

Anti-Money Laundering Bulletin

Regulatory News Update

Spring/Summer 2022

The Economic Crime (Transparency and Enforcement) Act: What does it mean for commercial real estate?

Further FCA AML failings identified in challenger banks

UK financial regulatory authorities publish joint statement on sanctions and the cryptoasset sector

FCA begins consultation on use of 'side pockets' for retail funds with Russian, Ukrainian or Belarusian exposure

Latest sanctions block Russia's largest banks, cyber actors and more; Biden's executive order prohibits investments in Russia by US persons

FATF report on state of effectiveness and compliance with FATF standards and Moneyval statement



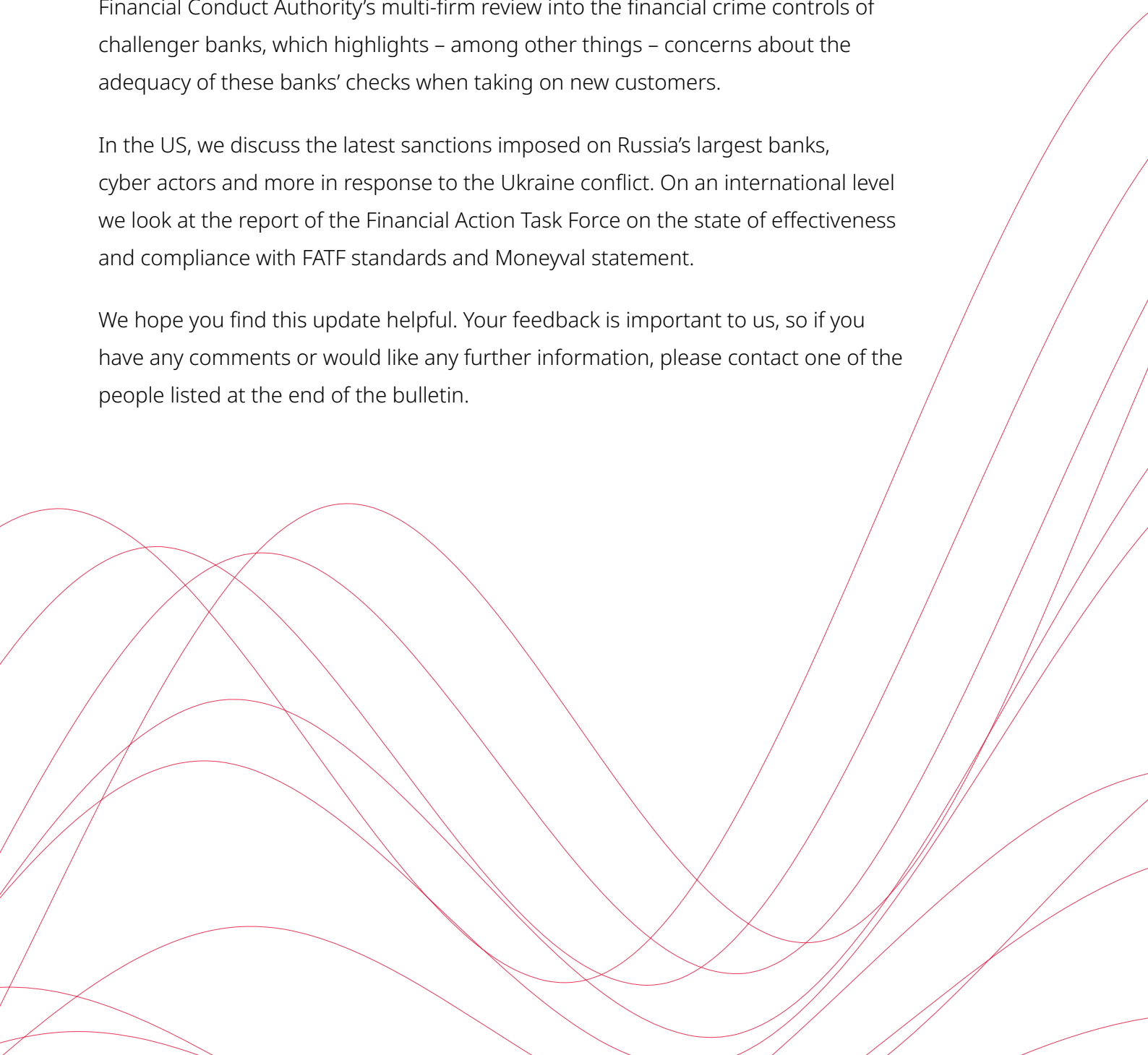
Introduction

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

In the UK, we provide insights on the new Economic Crime (Transparency and Enforcement) Act, which has been introduced following an increased focus on the ownership of UK property by people potentially subject to sanctions and establishes a new Register of Overseas Entities. In addition, we analyse the findings of the Financial Conduct Authority's multi-firm review into the financial crime controls of challenger banks, which highlights – among other things – concerns about the adequacy of these banks' checks when taking on new customers.

In the US, we discuss the latest sanctions imposed on Russia's largest banks, cyber actors and more in response to the Ukraine conflict. On an international level we look at the report of the Financial Action Task Force on the state of effectiveness and compliance with FATF standards and Moneyval statement.

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

The Economic Crime (Transparency and Enforcement) Act: What does it mean for commercial real estate?

The Economic Crime (Transparency and Enforcement) Act (the Act) was first introduced to Parliament as a Bill on March 1, 2022 and received Royal Assent on March 15. Fast-tracked as part of the government's response to the Ukraine conflict, which has given rise to an increased focus on the ownership of UK property by people potentially subject to sanctions, the Act will have a significant impact on commercial real estate. The main operative provisions of the Act have not yet come into force. However, it's clear the UK government wants to see it take effect quickly and it's vital that businesses start planning now – as far as possible, given that the precise details of how the new regime will work are not yet in place – to deal with its effects.

