon, was arrested in Montenegro, which has since received extradition requests from South Korea and the U.S.[7] FTX's founder, Sam Bankman-Fried, decided not to fight an extradition request from the U.S. when he was arrested in the Bahamas at the end of last year, and he is currently awaiting trial on a number of charges linked to the collapse of his cryptocurrency exchange.[8] Similar enforcement action has recently taken place in relation to BitMEX and Binance. Following the arrest of BitMEX's co-founder and CEO, Arthur Hayes pleaded guilty to failing to implement AML controls.[9] Earlier this year, U.S. regulators sought to ban the world's largest crypto trading platform, Binance, for similar conduct.[10] Whilst these investigations are at an early stage, they reveal that many major crypto exchanges had very weak internal controls and, in some cases, appear to have actively evaded regulatory requirements.

The rise of the use of NFTs and the amount of money being spent[11] by buyers has also attracted a great deal of public interest. Whilst NFT transactions linked to money laundering are currently few in number, industry research suggests that such practice does exist,[12] and, given that some estimates put money laundering in cryptocurrency at nearly US$9 billion, the current lack of regulation makes it inevitable that bad actors will try to take advantage of the ease with which it is possible to launder large sums through NFT-linked transactions. The fact that NFTs will be excluded from the UK Financial Conduct Authority's (**FCA**) definition of "qualifying cryptoassets", such that they will not be brought within the remit of the financial promotions rules, gives rise to the question as to how these assets will be regulated.

Crypto mixers present a further challenge in terms of regulation. So-called "CoinJoins" allow users to combine their transactions, allowing coins from different wallets to be shuffled and redistributed, thereby obscuring origination and avoiding detection. Given that a core principle and much of the appeal of crypto is its decentralised nature, designing a regulatory framework around crypto mixers may, for some, defeat the object; for the same reasons, however, they are a potential hotbed for money launderers. In 2021, the founder of Helix, a darknet-based cryptocurrency mixer, pleaded guilty[13] to money laundering charges and admitted that the platform explicitly advertised itself to customers on darknet marketplaces as a way to conceal transactions from law enforcement.

The UK's National Crime Agency (**NCA**) recently called for regulation of crypto mixers.[14] Regulation would place crypto mixers under an obligation to carry out customer checks and audit trails of currencies passing through their platform, as well as allowing law enforcement agencies to properly investigate potentially serious crime, such as state-sponsored crime and terrorism.

Global AML Enforcement and Legislative Reform

Historically, the UK has been one of the more active jurisdictions worldwide in AML enforcement; from the time of the Proceeds of Crime Act 2002 (**POCA**) and antecedent legislation, AML enforcement by the UK authorities has remained active. The passing of the Economic Crime (Transparency and Enforcement) Act 2022 (**ECA 2022**) brings in a number of changes related to the identification of the beneficial ownership of overseas entities and provides regulators with the tools to obtain unexplained wealth orders more easily.

Although, Europe appears to be taking the lead in respect of developing a comprehensive regulatory framework around cryptoassets. In April 2023, the EU Parliament voted to pass the Markets in Crypto-assets (**MiCA**) Regulation which seeks to facilitate the tracing of crypto-transfers and prevent suspicious transactions. In 2021, the EU also announced a significant overhaul of AML enforcement following on from the Sixth AML Directive: the creation of a new EU AML and counter-terrorist financing (**CTF**) authority (the Anti-Money Laundering Agency (**AMLA**)), with extended powers to ensure consistent application of EU AML/CTF rules and supervise selected high-risk financial institutions. AMLA is expected to become operational in 2026.

Across the Atlantic, the Biden administration passed legislation to tighten rules relating to beneficial ownership disclosure to the U.S. Financial Crimes Enforcement Network (**FinCEN**) and ban the use of anonymous shell companies that can be used to obfuscate the identity of a company's ultimate beneficial owner (**UBO**). Following a string of successful pursuits of perpetrators as discussed above, the U.S. is widely expected to continue to usher in a more stringent regulatory environment in the financial sector and vigorously pursue those that fall foul of such regulation. A recent proposal for new legislation, the Digital Asset Anti-Money Laundering Act, which would introduce AML controls and reporting in relation to cryptocurrency transactions, is one such example.[15] The high-profile trial of Sam Bankman-Fried, which is currently due to take place in October this year, will almost certainly drive further legislative reforms and enforcement in the U.S., as well as further afield.

