# Anti-Money Laundering Bulletin
# Regulatory News Update
# Winter 2022

UK financial crime: What to expect in 2022

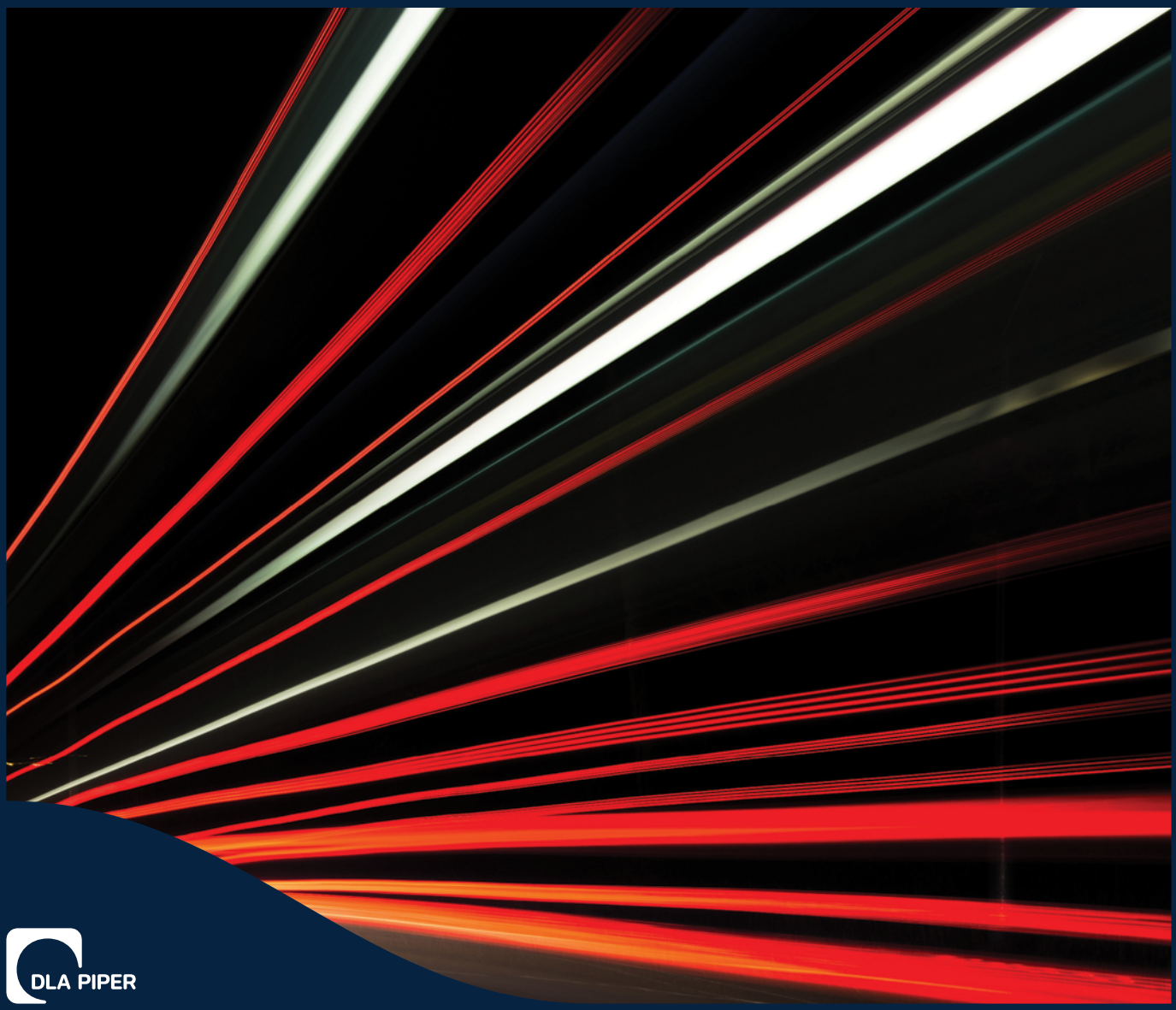
Overview of the FCA's recent AML supervisory activity