Although this article focuses on the position in, and mainly uses terminology applicable to, England and Wales, the new Act applies throughout the UK.

What does the Act say?

The Act establishes a new Register of Overseas Entities, to be maintained at Companies House. Any overseas entity that owns or plans to own a "qualifying estate" in UK property must apply to become a "registered overseas entity" on

this register. To do this, it must submit details of its "beneficial owners" to Companies House (including, for individuals, personal details such as name, date of birth and residential address although some of this information will not appear on the public register), and this information must be updated regularly. Overseas entities that already own property in the UK have to become registered within six months from the date on which Companies House is first required to open the overseas register under the Act (this is known as the "transitional period," but the exact date is not yet known). That transitional period of six months has been substantially reduced from the original 18-month period when the Act was first introduced to Parliament.

A "qualifying estate" in England is a freehold or a lease of more than seven years. (In Scotland, the relevant property interests are ownership, and leases of more than 20 years.) The definition in the Act of "beneficial owner" is similar to that currently used in relation to the Persons with Significant Control (PSC) register. The PSC register is maintained at Companies House in relation to UK corporate entities and Scottish legal partnerships and is, broadly, a person owning 25% or more of the shares or voting rights in that entity, or who has a right to appoint or remove a majority of the board of directors, or who exercises or is entitled to exercise significant control over that entity.

How will the Act prevent an overseas entity from disposing of its property?

Before the end of the transitional period, the Land Registry will place a restriction on every registered title owned by an overseas entity (provided that it acquired that property on or after January 1, 1999). The restriction will prohibit any "relevant disposition" (meaning, broadly, a transfer, a lease of more than seven years or a legal charge) unless the overseas entity is a registered overseas entity at the time of the disposition

(which means it must also have complied with the new annual updating duty) or is exempt. It's also worth noting that the restriction:

- doesn't affect the legal title to the property, only the ability to dispose of it;
- will only take effect at the end of the six-month transitional period; and
- will contain carve outs for certain dispositions such as dispositions required to be made in pursuance of a statutory obligation, court order, contractual obligation pre-dating the restriction, a power of sale conferred on a secured creditor or receiver or a disposition by an insolvency practitioner.

Restrictions will not be placed on titles in the Land Register of Scotland, but provisions with similar practical effect will take effect in relation to property (including leases of more than 20 years) acquired on or after December 8, 2014.

If the restriction only takes effect at the end of the transitional period, can an overseas entity just sell its property before the end of the transitional period to avoid having to reveal the identity of its beneficial owners?

No. An overseas entity must disclose whether or not it has made a "relevant disposition" of qualifying property during the period from February 28, 2022 until the end of the transitional period. If it has, it will need to give details of the identity of its beneficial owners as they were immediately before the disposition. These provisions are intended to prevent entities from making a quick sale simply to avoid having to reveal beneficial ownership information.

Are there any exemptions?

There is no set list of exemptions from the Act as a whole. The only exemption is where the UK government chooses to exempt an entity on the basis of national security or for the purposes of preventing or detecting a serious crime – and, as noted above, the restriction will also not apply to certain types of disposition (such as a sale pursuant to a statutory obligation or prior contractual obligation).

Penalties

Failure to comply with the Act is a criminal offence punishable by fines (the daily fine stands at GBP2,500 for both the overseas entity itself and each officer of it

which is in default) which is a substantial increase from the GBP500 suggested in the original draft legislation; or, for some offences, imprisonment.

The Act unfortunately retains the rather unclear wording that we first saw in the draft legislation, stating that unpaid sums under the Act (presumably fines) may (in England) be secured by a charge over the property owned by the overseas entity and that the regulations introduced should include "provision about the priority of any such charge" – it's unclear how this would work in practice and we await further guidance from the UK government.

What about trusts and nominees?

- **Trusts:** substantial amendments have been introduced to the Act in an effort to close perceived potential loopholes which would have prevented the Act from having the effect desired by the UK government. The new provisions require that, where the beneficial owner of an overseas entity is a trust, information must be given about the trust, its trustees and also the beneficiaries of the trust as if they were beneficial owners of the overseas entity that owns the property.
- **Nominee companies:** A further loophole that was much debated, but which appears not to have been closed by the Act, relates to the use of nominees. The Act only captures beneficial owners of the entity which is the registered proprietor of the property, not beneficial owners of the property itself (which is a subtle but important difference). The example cited in the House of Lords debate perhaps best illustrates the point, so we have summarized it below:

If an individual sets up an overseas company to buy a property in the UK, they will be a beneficial owner of the overseas company so will have to disclose their identity under the Act. However, the individual could ask a professional services company/firm to buy the UK property for them using its general nominee company (which nominee company is an overseas entity which owns a large number of properties all beneficially owned by different people). The nominee company issues a declaration that it is holding the land as the individual's nominee and that the individual is the beneficial owner of the property. In this case, the nominee company is the overseas entity that owns the property and the beneficial owner of the nominee company is the professional services firm that set it up, not the individual which is the true beneficial owner of the property. The declaration issued by the nominee company is private, so the individual remains anonymous.

We await further guidance and regulations which may close this loophole.

Practical steps

Whether you're an overseas entity or not, it's important to start thinking about and, as far as possible preparing for, the changes brought about by the Act.