UK AML Enforcement Post-Brexit

Prior to its departure from the EU, the UK was a key player in developing the Europe-wide AML framework through EU legislation in the form of a succession of AML Directives. The existing Fifth AML Directive is already fully implemented in UK law. The UK has not opted into the EU's Sixth AML Directive as the Government considers that the requirements of this Directive are already incorporated within the UK's existing AML legislative framework.

Building on the offence of failure to prevent bribery in the UK Bribery Act 2010, and the UK Government's recent announcement relating to the introduction of a new failure to prevent fraud offence by way of an amendment to its draft Economic Crime and Corporate Transparency Bill (**Economic Crime Bill**), the UK is also actively considering expanding the scope of "failure to prevent" offences in the financial sector. Proposals to amend the Financial Services Bill so that businesses or individuals regulated by the FCA would be held liable for failure to prevent economic crime are currently on hold but, if implemented, would extend not just to money laundering, but also to fraud, false accounting, POCA offences, insider dealing, and providing false or misleading statements. Such a development would have significant ramifications for financial institutions operating in the UK and their employees, particularly senior management; however, it remains to be seen whether it will once again be brought to the fore, given the spotlight on tackling money laundering in the UK.

Over half of the total value of all fines secured by the FCA last year related to failings in financial crime controls. Recent decisions by the FCA indicate that there is little chance of such means of enforcement slowing down. This year, in January alone, the FCA imposed two fines totalling in excess of £11 million for failings by two companies in respect of their AML processes.[16]

In December 2021, NatWest was handed a fine of nearly £270 million after it pleaded guilty to three offences related to breaches of the Money Laundering Regulations 2007 (**MLR 2007**) in a period covering 2011 to 2016.[17] The FCA determined that NatWest failed to conduct risk-sensitive due diligence and ongoing monitoring of its relationships with a UK-incorporated customer for the purposes of preventing money laundering with around £365 million paid into the customer's accounts, of which around £264 million was in cash.

The case is significant as it is the first criminal prosecution under the MLR 2007 by the FCA and the first prosecution under the MLR against a bank, and signals the increasingly tougher approach being taken by the FCA. The fact that the FCA chose to bring proceedings under the MLR rather than the specific AML offences set out in POCA suggests that the FCA identified significant regulatory failures rather than acts of deliberate involvement in money laundering, as was confirmed in the sentencing remarks delivered by Justice Cockerill, who noted in particular that "[w]ithout the Bank – and without the Bank's failures – the money could not be effectively laundered".[18]

For financial institutions and market participants, this prosecution is a timely reminder that regulatory oversights can also potentially invoke criminal liability in the UK. Like NatWest, many corporate entities use automation in relation to customer accounts, and the case demonstrates that automated functions cannot always account for the risk involved in customers acting in bad faith.

The UK tax authority HM Revenue & Customs (**HMRC**) is the supervisory authority for more than 30,000 businesses across the UK under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (**MLRs**). In 2021, it announced a record-breaking fine of £23.8 million on MT Global Ltd., a UK-based money transfer service, for significant breaches of the MLRs.[19]

U.S. AML Enforcement under the Biden Administration

In the U.S., the AML landscape has also seen significant movement as the Biden administration indicates its intentions to ramp up enforcement in this area. The National Defense Authorization Act for Fiscal Year 2021 (**NDAA**) was passed on 1 January 2021 and is the most significant amendment to the AML landscape in a generation since the adoption of the U.S. Patriot Act, and will require extensive implementation by the Treasury Department.

The regulatory and legislative changes together have two principal themes: (i) a conscious effort to evolve AML compliance and the 1970 Bank Secrecy Act and its implementing regulations (collectively, the **BSA**) to make the system more efficient and more effective; and (ii) the adaptation of the BSA to a new generation of threats. The NDAA extends the rules of the BSA to cover other sectors, including the art market; specifically, antiques and art dealers. The bill aims to improve AML efforts by making it harder for purchasers to obscure their identities through offshore entities and shell companies by requiring investors and collectors to identify an UBO. It remains to be seen how these businesses will synchronise these new requirements with the recent acceptance of cryptocurrencies as a form of payment.