First FCA criminal prosecution for breach of AML rules

EBA consults on new remote customer onboarding guidelines

Federal crypto enforcement team launched at US Department of Justice

FATF publishes updated guidance on AML requirements for Virtual Assets and Virtual Asset Service Providers



DLA PIPER

# Introduction

DLA Piper's Financial Services Regulatory team welcomes you to the January 2022 edition of our Anti-Money Laundering (AML) Bulletin. In this issue, we provide updates on AML developments in the UK, the EU and internationally.

In the UK, we provide insights on the supervisory activity of the Financial Conduct Authority in the area of AML for the period 2019-2020. In 2021, the FCA undertook its first criminal prosecution for breaches of the money laundering regulatory requirements against a UK bank – signalling an increasingly tougher approach regarding AML failings in the banking sector. Looking at the year ahead, we also discuss the key areas relating to financial crime more broadly that the UK government is expected to focus on in the course of 2022.

In the EU, the European Banking Authority has published draft guidelines on the use of remote customer onboarding solutions by financial services firms. The guidelines aim to streamline the approach by EU supervisory authorities by putting in place shared standards for market participants and regulators across the EU.

Digital assets remain a key area of focus, with the US Department of Justice launching a cryptocurrency enforcement team with responsibility for investigating and prosecuting criminal misuses of cryptocurrency. On an international level, the Financial Action Task Force has published updated guidance on AML requirements for virtual assets and virtual asset service providers, which clarifies important questions for the industry in evolving areas, such as stablecoins, peer-to-peer transactions, non-fungible tokens (NFTs) and decentralised finance (DeFi).

We hope you find this update helpful. Your feedback is important to us, so if you have any comments or would like any further information, please contact one of the people listed at the end of the bulletin.

# UK financial crime: What to expect in 2022

2022 is likely to see UK regulators continue to build on a number of regulatory initiatives and priorities they have been working on over the past few years.

In particular, there are four key areas to focus on:

- UK's Economic Crime Plan for 2019-2022
- Fraud
- Analysing feedback and implementing legislative initiatives following the 2021 consultations on changes to the money laundering regime
- Operational resilience

Some of these are areas the FCA and PRA have been focused on for a number of years – however, 2020-21 understandably saw the regulators divert resources to cover the financial impacts of the COVID-19 pandemic. It is, therefore, likely that UK regulators may be keen to push matters forward in 2022 as the UK returns to normality.

Taking each of the areas in turn:

## UK Economic Crime Plan 2019-2022

The UK Economic Crime Plan 2019-2022 (Plan) was published in July 2019 and sets out the government's response to a range of economic crimes that affect the UK, including money laundering, bribery, fraud and market abuse. The government anticipates that the response to these issues will involve both private and public sectors working together to fight economic crime affecting the UK.

Clearly, COVID-19 and its impact on economic crime was not expected when the Plan was published in July 2019. The pandemic has brought increased financial crime threats and challenges, with criminal actors taking advantage of the disruption caused to maximise opportunities to commit various forms of economic crime. While the government did, earlier in 2021 in its Statement of Progress, point to some achievements by the public and private sectors in delivering against the seven strategic priority areas set out in the Plan, it's clear that there is a lot to do in executing the rest of the plan through to the end of 2022. These include:

- continuing development of the National Economic Crime Centre (NECC) as a public-private hub to disrupt and prevent economic crime through use of collective resources – throughout 2022;
- cultivating the public private "cells" established in October 2021 to look at priority threat areas including risk management of unregistered money service businesses (MSBs) and understanding of over the counter cryptoasset brokers;
- building on the 2020-2021 pilot to deliver innovative approaches to reducing criminals' ability to exploit online infrastructure and communication techniques to enable or commit frauds using National Cyber Security Centre (NCSC) capabilities (by March 2022);
- enhancing the National Crime Agency's data and intelligence capabilities to respond to online threats, identify links to organised crime and support the Fraud Action Plan (March 2022); and
- creating a new public engagement hub in the NECC to bring together the existing work to educate the public and better understand what interventions work best (March 2022).