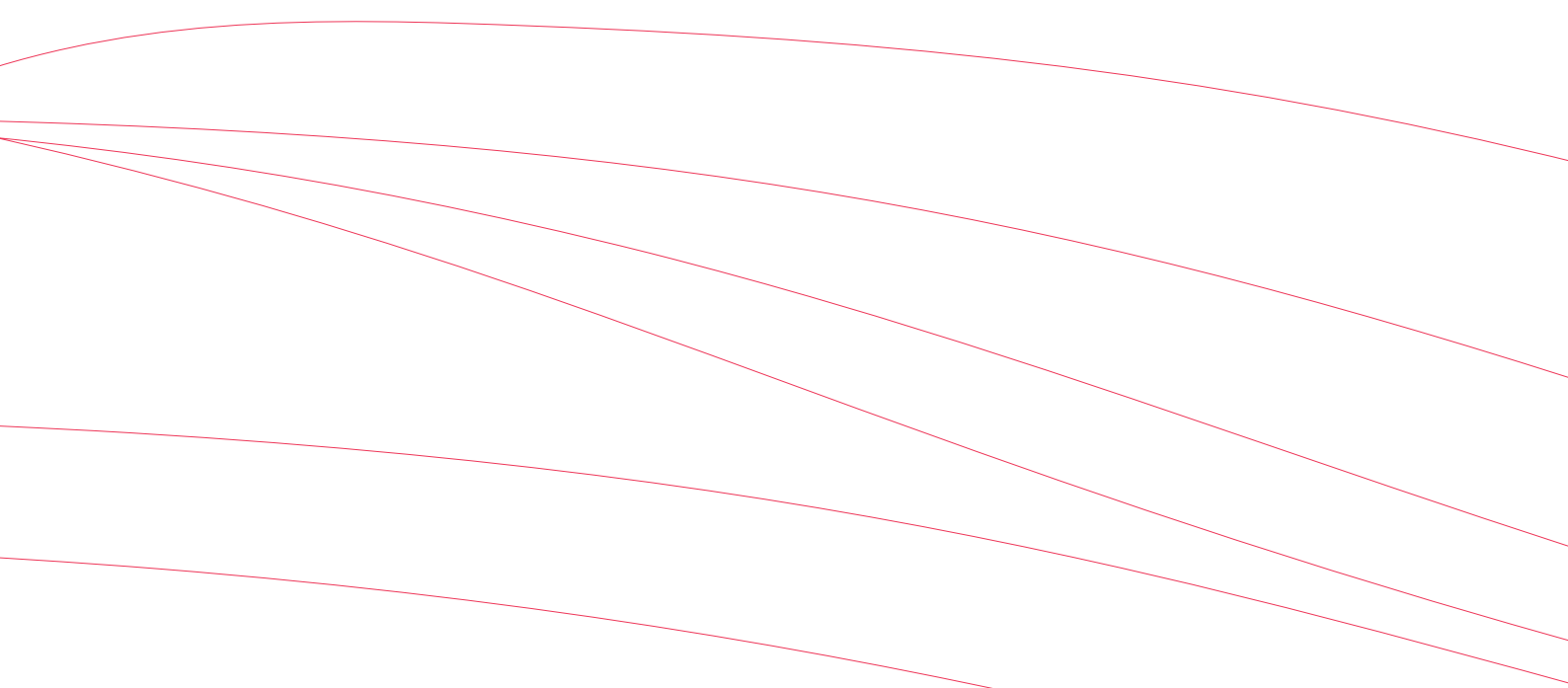
Overseas entities that own or plan to acquire UK property will want to consider the following:

- **Get ready to register:** speak to your company secretarial teams and start pulling together information on the beneficial ownership of the overseas entities in your group in readiness for making an application to become a registered overseas entity.
- **Register quickly:** submit your application promptly – when Companies House opens the doors to receiving applications, there will be a huge volume of applications and it's not yet clear what further support will be available to either Companies House or the Land Registry to help deal with the increased workload, so it's recommended getting in early.
- **Check the Land Registry:** check to see if the restriction has been added to the registered titles of any properties you already own. The Land Registry is being asked to consider notifying registered proprietors when this happens, but we do not yet know whether this will be possible.

Non-overseas entities or persons should not ignore the changes. If you are:

- **Selling to an overseas entity:** the entity will not be able to become the registered proprietor until they have become a registered overseas entity. Legal title will therefore remain with you and your involvement in and liability for the property may continue past the usual registration gap. It's in your interest to ensure an overseas buyer complies with its obligations under the new Act: ensure that you see evidence of registration as a registered overseas entity before completion.
- **Lending to an overseas entity:** lenders will want to ensure that borrowers are compliant with the Act; to do this, it'll be necessary to include conditions precedent to drawdown evidencing due registration, which should be supported by warranties as to the accuracy of the information submitted and undertakings to comply with the ongoing updating duty.
- **If you're involved in a landlord or tenant relationship with an overseas entity:** you should be aware that certain notices (for example, in England, certain notices under the Landlord and Tenant Act 1954) need to be served by the legal landlord/tenant so it's important to ensure your overseas entity counterparty is duly registered on the register of overseas entities.

While the new Act supports the UK government's plans to crack down on entities and people who are using UK property to launder money or may be caught by sanctions, it nevertheless presents an additional hurdle to legitimate overseas investors and anyone transacting with them.



Further FCA AML failings identified in challenger banks

Following the FCA's flurry of activity in 2021 and its recently announced 2022/23 Business Plan on April 7, 2022, the FCA has published findings of its [multi-firm review](#) into the financial crime controls of challenger banks.