On 17 March 2022, it was announced that USAA Federal Savings Bank (**USAA FSB**) would pay a US$140 million civil penalty to the FinCEN and the Office of the Comptroller of the Currency after it found that the USAA FSB had engaged in wilful violations of the BSA.[20] USAA FSB admitted that from 2016 through to 2021, it wilfully failed to implement and maintain an AML programme that met the minimum requirements of the BSA, and was also guilty of failing to ensure that, as its customer base grew, its compliance procedures kept pace.

At the end of last year, the U.S. Securities and Exchange Commission charged the founder of FTX, formerly one of the world's largest crypto exchanges, with fraud, money laundering, bribery and other related offences. At the beginning of this year, the Department of Justice announced that it had arrested the founder of the crypto exchange platform Bitzlato for failing to undertake sufficient KYC of its customers. Around the same time, crypto exchange platform, Coinbase, reached a US$100 million settlement with the New York State Department of Financial Services for AML failings. Such enforcement signifies U.S. regulators' focus on cryptocurrency money launderers and their determination to crack down on such conduct.

In October 2021, Deputy Attorney General Lisa O. Monaco announced the creation of the National Cryptocurrency Enforcement Team (**NCET**),[21] a taskforce to sit under the Criminal Division that will tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services and money laundering infrastructure actors.

Recent European AML Enforcement

In April 2021, ABN Amro was fined €480 million to resolve an investigation by the Dutch Public Prosecution Service (**OM**) into "serious shortcomings" in its AML procedures and other misconduct by its clients in the Netherlands between 2014 and 2020.[22]

The violations were so severe that the OM accused the bank itself of committing money laundering in addition to internal controls failures, such as: incomplete dossiers on high-risk customers; insufficient risk assessments on new clients; and failures to properly report suspicious transactions.

At the end of last year, authorities in Denmark issued its largest ever penalty of €470 million to Danske Bank for AML failings. Danske Bank's Estonia branch was a key enabler of the Azerbaijani Laundromat, a huge money laundering scheme and slush fund that saw billions of dollars run through the bank into offshore companies and paid to high-ranking officials and European politicians.[23] Another investigation, the Russian Laundromat, revealed that US$20 billion to US$80 billion was fraudulently moved out of Russia through a network of global banks that included Danske Bank.

In January 2022, the former chief executive of Swedbank was charged with fraud, market manipulation and the unauthorised disclosure of inside information after an investigation into the large-scale money laundering scandal in Estonia, resulting in a record US$386 million fine.

In March 2023, a number of Members of the European Parliament approved rules proposed in draft legislation relating to the financing provisions of the EU AML/CTF policy, which would include requirements for entities such as crypto asset managers to verify their customers' identity, what they own and who controls the company, as well as to record information relating to money laundering risks to a central register.[24]

FCA Rules and Guidance

While cryptocurrencies were born into a regulatory sandbox to avoid over-regulation and allow for innovation, with the increased investment into this volatile asset class, the FCA assumed responsibility as the AML and CTF supervisor for such firms. Since 9 January 2021, businesses operating in cryptoasset activity in the UK have been required to comply with the MLRs.[25] To assist the FCA in monitoring compliance, firms engaging in cryptoasset activities are required to register with

the FCA before conducting business, with the threat of civil or criminal enforcement. Cryptoasset activities have been broadly defined by the MLRs as:

1. exchanging or arranging to exchange money for cryptoassets or *vice versa*, or one cryptoasset for another;
2. operating machines that use automated processes to exchange cryptoassets for money, or *vice versa*; and
3. providing services to safeguard or administer cryptoassets for customers or private cryptographic keys.[26]

As the official gatekeeper for businesses in/seeking to expand into the cryptoasset space, the FCA's registration requirement allows for confirmation that the company has adequate systems and controls for AML compliance, and its management is fit and proper to carry out such activities. To ensure this is the case, the application for registration requires a plethora of information, including the organisational structure, key individuals involved in the business, beneficial owners, systems and controls (both IT and regulatory in relation to AML/CTF compliance), and any other governance arrangements, including diligence related to client onboarding and ongoing transaction monitoring. The FCA has recently reminded cryptoasset firms and cryptoasset businesses applying for AML registration of its expectations at the point of application. These include having a *bona fide* UK presence and evidencing understanding of and compliance with the MLRs.[27]

While it may be seen as a new asset class to regulate, the FCA has similar expectations in relation to AML monitoring that are in place for more conventional assets. In response to an announcement by the UK Treasury to categorise "qualifying cryptoassets" as Restricted Mass Market Investments, the FCA published a consultation[28] on strengthening the financial promotion rules for high-risk investments (the **FCA Consultation Paper 2022**), including cryptoassets (although excluding NFTs). The FCA Consultation Paper 2022 outlines that firms will therefore only be able to market cryptoasset-related products or services to consumers if they meet the definition of restricted, high-net-worth or certified sophisticated investors.