## Fraud

National Cyber Crime Force

The government intends to scope a pilot for the new National Cyber Crime Force by March 2022.

It is expected that this force will aim to deliver more fraud investigations and disruptions, and a more coordinated response to fraud across law enforcement. This will also deliver more pilot dedicated fraud investigation teams in four regional organised crime units (ROCUs) throughout England and Wales (currently there are ten ROCUs across England and Wales which have a range of specialist policing capabilities – only one of which is a dedicated cybersecurity team).

It is hoped that this will increase the UK's capabilities in combating cybercrime.

Joint Fraud Taskforce

The Joint Fraud Taskforce was relaunched in October 2021 and during 2022 this organisation will commit industry leaders to work with government to deliver new, innovative projects with the ultimate aim of reducing the growing threat and protecting the public (particularly in retail banking, telecommunications and accountancy).

New initiatives include: a pilot dynamic direct debit system that would introduce a banking authorisation step into applications for new telecommunications contracts (including mobile phone contracts) that have been applied for fraudulently or used for fraudulent purposes; a cross sector data breach plan to protect customers who have been subject to a data breach from becoming victims of fraud, and leveraging new technology to tackle the fraudulent practice of sending fake company text messages – known as "smishing."

The taskforce will include leaders from across government, the private sector, regulators, law enforcement and victim representatives.

Fraud Action Plan Framework

Development of a Fraud Action Plan by the government, private sector and law enforcement – due after the Chancellor's 2021 Spending Review (expected Q4 2021).

SFO Control Strategy

Improve the coordinated response to and dissemination of Serious Fraud Office's (SFO) reporting and analysis in key threat areas through the SFO's newly developed SFO Control Strategy.

## Analysing feedback from the 2021 consultations on changes to the money laundering regime

2022 will see the government continue to analyse the feedback they received from the 2021 reviews on the adequacy of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) and Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017 (OPBAS regulations).

HM Treasury's report is due no later than 26 June 2022. The review offers the opportunity to ensure the UK's AML regime responds to the nation's particular circumstances and risks, is as effective as possible in preventing and detecting illicit finance, and supports the UK's competitiveness by ensuring it's a clean and safe place to do business.

The consultation focused on three key themes:

- overall effectiveness of the MLR/OPBAS regimes and their extent (ie the sectors in scope as relevant entities)
- whether key elements of the current regulations are operating as intended
- the structure of the supervisory regime including the work of OPBAS to improve effectiveness and consistency of Professional Body Supervisors (PBS) supervision

UK regulators have reiterated their commitment to maintaining efforts to uphold FATF international standards, in particular the application of a risk-based approach to applying our regulatory framework.

While the review considers important areas of overlap with the Proceeds of Crime Act 2002 (POCA) – for example, the feedback system of high-value intelligence to law enforcement resulting from activity under the MLRs, and the role of AML/CFT supervisors in the Suspicious Activity Reporting (SAR) regime, it does not aim to recommend significant changes to the operation of POCA or other legislation.

As a result of the review, the government will be laying forth secondary legislation in Spring 2022 (SI 2022) which is likely to:

- exclude Account Information Service Providers (AISPs) from certain requirements under the MLRs;
- provide more flexible information gathering powers for the FCA to use in relation to Annex I financial institutions (which include for example commercial lenders);
- expand regulation 30A of the MLRs to introduce an ongoing requirement to report discrepancies in beneficial ownership information;
- amend the MLRs/OPBAS Regulations to meet latest recommendations by the Financial Action Task Force (FATF) in relation to proliferation financing risk assessments; and
- consider any additional changes required to deal with AML risk associated with crypto assets.

In addition, in the coming months we also anticipate the government to consider further legislative changes to the POCA to provide law enforcement with stronger powers and the ongoing progression of SARs IT reform.