The review highlights concerns about the adequacy of these banks' checks when taking on new customers and expects challenger banks to evaluate their approaches to identifying and assessing anti-money laundering (AML) risks, particularly as their customer base and business areas grow.

Challenger banks should note the key findings of the FCA's review, the wider UK National Risk Assessment which partly prompted this review and the FCA's [Dear CEO Letter](#) from May 2021 addressed to retail banks. See our briefing [here](#) on the Dear CEO Letter.

Additionally, challenger banks must be prepared to give the FCA an update on their own financial crime framework as part of monitoring compliance with money laundering regulations – including any changes and remedial activity that may be undertaken.

In the event of enforcement action for AML failings, a failure to carry out a gap assessment and consider changes to financial crime controls could be deemed to be an aggravating factor in any penalty calculation (see Step 3 of the FCA's Decision Procedures and Penalties Manual).

Scope of the review

Acknowledging there is no universally agreed definition of the term "challenger banks," the FCA cites the UK's National Risk Assessment description: "a sub-set of retail banks that aim to reduce the market concentration of traditional high street banks using technology and more up-to-date systems" (Challenger Banks). It is also useful

to note that the FCA considers there to be a further subset of Challenger Banks, known as "digital banks" which have the following common features:

- They primarily offer personal accounts.
- They operate without a branch network.
- They provide financial services through smartphone apps.

The scope of the FCA's review, conducted in 2021, included six retail Challenger Banks which primarily consisted of digital banks (over 50% of the relevant firms) and covered over 8 million customers (meaning over 10% of the UK population). The review of financial crime controls covered a broad range of topics:

- governance and management information
- policies and procedures
- risk assessments
- identification of high risk/sanctioned individuals or entities
- due diligence and ongoing monitoring
- communication, training and awareness

Summary findings

The FCA did observe the following good practices, praising Challenger Bank innovation and the nature of certain controls operated:

Effective and innovative uses of data and information
Challenger Banks collected to mitigate risks.
These included non-traditional approaches to identify, verify and monitor customers – such as video selfies and mobile phone geolocation data.

Evidence of stand-alone financial crime policies and procedures being regularly updated and were tailored to the financial crime risks of their specific business.

Some Challenger Banks mitigating fraud risk through incorporating additional monitoring for known fraud typologies at onboarding and as part of account monitoring. This included Credit Industry Fraud Avoidance System checking, as well as checks on customers using multiple devices to manage their accounts.

However, the FCA identified failings outweighing the positive features identified above, highlighting that the National Risk Assessment states that “many challenger banks depend on rapid customer growth for survival.” The FCA is clear in stating that this must not come at the detriment of, for example, complying with customer due diligence obligations as set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

The top four findings are:

Customer risk assessment (CRA)

- Certain Challenger Banks did not have a suitably developed or detailed CRA and some Challenger Banks did not have one at all.
- All Challenger Banks should have a suitable CRA – without it, due diligence measures and ongoing monitoring activities cannot be effective or proportionate to a Challenger Banks’ customer base and such risk assessments form the backbone of systems in place to identify, assess, monitor and manage AML risk.
- Once a CRA is established, they should also be regularly updated to reflect changes to business models, products and customers.

Customer due diligence (CDD) and enhanced due diligence (EDD)

- While basic identification and verifications were met, full customer information was not always obtained (including income and occupation details) to determine a customer’s risk profile. This led to an inability to fully assess the purpose and intended nature of a customer’s relationship, not allow Challenger Banks to fully identify high risk customers and, subsequently, also undermine transaction monitoring.
- CDD procedures were not always in place at customer onboarding and the FCA states that transaction monitoring systems alone will not be sufficient,

and Challenger Banks must comply with CDD requirements. Inadequate CDD means less effective transaction monitoring.

- EDD was also not consistently applied, nor documented formally. A clear process for identifying and applying EDD to high-risk customers, including other types of high-risk customers to politically exposed persons and ineffective transaction monitoring alert management.
- Challenger Banks had inconsistent and inadequate rationales for discounting alerts, lacked basic information in investigation notes and lacked holistic reviews of such alerts.
- Similarly, transaction monitoring alerts should be reviewed in a timely manner and adequate resources should be in place to enable this. Maintaining adequate resources is, as a reminder, a fundamental FCA threshold requirement (both at authorization and on an ongoing basis, for regulated firms).
- The above meant that suspicious activity reports (SAR) were affected and not necessarily made as soon as practicable, as required under the Proceeds of Crime Act 2002.

SAR submission

- Noting the substantial increase in the volume of SARs and Defence Against Money Laundering (DAML) reports that Challenger Banks have submitted to the UK Financial Intelligence Unit (UKFIU) at the National Crime Agency (NCA), often these reports were for very low amounts which have a lower likelihood of resulting in law enforcement action.
- Making reports, particularly DAML, when exiting customers which do not fit within your risk appetite should prompt Challenger Banks to consider whether such clients should have been onboarded in the first instance. Additionally, Challenger Banks must apply appropriate blocks where transactions are reported and Challenger Banks await a response from the UKFIU regarding a DAML.
- Finally, the overall quality of SARs can be improved by:
 - describing why certain transactional data is suspicious;
 - detailing the circumstances giving rise to the suspicion; and
 - using SARs to report suspicious activity, rather than fraud or send information about predicate offences.

- UKFIU publications, JMLSG guidance and the FCA's Financial Crime guide all provide further information to help Challenger Banks with their reporting, while also considering other channels such as Action Fraud, to safeguard customers.