On 1 February 2023, the UK government published their intention to introduce an exemption in the Financial Promotion Order 2005 (the **Order**) to allow cryptoasset firms registered with the FCA for AML supervision purposes to communicate their own cryptoasset financial promotions to UK customers without breaching the Order, and to shorten the implementation period from six to four months.

The FCA has stated that it will take a risk-based approach to supervision. Therefore, the larger the potential for money laundering and terrorist financing, the more scrutiny a firm will receive and the higher the likelihood for FCA enforcement where misconduct is detected. Components of an effective compliance programme will also follow in the footsteps of conventional wisdom. These include ensuring that the business has policies, controls and procedures that effectively manage money laundering risks proportionate to the size and nature of the business' activities. Additionally, regular assessments of the governance system will need to be conducted, with a specific focus on the impact that a change in the business' operating model may have on its risk profile. With the inherent volatility and requirement for a degree of anonymity imbedded in the basic structure of cryptoassets, businesses will be required to take an even more proactive monitoring role. Some of the requirements, though not exhaustive, highlighted by the FCA include:

- taking appropriate steps to identify and assess the risks of money laundering;
- assess risks related to new technologies prior to launch and take appropriate steps to manage or mitigate such risks;
- maintain policies, systems and controls appropriate for mitigating the risk of the business being used as a vehicle of illicit financial activity;
- undertake adequate due diligence, including employee screening and customer due diligence (both at the onboarding stage and periodically thereafter); and
- ensure ongoing monitoring of all customers and transactions to make sure that they are consistent with the business' knowledge of the client's risk profile.

As above, the FCA's requirements from firms engaging in cryptoassets, for a large part, mirror the expectation for the broader market. It is therefore worthwhile to consider what the FCA has indicated would be effective systems and controls through enforcement actions and guidance.

UK Enforcement

Recent FCA investment in enforcement capabilities

In 2018, the UK Government established a Cryptoassets Taskforce, comprising representatives from HM Treasury, the Bank of England and the FCA (the **Taskforce**). The Taskforce's report, which was published later that year, sought to set out, amongst other things, the UK's regulatory approach to cryptoassets.[29] In the same year, the FCA published a notice on its ScamSmart webpage containing details about cryptoasset investment scams and how to identify and avoid them.[30] In January 2020, following the publication of the Taskforce's report, the FCA became the AML/CTF supervisor for cryptoasset firms. Following its announcement requiring firms to register for FCA approval as a registered cryptoasset service provider, over 100 firms applied and only a third were granted a licence allowing them to operate in the UK. Just over half of the original applicants withdrew their applications or were rejected, reportedly resulting in those firms looking to other jurisdictions that are seen as more crypto-friendly; the stringent process mandated by the FCA, however, maintains the UK's position as a leading cryptoasset market.[31] Pursuant to the MLRs (as amended), it is a criminal offence for a cryptoasset firm to operate without being registered with the FCA.

Since the FCA's assumption of the role of AML/CTF supervisor of cryptoasset firms, it has undertaken a number of enforcement actions in this area. It banned the sale of derivatives based on cryptocurrencies to retail investors, stating that: "[S]ignificant price volatility, combined with the inherent difficulties of valuing cryptoassets reliably, places retail consumers at a high risk of suffering losses from trading crypto-derivatives. We have evidence of this happening on a significant scale. The ban provides an appropriate level of protection."[32] In 2021, the FCA issued a statement warning against an unregistered firm that had been offering "trading services in digital currencies".[33] In the same month, it was reported that the FCA had opened 52 investigations into cryptocurrency businesses in the previous year.[34] Last month, as part of a joint operation with West Yorkshire Police's Digital Intelligence and Investigation Unit, the FCA entered and inspected several sites in the UK which were suspected of hosting illegally operated crypto ATMs.[35]

The FCA continues to comment in relatively strong terms on the volatile nature of cryptoassets, stating that "if consumers invest in these types of product, they should be prepared to lose all their money",[36] while reinforcing its views in the FCA Consultation Paper 2022. Given the infancy of its regulatory remit in this field, it remains to be seen how, and to what extent, the FCA will enforce its powers in respect of non-compliant cryptoasset firms.