## Operational resilience

The past year has seen an array of regulatory guidelines and requirements relating to operational resilience and outsourcing.

Most notably in March 2021, the FCA published its long-awaited operational resilience Policy Statement. It sets out several far-reaching requirements, including, for example:

- an emphasis on "impact tolerances" (the maximum tolerable amount of disruption to an important business service)
- requiring the use of mapping exercises to prepare "impact tolerances" for important business services
- the testing of such "impact tolerances" through disruption scenarios

The FCA will continue to assess firms' progress in implementing these new requirements and identify areas for improvement, and that it will, from 31 March 2022 to 31 March 2025, assess firms' ability to remain within their "impact tolerances." We expect the FCA to re-engage with operational resilience as a priority area in the coming years.

# Overview of the FCA's recent AML supervisory activity

On 19 November 2021, HM Treasury published its Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Supervision Report 2019-20 (Report). The Report looks at the performance of AML/CTF supervisors, including the Financial Conduct Authority (FCA), during 2019 – 2020 based on supervisory enforcement data.

The FCA is responsible for the supervision of c. 22,000 financial services firms. Following its sector risk assessments, the FCA found that the retail banking, wholesale banking and wealth management sectors are the ones which are most vulnerable to financial crime and pose increased money laundering risk.

The FCA's supervisory approach involves as a general rule the following three key proactive programme categories (although a different approach may be taken for firms under enhanced supervision or to respond to specific events or crystallised risks):

- **The Systematic Anti Money Laundering Programme** – covering the 14 largest retail and investment banks active in the UK, who are subject to stricter AML/CTF supervision. In light of the increased risk these institutions present, the FCA's engagement with them is continuous and each has a dedicated supervision team.
- **The Proactive Money Laundering Programme** – focusing primarily on smaller firms that are considered to be higher risk. This covers approximately 30 firms per year.
- **The Risk Assurance Programme** – covering the rest of the firms which are supervised by the FCA.

Since January 2020, the FCA has been responsible for the supervision of certain cryptoasset business for compliance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs). Under the new rules, in-scope cryptoasset firms are required to register with the FCA for AML supervision. On 16 December 2020, the FCA put in place the Temporary Registration Regime for cryptoasset businesses to allow firms that were trading prior to 10 January 2020, and which had submitted registration applications, to continue trading pending assessment of their applications. This temporary regime has been extended until 31 March 2022. During this assessment process, a significant number of firms were found that had failed to meet the required standards under the MLRs, which led to firms withdrawing their applications or being refused registration.

During the reporting period concerned, the FCA undertook 147 Desk-Based Reviews (DBRs) in total and 30 onsite visits focusing primarily on firms that were considered as high risk. As a whole, approximately 0.8% of the firms under FCA supervision was subject to either a DBR or an onsite visit (marking a slight increase compared to 2018-19). According to the FCA, 33% of the firms subject to a DBR and 47% of firms visited were considered as "generally compliant." It was reported that 6% of firms subject to a DBR were classed as non-compliant and 50% of firms visited were non-compliant with the applicable requirements. Common breaches identified by the FCA included inadequate customer due diligence (CDD) and enhanced due diligence (EDD), resulting in poor identification and monitoring of high-risk customers; lack of, or inadequate, firmwide risk assessments; and inadequate screening of employees through record retention and electronic checks.

Firms that were found non-compliant put in place remediation plans to address their specific deficiencies. The FCA took formal action against firms with significant failings (approximately 6% of firms reviewed and approximately 50% of the firms visited). Formal action can involve appointing a skilled person, imposing restrictions on business activities or financial penalties.