Financial crime change programs

- As Challenger Banks grow, either with new products, developing into new areas or taking on new and different types of customers, management must provide adequate oversight and appropriately implement change programs to align with the nature, scale and complexity of its business and activities.
- Clear project plans for control changes with key milestones, accountable executives and delivery dates are essential. Also, senior management should track projects and ensure key deadlines are met.
- Wider governance, such as Risk Committees, Audit Committees and the CEO should be involved in overseeing material developments in such programs, to bolster the governance and provide challenge in financial crime change programs.

Challenger Banks should also not forget their FCA Principle 11 notification obligations. In the context of this review, the FCA identified instances where there have been significant financial crime control failures and the Challenger Bank failed to notify the FCA. This could be prompted by Internal Audit findings, compliance reviews or whistleblowers which highlight that financial crime control frameworks may not be fully compliant and remedial steps are required.

Summary

The FCA's identified AML failings are wide-ranging, covering senior management and governance arrangements down to the quality of SAR submissions and the specificity of CDD and EDD checks, echoing and developing on findings from last year's [Dear CEO Letter](#).

Challenger Banks should conduct a gap analysis of the areas above and promptly work to amend the AML processes and procedures in place as necessary using appropriate resources and considering the breadth of financial crime guidance available to them.



UK financial regulatory authorities publish joint statement on sanctions and the cryptoasset sector

On March 11, 2022, the Financial Conduct Authority (FCA) published a joint statement, with the Bank of England (BoE) and the Office of Financial Sanctions Implementation (OFSI), regarding the implementation of the latest sanctions against Russia in the cryptoasset sector (Joint Statement).

The UK regime on sanctions is primarily set out in the Money Laundering Regulations 2017 (MLRs) and regulations made under the Sanctions and Anti-Money Laundering Act 2018 (SAML). The OFSI, which forms part of HM Treasury, is the regulatory body responsible for implementing sanctions in the UK.

Using cryptoassets to evade economic sanctions is a criminal offence in the UK. In addition, since January 2020, a number of cryptoasset firms are required to register with the FCA under the MLRs and comply with a number of requirements aiming to prevent money laundering (eg undertake customer due diligence when establishing new business relationships and on an ongoing basis thereafter).

The Joint Statement restates that cryptoasset firms, like all financial services firms in the UK, are expected to comply with applicable sanctions measures. This includes reporting concerns about sanctions breaches to the UK Financial Intelligence Unit (UKFIU) of the National Crime Agency pursuant to the Proceeds of Crime Act 2002 (POCA).

Cryptoasset businesses must take certain steps if they are aware or have “reasonable cause to suspect” they are in possession or control of or are in any manner dealing with funds or economic resources belonging to

a “designated person” under the applicable sanctions list. This involves in most cases freezing the relevant assets and not dealing with them or making them available to a designated person.

The obligation to comply with sanctions measures goes beyond the requirements under the MLRs, although parallels can be drawn in certain respects. So, in addition to measures such as identifying customers and monitoring transactions, cryptoasset firms are expected to implement further controls relating to sanctions specifically. These may include taking the following steps:

- updating their existing risk assessments in respect of their business and customers to take into account current sanctions measures;
- ensuring that appropriate processes are in place to identify customers using corporate vehicles to conceal ownership or the source of funds;
- screening customers and transactions against updated sanctions lists and implementing regular re-screening as required;
- identifying suspicious behavior and transactions in a timely manner and reporting it as required; and
- where relevant, using blockchain analytics solutions to identify transactions that are connected to higher risk wallet addresses.

Firms should also look out for potential red flags, such as the involvement of cryptoasset providers, which are known to be high-risk or the use of tools that aim to hide the location of the customer or the source of cryptoassets (eg VPNs, proxies, mixers and tumblers). Overall, each case should be assessed holistically and take into account a combination of risk indicators where relevant.

FCA begins consultation on use of ‘side pockets’ for retail funds with Russian, Ukrainian or Belarusian exposure

The FCA has launched a consultation with the industry regarding the use of “side pockets” in dealing with sanctioned assets. Fund managers are currently facing significant challenges in valuing and selling Russian, Belarusian and Ukrainian assets. As a result, the FCA is considering permitting the segregation of these illiquid assets by designating them to a side pocket account. Due to the urgency and fast-paced nature of the issues faced, the FCA’s consultation was a short one, opening on April 28 and closing two and a half weeks later on May 16.

The FCA states that the use of side pockets could potentially allow new investors to enter into the fund without exposure to sanctioned and illiquid assets. And it could also allow existing investors to redeem the majority of their contribution while leaving the sanctioned assets untouched in the side pocket, still retaining rights to any eventual value that may materialize. The use of side pockets could also be the catalyst that allows previously suspended funds to start dealing again, as the sanctioned assets are ring-fenced from the fund’s other scheme property.