FCA Enforcement Powers

There are a number of regulatory tools available to the FCA, of which enforcement is one. The FCA will refer an individual or firm to its Enforcement Division and commence an investigation into that individual or firm in circumstances where it considers that there has been potential serious misconduct. While the FCA states that not all harm is caused by serious misconduct, it notes that "serious misconduct will likely cause harm to market integrity, confidence in the financial system or cause harm to consumers".[37] When selecting cases to investigate, the FCA's *Enforcement Guide* states that it will assess whether such an investigation is likely to further its aims and objectives by considering the following:

1. any available supporting evidence and the proportionality and impact of opening an investigation;
2. what purpose or goal would be served if the FCA were to end up taking enforcement action in the case; and
3. relevant factors to assess whether the purposes of enforcement action are likely to be met.[38]

In the event that the FCA decides to take action against an individual or firm, it has an extensive range of civil, criminal and regulatory enforcement powers at its disposal.[39]

The FCA employs its criminal enforcement powers far less frequently than its civil and regulatory enforcement powers. Indeed, in its Annual Report for 2020/2021, it recorded that of the 147 outcomes it had secured using its enforcement powers, only three related to criminal disposals.[40]

Enforcement Relating to Other UK Prosecuting Agencies

As well as the FCA, other UK enforcement agencies are beginning to focus their efforts on cryptocurrencies being used as a vehicle for fraud. While at present it appears that the number of cases prosecuted by the Crown Prosecution Service (**CPS**) involving cryptocurrencies is small in comparison to the total number of prosecutions brought by the CPS, it is anticipated that the number of prosecutions involving cryptocurrencies will continue to increase. Indeed, the CPS recently stated that 86% of reported fraud "is now estimated to be cyber enabled, fuelled by advances in technology". The CPS released such data as it launched its first Economic Crime Strategy (the **Strategy**) in March 2021, recognising economic crime "as a growing area of criminality". The Strategy sets out the CPS' plan to tackle economic crime over the next five years.[41] In January of this year, four offenders were sentenced to a total of 15 years imprisonment for laundering Bitcoin and other cryptocurrency estimated to be worth tens of millions of pounds from a cryptocurrency exchange.[42]

Similarly, in light of the increasing number of high-profile endorsements of cryptoassets which are likely to continue to drive interest in and demand for such assets, the NCA and Serious Fraud Office are likely to see an increase in the number of its investigations involving cryptoassets.

The ECA 2022 introduces a new register of overseas entities which includes information such as the beneficial owners of all property bought in England and Wales. It also reduces the financial liability of pursuing a case in respect of unexplained wealth orders for the relevant investigating authority, provided that the agency can demonstrate that it behaved reasonably and honestly. The ECA 2022 provides agencies with the tools they need to confiscate and seize assets, and not just investigate them. The draft Economic Crime Bill will also deliver additional powers to seize and recover suspected criminal cryptoassets and strengthen AML powers, enabling better information sharing in respect of AML and related crimes.[43]

In February 2023, HM Treasury published a consultation and call for evidence on a "Future Financial Services Regulatory Regime for Cryptoassets". Among the proposals being made is an expansion of the list of "specified investments" in Part III of the Financial Services and Markets Act 2000 (**FSMA**) (Regulated Activities) Order 2001 to include "cryptoassets".[44] That means that the conduct of certain activities in or into the UK by way of business would require direct authorisation under FSMA. That would in turn mean that firms undertaking regulated crypto activities will be subject to the full FSMA financial crime regime, including money laundering, bribery and corruption, sanctions and fraud provisions.

Summary and Key Takeaways

- Cryptocurrency and, more generally, cryptoassets constitute an increasingly important growth area, but it is fundamental that companies invest in robust internal controls to stay on the right side of UK regulators.
- AML will be the big focus for regulators and criminal enforcement over the next few years; in particular, leading financial markets such as the UK to further develop and strengthen the regulatory framework for investing in cryptoassets.
- Companies should be prepared for enhanced cross-border AML/CTF scrutiny.
- Emerging cryptocurrency businesses have a number of inherent vulnerabilities that make them a ripe target for regulatory enforcement: technical challenges in managing the pseudonymous nature of cryptoassets to conform with AML KYC requirements; underinvestment in risk functions (a blind spot shared with other "disruptor" business models); and others.
- Cryptocurrency companies must obtain the right advice to design their internal controls and to assist with their external communications with regulators and law enforcement.