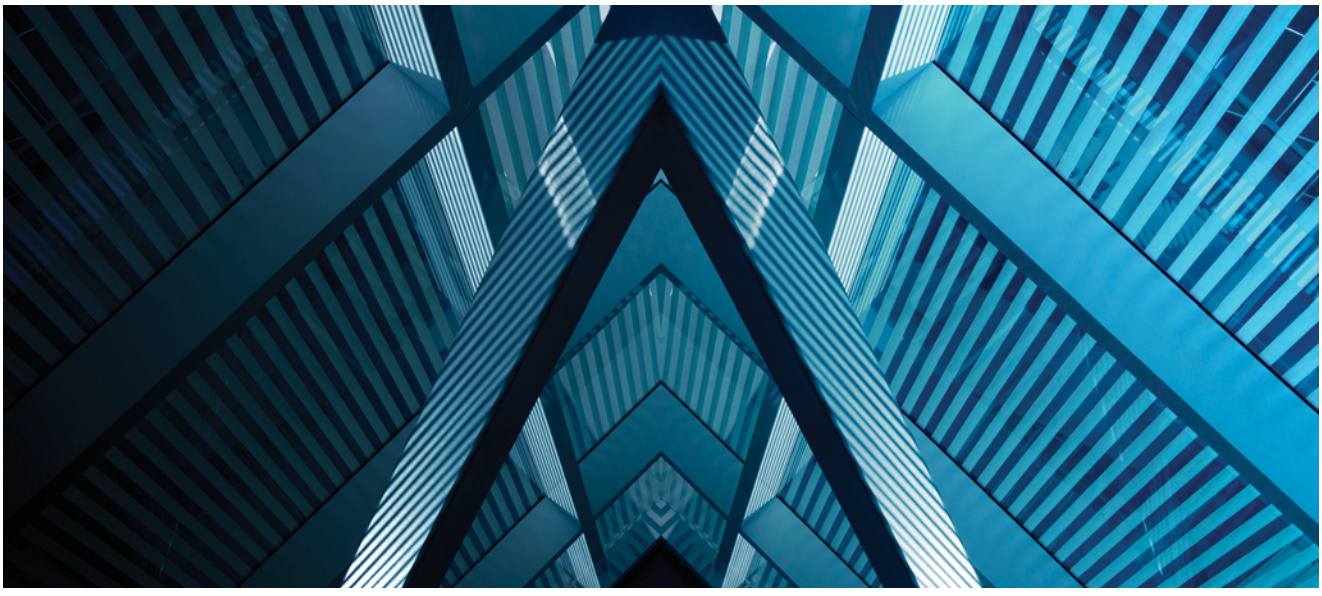
# First FCA criminal prosecution for breach of AML rules

7 October 2021, National Westminster Bank Plc (NatWest) pleaded guilty to criminal charges brought by the Financial Conduct Authority (FCA) under the Money Laundering Regulations 2007 (MLR 2007). This marks the first criminal prosecution by the FCA concerning AML failings by a firm. No individuals within the bank have been charged as part of these proceedings.

The case involved failings to put in place adequate anti-money laundering systems and controls to prevent money laundering in relation to a specific customer account. In particular, the failings concerned deposits made by a jewellery and gold dealing business.
In the course of three years, the customer deposited GBP365 million, including GBP264 million in cash (even though the original predictions were for a GBP15 million turnover). It was found that, even though the bank did undertake initial customer due diligence checks, it did not perform adequate ongoing monitoring or conduct enhanced customer due diligence (EDD) in the course of the relationship.

This is a reminder that breach of certain regulatory requirements, including AML, is a criminal offence which may lead to criminal action by the FCA, in addition to disciplinary measures, if the FCA chooses to take that route (noting that it may not necessarily involve prosecution of individuals).

The case also signals the increasingly tougher approach taken by the FCA in the area of AML, particularly in relation to the banking sector. Earlier in 2021, the FCA published a "Dear CEO" letter concerning continued failings identified in retail banks' AML frameworks. According to the letter, UK banks were requested to have completed a gap analysis against the common failings identified by 17 September 2021 and expected to work thereafter promptly to close any gaps. Banks are strongly advised to be prepared to demonstrate the steps they have taken in response to the letter in any future engagement with the regulator.