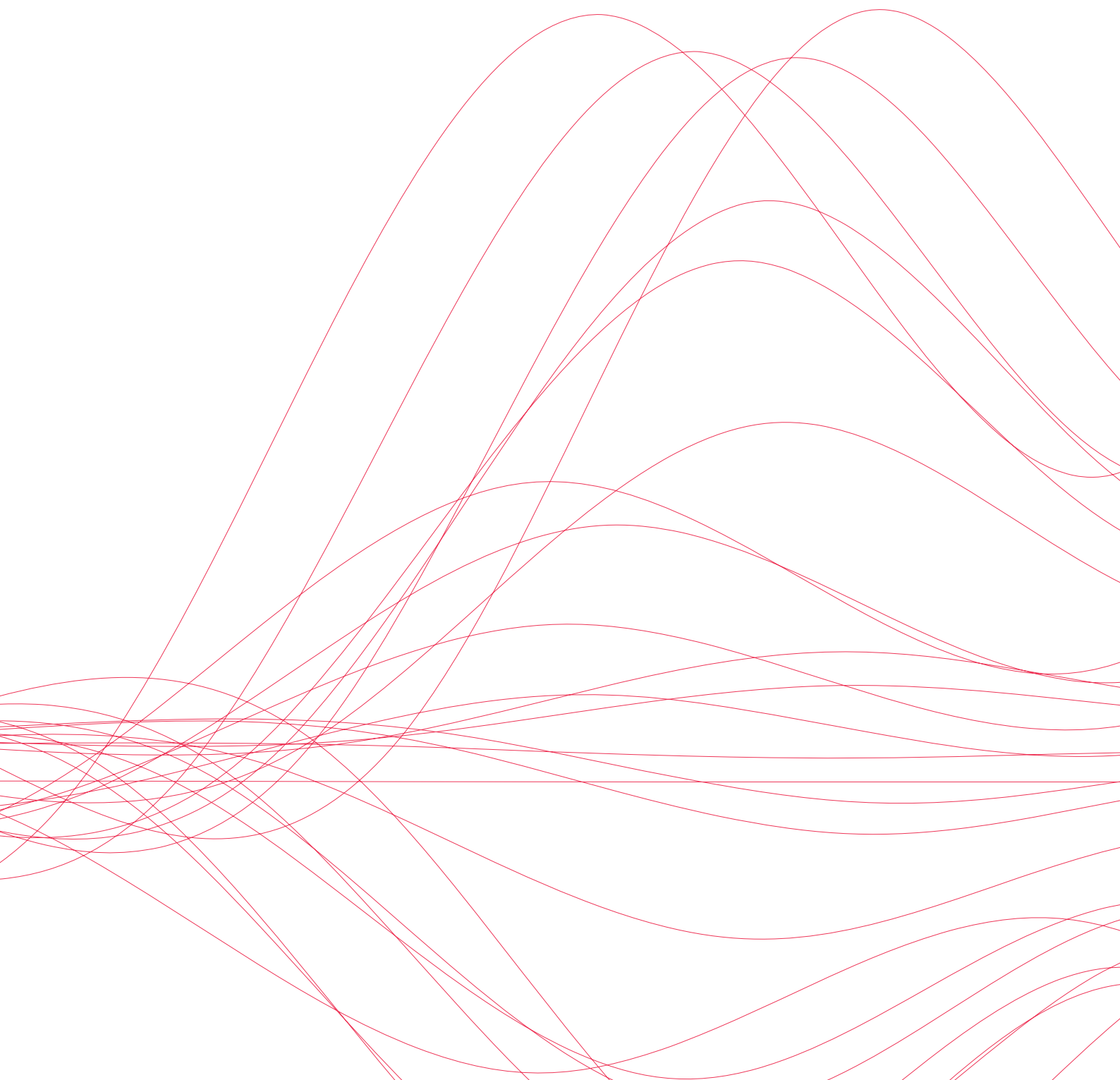
Currently, placing assets in a side pocket is only permitted for alternative investment funds, so the FCA’s proposals to restrict the scope of assets subject to the new regime prevents a more significant change to the regulatory landscape. The FCA suggests that assets suitable to designate to go into side pockets should be those subject to direct or indirect contravention of the financial sanctions regime, or those assets economically impacted due to connections with Russia, Ukraine and/or Belarus. The FCA provides an example of what the latter may involve and suggests that for funds where the sale of underlying assets is being prevented by authorities of the affected countries, the use of a side pocket may alleviate some of the resulting financial impact.

The side pocket would still be managed by the authorized investment fund manager, although this would be done with a view to exiting the investments as soon as practicably possible in a way that is in the investor’s best interests. The FCA also stated that the proposed regime would be permissive and there is therefore no obligation on fund managers to implement a side pocket where affected assets are involved.

The FCA recognized it may be the case that the creation of a side pocket is an unnecessary measure to protect the interests of unit holders and may also lead to the unfair treatment of investors across the fund. The fund manager must consider all options and make decisions in the unitholders’ best interests – which means that the creation of a side pocket may be inappropriate when compared to a fund suspension in some circumstances.

The FCA will require the fund manager to amend the fund agreement and prospectus before creating the side pocket. While conceding that in doing so the process of creating a side pocket is in danger of becoming quite lengthy, transparency concerns dictate that the FCA's Fund Authorisation team will still require notification of any changes to the fund agreement and prospectus and conversely funds will need their

subsequent approval. Whether approval will be granted depends on factors such as whether the scheme documents empower the fund manager to issue units in such a manner and whether the terms on which the side pocket will operate are sufficiently clear. The FCA notes that it will not express a view on whether the creation of the side pocket is in the unitholders' best interests – it is for the fund manager alone to make such a decision.





US

Latest sanctions block Russia's largest banks, cyber actors and more; Biden's executive order prohibits investments in Russia by US persons

On April 6, 2022, the [White House](#) [announced](#) a new Executive Order banning new investment in the Russian Federation and an array of additional blocking sanctions targeting Russian financial institutions, elites and cyber actors. Notably, as a result of these new measures, new investments in Russia by US persons have been prohibited and two of Russia's largest banks, Sberbank and Alfa-Bank, which had previously been subject to narrower restrictions, have now been blocked.

Secretary of the Treasury, in consultation with the Secretary of State, to any person located in the Russian Federation." We anticipate further guidance from OFAC regarding new investment and the categories of services covered by the executive order. However, the term "new investment" was defined previously by OFAC in connection with the energy sector to include "a commitment or contribution of funds or other assets for, or a loan or other extension of credit to, new energy sector activities (not including maintenance or repair) located or occurring in the Russian Federation..."