The days of cryptocurrency operating in the Wild West are over. The sheriff has arrived in town, and times are changing.

Endnotes

1. https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf.
2. https://www.institutionalinvestor.com/article/b20qb0dsfp3m4l/VCs-Poured-41-Billion-Into-Crypto-in-the-Past-18-Months-Is-There-Any-Hope-for-a-Profit.
3. https://www.forbes.com/sites/anthonytellez/2021/08/19/blackrock-joins-fidelity-and-vanguard-as-a-bitcoin-mining-investor/?sh=5c6fe4ee2738.
4. https://www.cityam.com/the-time-is-now-right-natwest-creates-new-digital-team-in-blockchain-push/.
5. https://www.bankofengland.co.uk/the-digital-pound.
6. https://www.forbes.com/sites/digital-assets/2023/03/01/blockchain-projects-still-stuck-in-venture-capitals-crypto-winter/?sh=3e9d957e45a8.
7. https://www.bbc.co.uk/news/technology-65058533.
8. https://www.bloomberg.com/news/articles/2023-01-03/bankman-fried-s-not-guilty-plea-sets-up-path-to-fraud-trial?leadSource=uverify%20wall.
9. https://www.reuters.com/legal/government/crypto-exchange-bitmex-co-founder-gets-6-months-house-arrest-us-charges-2022-05-23/.
10. https://www.bbc.co.uk/news/business-65091480.
11. https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis%20NFT%20Market%20Report.pdf.
12. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

13. https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.
14. https://www.ft.com/content/c6df2b68-a244-4560-9911-88cc1fa61576.
15. https://www.warren.senate.gov/imo/media/doc/Crypto%20National%20Security%20One-Pager%20draft_12.13.22.pdf.
16. https://www.fca.org.uk/news/press-releases/fca-fines-guaranty-trust-bank-uk-limited-ps76-million-further-failures-its-anti-money-laundering; https://www.fca.org.uk/news/press-releases/fca-penalises-al-rayan-bank-plc-anti-money-laundering-failures.
17. https://www.fca.org.uk/news/press-releases/fca-starts-criminal-proceedings-against-natwest-plc.
18. https://www.judiciary.uk/wp-content/uploads/2022/07/FCA-v-Natwest-Sentencing-remarks-131221.pdf.
19. https://www.gov.uk/government/news/hmrc-issues-record-238m-fine-for-money-laundering-breaches.
20. https://www.fincen.gov/news/news-releases/fincen-announces-140-million-civil-money-penalty-against-usaa-federal-savings.
21. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.
22. https://www.prosecutionservice.nl/latest/news/2021/04/19/abn-amro-pays-eur-480-million-on-account-of-serious-shortcomings-in-money-laundering-prevention.
23. https://www.euronews.com/2022/12/14/danske-bank-fined-470m-over-international-money-laundering-scandal.
24. https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing.
25. Regulation 14A of the MLRs defines cryptoasset activities as: (1) exchanging or arranging to exchange cryptoassets for money or one type of cryptoasset for another; (2) operating a machine such as a crypto ATM that uses automated processes to exchange cryptoassets into money, or *vice versa*; and (3) providing custodian services for customers' cryptoassets or private cryptographic keys.
26. For further information on the types of cryptoassets that fall within the FCA's regulatory remit, see Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3, https://www.fca.org.uk/publication/policy/ps19-22.pdf.
27. FN-FCA Statement 06.02.2023.
28. https://www.fca.org.uk/publications/consultation-papers/cp22-2-strengthening-our-financial-promotion-rules-high-risk-investments-includingcryptoassets.
29. https://www.gov.uk/government/publications/cryptoassets-taskforce.
30. https://www.fca.org.uk/scamsmart/cryptoasset-investment-scams.
31. https://www.ft.com/content/e2294ba4-3249-4272-91c4-0aee44e3368e.
32. https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivatives-retail-consumers.
33. https://www.fca.org.uk/news/warnings/dalsari.
34. The FCA's year end is 30 June. This information was released by the FCA following a Freedom of Information Request by Reynolds Porter Chamberlain LLP.
35. https://www.fca.org.uk/news/press-releases/fca-takes-action-against-unregistered-crypto-atm-operators-leeds.
36. https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets#:~:text=If%20consumers%20invest%20in%20these.
37. https://www.fca.org.uk/about/enforcement/investigation-opening-criteria.
38. Section 2.2.8.
39. https://www.fca.org.uk/about/enforcement.
40. https://www.fca.org.uk/data/enforcement-data-annual-report-2020-21.
41. https://www.cps.gov.uk/cps/news/cps-launches-ambitious-plan-combat-economic-crime#:~:text=86%25%20of-%20reported%20fraud%20is,fuelled%20by%20advances-%20in%20technology.&text=Huge%20increases%20in-%20the%20number,vulnerable%20to%20computer%20service%20fraud.
42. https://www.cps.gov.uk/cps/news/sentence-update-fraudsters-sentenced-ps21m-loss-cryptocurrency.
43. https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-economic-crime-and-corporate-transparency-bill-overarching.
44. "Cryptoassets" are defined in the Financial Services and Markets Bill as being: "Any cryptographically secured digital representation of value or contractual rights that: (a) can be transferred, stored or traded electronically; and (b) that uses technology supporting the recording or storage of data (which may include distributed ledger technology)."