# EBA consults on new remote customer onboarding guidelines

On 10 December 2021, the European Banking Authority (EBA) launched a public consultation on its draft Guidelines on the use of remote customer onboarding solutions. These Guidelines have been developed in line with the European Commission's Digital Finance Strategy 2020. This consultation runs until 10 March 2022.

The Guidelines set out the prevailing understanding by competent authorities of the steps financial sector firms should take to ensure safe and adequate remote customer onboarding practices in line with anti-money laundering and countering the financing of terrorism (AML/CFT) legislation and the EU's data protection framework. The intention is for the Guidelines to apply to all financial sector operators that are within the scope of the Anti-money Laundering Directive (AMLD).

Financial service organisations are experiencing high demand for remote customer onboarding solutions. This trend has been accelerated by travel restrictions due to the COVID-19 pandemic. Therefore, the EBA wishes to provide competent authorities and financial sector firms with in-depth knowledge of the various new remote solutions, in order for them to leverage the opportunities on offer. Moreover, competent authorities and financial sector firms should understand how to use remote solutions responsibly, being cognisant of AML/CFT risks arising from the use of such tools.

Therefore, the draft Guidelines set out shared EU standards on the development and implementation of safe, risk-assessed customer due diligence policies and processes in the remote customer onboarding context. They also set out the steps financial service operators should take to comply effectively with their AML/CFT obligations, when choosing remote customer onboarding tools and when assessing the adequacy and reliability of such tools:

Key takeaways of the Guidelines include:

- **Compliance and reporting obligations:** the Guidelines operate on a comply or explain basis. As such, competent authorities must make every effort to comply with the Guidelines. If a competent authority does not comply, it must report its reasons for non-compliance to the EBA.
- **Initial policies and procedures:** the Guidelines set out policies and procedures relating to remote customer onboarding, including minimum requirements that such policies should contain. This section also provides key objectives for governance and management of financial operators, as well as requirements for pre-onboarding impact assessments.
- **Acquisition of information:** the Guidelines set out key requirements when acquiring information, including the need to identify natural and legal entities, ascertain the nature and business purpose of the client and ensure any documents/records used are accurate and authentic.
- **Outsourcing:** the Guidelines set out minimum requirements to be met by a financial sector operator when outsourcing its obligations.

# Federal crypto enforcement team launched at US Department of Justice

The US Department of Justice (DOJ) announced on 6 October 2021 the creation of a National Cryptocurrency Enforcement Team (NCET) with responsibility for investigating and prosecuting criminal misuses of cryptocurrency.

Under the supervision of Assistant Attorney General Kenneth Polite, the new team will focus on crimes committed by virtual currency exchanges, mixing and tumbling services, and the leaders of money laundering operations. NCET will draw on the resources of the DOJ's Criminal Division's Money Laundering and Asset Recovery Section, Computer Crime and Intellectual Property Section and other sections, with experts detailed from US Attorneys' Offices. The team will also assist in tracing and recovering assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups.

In announcing the launch of the new initiative, Deputy Attorney General Lisa Monaco said NCET will augment the DOJ's "capacity to dismantle the financial entities that enable criminal actors to flourish — and quite frankly to profit — from abusing cryptocurrency platforms," adding, "As the technology advances, so too must the Department evolve with it so that we're poised to root out abuse on these platforms and ensure user confidence in these systems." The DOJ said that NCET will also play a critical support role for international, federal, state, local, tribal and territorial law enforcement authorities grappling with new technologies and new forms of criminal tradecraft.

# FATF publishes updated guidance on AML requirements for Virtual Assets and Virtual Asset Service Providers

On 28 October 2021 the (FATF) published its updated guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs). The guidance aims to help VASPs and their supervisors understand the relevant anti-money laundering and counter-terrorist financing (AML/CTF) requirements under FATF's standards (Standards). It provides important clarifications in relation to evolving areas, such as stablecoins, peer-to-peer (P2P) transactions, non-fungible tokens (NFTs) and decentralised finance (DeFi), among other things.