In a background press briefing held as the executive order was announced, a senior Biden administration official stated that the purpose of this executive order is to ensure that "the mass exodus from Russia that we're seeing from the private sector, which is now over 600 multinational companies and growing ... will endure."

Full blocking sanctions imposed on major Russian financial institutions Sberbank and Alfa-Bank, additional Russian elites and cyber actors

The [Treasury Department](#) and OFAC also announced a significant escalation of the economic measures imposed on the Russian financial sector, including the imposition of full blocking sanctions on Sberbank and 42 subsidiaries, Alfa-Bank and 6 subsidiaries, and 5 Alfa-Bank-owned maritime vessels. Blocking sanctions were also imposed on numerous Russian elites and [cyber actors](#).

Sberbank, Russia's largest bank, [was previously subject to more targeted sanctions](#) pursuant to Directive 2 under Executive Order 14024, and Alfa-Bank, Russia's fourth largest bank, [was previously subject to sanctions](#) pursuant to Directive 3 under the same executive order. Both institutions have now been added to OFAC's Specially Designated Nationals (SDN) List.

These new measures supplement the extensive measures previously announced by the US government and described in our previous client alerts published on [February 23](#), [February 25](#), [February 28](#), [March 4](#), [March 9](#), [March 16](#), [March 29](#) and [April 5, 2022](#).

New executive order prohibits investment in the Russian Federation by US persons

The White House issued a new executive order titled "[Prohibiting New Investment in and Certain Services to the Russian Federation in Response to Continued Russian Federation Aggression](#)," which prohibits "new investment in the Russian Federation by a United States person, wherever located," and the "the exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any category of services as may be determined by the

In connection with these new blocking sanctions, OFAC revised or issued the following general licenses:

- [General License 8B](#): Adding Alfa-Bank to the list of entities, which already included Sberbank, in connection with the authorization of transactions related to energy through 12:01 am (EDT) on June 24, 2022.
- [General License 22](#): Authorizing the wind down of transactions involving PJSC Sberbank through 12:01 am (EDT) on April 13, 2022.
- [General License 23](#): Authorizing the wind down of transactions involving Alfa-Bank through 12:01 am (EDT) on May 6, 2022.

General Licenses 9B, 10B and 21, which were included among the General Licenses issued on April 6, were superseded on April 7 following the issuance of General Licenses 9C, 10C and 21A, which are described below.

Also on April 6, 2022, blocking sanctions were imposed on [additional Russian elites, members of the Russian Security Council and their family members](#), including President Putin's adult children, Foreign Minister Lavrov's wife and daughter, and former President and Prime Minister of Russia Dmitry Medvedev and Prime Minister Mikhail Mishustin.

On April 5, 2022, [the Department of the Treasury and OFAC](#) also announced blocking sanctions on major Russia-based cyber actors, including Hydra Market, the world's largest darknet market, and Garantex Europe OU, a virtual currency exchange.

Full blocking sanctions imposed on two major Russian state-owned enterprises, United Shipbuilding Corporation and Alrosa

On April 7, 2022, [the Department of the Treasury, Department of State and OFAC](#) announced blocking sanctions targeting two Russian state-owned entities, Public Joint Stock Company Alrosa, the world's largest diamond mining company, and United Shipbuilding Corporation, Russia's largest shipbuilder, and their sprawling network of subsidiaries. The members of United Shipbuilding Corporations' board of directors were also subject to these new sanctions.

With these new sanctions, OFAC revised or issued the following general licenses:

- [General License 9C](#): Authorizing all transactions prohibited by the Russian Harmful Foreign Activities Sanctions Regulations that are ordinarily incident and necessary to dealings in debt or equity of Sberbank, Alfa-Bank or Alrosa, or any entity in which they own, directly or indirectly, a 50% or greater interest, provided that any divestment or transfer of, or facilitation of divestment or transfer of the debt or equity must be to a non-US person. Note that the date of the issuance of the debt and the length of the authorization varies for each of the three entities.
- [General License 10C](#): Authorizing transactions that are ordinarily incident and necessary to the wind down of derivative contracts that include Sberbank, Alfa-Bank or Alrosa as a counterparty or are linked to debt or equity of those companies, provided that any payments to a blocked person are made into a blocked account. Note that the date of the underlying derivative contracts and the length of the authorization varies for each of the three entities.
- [General License 21A](#): Authorizing US persons to engage in all transactions ordinarily incident and necessary to the wind down of Sberbank CIB USA, Inc. and Alrosa USA, Inc., or any entity in which they own, directly or indirectly, a 50% or greater interest, including the processing and payment of salaries, severance and expenses; payments to vendors and landlords; and closing of accounts through 12:01 am (EDT) on June 7, 2022.
- [General License 24](#): Authorizing the wind down of transactions involving Alrosa through 12:01 am (EDT) on May 7, 2022.
- [General License 25](#): Authorizing all transactions ordinarily incident and necessary to the receipt or transmission of telecommunications involving the Russian Federation, as well as the exportation or re-exportation, sale, or supply, directly or indirectly, from the US or by US persons, wherever located, to the Russian Federation of services, software, hardware, or technology incident to the exchange of communications over the internet, such as instant messaging, videoconferencing, chat and email, social networking, sharing of photos, movies, and documents, web browsing, blogging, web hosting and domain name registration services.