Kevin Roberts is a partner in Cadwalader's White Collar Defense and Investigations Group, resident in the London office. Specialising in regulatory compliance and investigations and white-collar crime, Kevin's practice ranges from regulatory matters dealt with by the FCA, Medicines and Healthcare Products Regulatory Agency, and the Health and Safety Executive, to prosecutions brought by the Serious Fraud Office. Kevin advises corporations and individuals on: money laundering compliance and investigations; anti-corruption and regulatory compliance; asset-tracing and recovery; tax investigations; and fraud. As part of his global practice, Kevin advises clients on mutual assistance requests and extradition. He also counsels them on Parliamentary Select Committee appearances.

Cadwalader, Wickersham & Taft LLP
100 Bishopsgate
London, EC2N 4AG
United Kingdom

Tel: +44 20 7170 8590
Email: kevin.roberts@cwt.com
URL: www.cadwalader.com

Alix Prentice is a partner in Cadwalader's Financial Services Group, resident in the London office. Alix advises: banks; broker-dealers; fund managers; family offices; and intermediaries on compliance with conduct of business and prudential regulations issued by the FCA and Prudential Regulation Authority (**PRA**), primarily in the areas of funds and structured finance. Alix also provides support to Cadwalader's White Collar Defense and Investigations Group on investigations involving the FCA and PRA.

Cadwalader, Wickersham & Taft LLP
100 Bishopsgate
London, EC2N 4AG
United Kingdom

Tel: +44 20 7170 8710
Email: alix.prentice@cwt.com
URL: www.cadwalader.com

Duncan Grieve is an associate in Cadwalader's White Collar Defense and Investigations Group, resident in the London office. Duncan advises a range of organisations, including multinationals, both on internal corporate investigations and during investigation or prosecution, by regulatory bodies including the SFO, the FCA, the U.S. Department of Justice and the U.S. Securities and Exchange Commission. He has deep experience in dealing with international investigations involving issues in foreign jurisdictions, including Brazil, Lusophone Africa and Portugal, as well as Canada, China, the Czech Republic, India, Japan, Romania and Russia. Duncan also represents individuals subject to internal, regulatory and criminal investigation.

Cadwalader, Wickersham & Taft LLP
100 Bishopsgate
London, EC2N 4AG
United Kingdom

Tel: +44 20 7170 8579
Email: duncan.grieve@cwt.com
URL: www.cadwalader.com

Charlotte Glaser is an associate in Cadwalader's White Collar Defense and Investigations Group, resident in the London office. Charlotte has advised clients involved in multijurisdictional bribery and corruption, complex fraud and money laundering investigations commenced by a number of enforcement agencies, including the SFO and HMRC. She has experience representing individuals in relation to contentious regulatory matters; in particular, investigations conducted by the FCA, the CMA and the Brazilian competition regulator, the Administrative Council for Economic Defense (**CADE**). Charlotte also has experience advising multinational corporations in relation to internal investigations.

Cadwalader, Wickersham & Taft LLP
100 Bishopsgate
London, EC2N 4AG
United Kingdom

Tel: +44 20 7170 8628
Email: charlotte.glaser@cwt.com
URL: www.cadwalader.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group