The updates concern the following main areas:

- clarification of the definitions of virtual assets and VASPs
- guidance on how the FATF Standards apply to stablecoins
- additional guidance on the risks and the tools available to regulators to address the money laundering and terrorist financing (ML/TF) risks associated with peer-to-peer transactions
- updated guidance on the licensing and registration requirements for VASPs
- additional guidance on the implementation of the "travel rule"
- principles of information-sharing and cooperation among VASP supervisory authorities

Some key takeaways are summarised below.

## Non-Fungible Tokens

NFTs are digital assets that are unique, rather than interchangeable, and are typically used as collectibles and not for payment or investment purposes. The Guidance clarifies that NFTs do not generally fall within the FATF definition of Virtual Assets, unless they are intended to be used as payment or investment instruments.

## Stablecoins

The Guidance reaffirms that stablecoins are generally covered by the FATF Standards, either as Virtual Assets or financial instruments. According to FATF, the potential for mass adoption is a key factor that regulators should take into account when assessing the ML/TF risks involved in stablecoins.

## Peer-to-peer transactions

P2P transactions are defined as virtual asset transfers undertaken without the use or involvement of a VASP or other obliged entity. For example, these include Virtual Asset transfers between two unhosted wallets whose users are acting on their own behalf.

The Guidance clarifies that P2P transactions generally fall outside the scope of the FATF Standards, which as a rule place obligations on intermediaries rather than individuals. There is, therefore, an increased risk that P2P transactions could be used for illicit activities by bypassing the FATF Standards. The Guidance does not change this position, but does state that regulatory authorities should monitor P2P transactions and determine the types of arrangements that present increased ML/TF risks, which may require additional mitigating measures.

## Decentralised Finance

This is a key area of focus and market participants should be aware that most "decentralised" arrangements are still likely to be caught by the AML rules, particularly where there is an identifiable entity with significant control or influence over a particular project.

Decentralised technology solutions, often referred to as decentralised finance (DeFi), may be used to facilitate the exchange or transfer of digital assets. Even though they often use a decentralised ledger, there is typically a central party with some level of involvement or control over the operations – for example, such party creates and launches the virtual assets, develops the functions of the application and the user interfaces for accounts holding an administrative "key" or is responsible for collecting fees.

According to the Guidance, the software program constituting the DeFi application is not a VASP under the FATF Standards, because the rules do not apply to the underlying technology. That being said, however, *creators, owners and operators* or some other persons who maintain control or sufficient influence over the DeFi application may be caught by the FATF Standards as VASPs, in cases where they are providing or *actively facilitating* VASP services (notwithstanding the fact that some aspects of the process may be automated or operated via smart contracts).

The Guidance encourages regulators to take a broad approach in determining whether there are identifiable legal or natural persons providing covered services in relation to DeFi projects. Description of an arrangement as "decentralised" or "distributed" is not determinative and regulators are expected to take a functional approach when identifying in-scope persons. Even where no person with sufficient control has been identified, regulators may still require as a mitigating measure that a regulated VASP is involved in activities related to the DeFi project.

## Central bank digital currencies

Central bank digital currencies (CBDCs) do not fall within the definition of a Virtual Asset, but the FATF Standards would apply to them in a similar manner as any other form of fiat currency.

## Conclusion

The Guidance provides useful insights on some of the key issues affecting the digital assets industry. The FATF is the global standard-setting body in the area of AML/CTF and its Standards are typically followed by most jurisdictions. Market participants should, however, be aware that individual jurisdictions may implement these standards in a slightly different manner and, therefore, the FATF requirements should always be read together with local requirements.

# Key contacts


**Michael McKee**
Partner
London
+44 20 7153 7468
michael.mckee@dlapiper.com

**Tony Katz**
Partner
London
+44 20 7153 7835
tony.katz@dlapiper.com

**Sam Millar**
Partner
London
+44 20 7153 7714
sam.millar@dlapiper.com

**Chris Whittaker**
Senior Associate
London
+44 20 7796 6035
chris.whittaker@dlapiper.com