Department of Commerce identifies additional restricted entities and private and commercial aircraft; adds major Russian airlines to Denied Persons List

On March 30, 2022, BIS added 73 more private and commercial aircraft to its list of aircraft that have allegedly violated the Export Administration Regulations (EAR) for flying into Russia or Belarus from other countries and removed 12 aircraft that it has authorized to return to the owners. The current non-exhaustive list of aircraft in violation of the EAR, for which any subsequent actions taken with regard to any of the listed aircraft by any person worldwide, including, but not limited to, refueling, maintenance, repair or the provision of spare parts or services, are prohibited can be found on [the BIS website](#).

Effective April 1, 2022, BIS has also added 120 Russian entities to its restricted Entity List. The designated entities include major Russian transportation, electronics and aerospace companies as well as various research institutions. As a result of the designations, virtually all exports, reexports and transfers of goods, technology and software subject to the EAR to the

listed entities, as well as sales or transfers to the listed entities of the non-US made products of US technology, software and equipment (ie so-called “foreign direct products”) are effectively banned.

On April 7, 2022, BIS issued orders (initially for six months) denying the export privileges of three Russian Airlines – Aeroflot, Azur Air and UTair – due to ongoing export violations related to the new comprehensive export controls on Russia. The denial orders prohibit any person anywhere from exporting, reexporting, transferring (in-country), servicing or taking any action that facilitates the acquisition or attempted acquisition of the ownership, possession or control of any item subject to the EAR to or on behalf of these airlines. This effectively puts global Maintenance, Repair and Operation (MRO) vendors on notice that they will be in violation of the EAR if they service or support these aircraft no matter where they are located. Items directly related to the safety of flight may be authorized by BIS. BIS noted that “[c]ompanies that violate the expansive export controls we have imposed on Russia will find themselves the target of Commerce Department enforcement action.”



FATF report on state of effectiveness and compliance with FATF standards and Moneyval statement

FATF Report

On April 19, 2022, the Financial Action Task Force (FATF) published its report on the state of global efforts to tackle money laundering, terrorist and proliferation financing. The report noted that 76% of countries have now satisfactorily implemented the FATF's 40 Recommendations, which is a significant improvement in technical compliance with laws and regulations compared with the figure of 36% from 2012.

However, while the headline figure was favorable, the report also highlighted that many countries face substantial challenges in taking effective action in line with the risks they face. In particular, the FATF cited difficulties in investigating and prosecuting high-profile cross-border cases and preventing anonymous shell companies and trusts being used for illicit purposes. Nearly all (97%) of 120 countries assessed by the FATF were found to have low to moderate effectiveness ratings for preventing money laundering and terrorist financing in the private sector, while only 40% of jurisdictions have used terrorism finance targeted financial sanctions to freeze terrorist assets and 22% have used terrorism finance confiscation measures in accordance with the relevant UN Security Council Resolutions.

Perhaps most damningly, the FATF noted that only 10% of jurisdictions had effectively implemented supervisory measures, while around 52% of countries have the necessary laws and regulations to understand, assess the risks of, and verify the beneficial owners or controllers of companies.

To address some of these deficiencies and increase international cooperation, the FATF recommended that countries should establish dedicated liaison officers overseas to facilitate exchanges and joint investigations into complex cases involving multiple jurisdictions.

Moneyval Annual Report

Following on from the FATF Report, on May 6, 2022, Moneyval, the Council of Europe's anti-money laundering body, observed that EU governments needed to increase their efforts to combat financial crime through crypto-assets.

Moneyval, which assesses EU states' compliance with international anti-money laundering and countering the financing of terrorism (AML/CFT) standards, said in its [annual report](#) that the cryptoasset sector's growth had become a significant challenge to combating money laundering since traditional forms of control that banks and institutions have on financial flows and services could not be used to police it.

Of particular concern was the decentralized finance (DeFi) sector, which allows greater anonymity for users, as well as special, smaller cryptoassets set up specifically for the purpose of money laundering.

It was noted in the report that:

- money launderers have been abusing cryptocurrencies from their inception a decade ago, initially to transfer and conceal proceeds from drug trafficking;
- Moneyval suspected some of the smaller cryptocurrencies have been set up specifically with the motive of laundering;
- supervisory cooperation in this field is at its very nascent stages, and is not yet keeping pace with the rapid evolution of technology; and
- the global nature of the sector made it difficult to police entities or crypto-financial products that often are spread across multiple countries.

Moneyval noted that it was looking into the regulatory framework for virtual assets in EU Member States and expects to issue a typologies study dedicated solely to cryptocurrency money laundering trends later this year.

This work will align with other EU legislative and regulatory measures in the pipeline, most notably the Markets in Crypto-Assets (MiCA) regulation, a single AML rulebook that will cover cryptoassets, and the establishment of an EU-level Anti-Money Laundering Authority (AMLA).

Moneyval also recommended that greater focus should be on the role of specialized “gatekeeper” professions, such as lawyers, accountants and other services providers, who in its view often assist launderers. In this respect, Moneyval noted that the median level of compliance with FATF standards was

below the satisfactory threshold in the supervision of the financial sector and said a lack of resources at national AML agencies was often the root cause for poor compliance ratings, with insufficient resources allocated to supervisors in a majority of countries.

It also stressed that there was a lack of communication between financial intelligence units, law enforcement and the private sector, with convictions for serious and complex money laundering offences remaining rare in many EU countries.

According to the report, the agency remains on track to complete its fifth round of mutual evaluations by 2024, and to start its sixth round of evaluations in the same year. The sixth round will feature include increased focus on gatekeeper functions, as well as on assessing the EU AML/CFT framework.



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

