JONES DAY | One Firm Worldwide®

WHITE PAPER

March 2022

2021 Anti-Money Laundering and Sanctions Year in Review

2021 was a precedent-setting year for anti-money laundering ("AML") enforcement and legislation. The digital assets industry continued to grow exponentially, driving the associated AML risks to the forefront of regulatory concerns. In the United States, the new administration established corruption, including money laundering, as a core national security interest. Legislators and regulators alike called for a "whole of government" approach to combatting illicit activity associated with cryptocurrencies, and federal agencies—from OFAC to the FDIC—issued long-awaited guidance for the virtual asset industry.

In the European Union, lawmakers introduced a comprehensive legislative package to harmonize the Union's approach to AML and countering the financing of terror ("CFT"). The proposal calls for the creation of a new AML authority and advances efforts to establish a "single rulebook" for AML/CFT in the European Union.

In Mainland China, new legislation expanded the list of entities subject to AML requirements to include loan companies, insurance agents, and insurance brokers, among others. In Australia, legislative amendments were enacted to reform certain customer due diligence and identification procedures.

This Year in Review explores the above developments and discusses other notable legislative and enforcement activity, including cross-border and intergovernmental initiatives. The Year in Review also provides an outlook on emerging trends and the resulting implications for financial institutions in 2022 and beyond.

TABLE OF CONTENTS

UNITED STATES

FinCEN's RFI for Modernizing AML/CFT Regulations

In December 2021, the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") issued a request for information ("RFI") soliciting comments on ways to "streamline, modernize, and update the anti-money laundering and countering the financing of terrorism ("AML/CFT") regime of the United States."[1] This RFI supports FinCEN's broader ongoing formal review of Bank Secrecy Act ("BSA") regulations as required by Section 6216 of the Anti-Money Laundering Act of 2020. Section 6216 also requires Treasury Secretary Janet Yellen to submit a report on the findings of the formal review to Congress by January 1, 2022. The public release of that report is still pending.

As discussed in the request, the BSA requires a risk-based approach to AML/CFT, which is meant, in part, to ensure that financial institutions dedicate "more attention and resources toward higher-risk customers and activities" rather than toward lower-risk ones. FinCEN noted in the RFI that it is "particularly interested in new and innovative approaches to BSA compliance that promote a risk-based approach to protecting the financial system[.]" FinCEN pointed to its list of National Priorities issued in June 2021 to identify the most significant AML/CFT threats currently facing the U.S. financial system and contributing to increased risk. These National Priorities are: (i) corruption; (ii) cybercrime; (iii) foreign and domestic terrorist financing; (iv) fraud; (v) transnational criminal organization activity; (vi) drug trafficking organization activity; (vii) human trafficking and human smuggling; and (viii) proliferation financing. The RFI's reference to the National Priorities suggests that FinCEN's future enforcement and regulatory efforts will focus on these areas.

In addition to highlighting the risk-based approach and National Priorities, the RFI contains 26 far-ranging questions asking, among other things, whether the Treasury Department's current AML safeguards are sufficient; whether current BSA reporting and recordkeeping requirements require modification; whether any BSA regulations are outdated, redundant, or ineffective; whether any BSA regulations fail to conform with international standards; and whether any BSA regulations or guidance should be amended to improve their efficiency.

The RFI also asks about deficiencies in the U.S. AML/CFT framework, previously identified by the Financial Action Task Force ("FATF"), an intergovernmental watchdog that sets internationally accepted standards for AML/CFT policies. The FATF found that the United States is deficient in monitoring beneficial ownership information and regulating designated nonfinancial businesses and professionals such as accountants, lawyers, notaries, and real estate agents. Looking ahead, it is likely that FinCEN will move to address these deficiencies and bring U.S. regulations closer in line with FATF standards. FinCEN has already taken steps toward that end; in December 2021, the agency promulgated a proposed rule imposing filing requirements on beneficial owners pursuant to the Corporate Transparency Act and issued an advance notice of proposed rulemaking regarding potential reporting requirements for certain real estate transactions.

The RFI further asks whether BSA regulations should "account for technological advancements, such as digital identification, machine learning, and artificial intelligence." FinCEN has recognized the need for the BSA to adapt to the changing technological landscape. This question signals that future regulations may allow firms to utilize new technologies such as these to carry out their AML/CFT obligations more efficiently.

AML Developments Related to Virtual Currencies

In 2021, policymakers issued notable guidance regarding AML issues and digital currencies. On November 1, the President's Working Group on Financial Markets ("PWG"), in conjunction with the Federal Deposit Insurance Corporation ("FDIC") and the Office of the Comptroller of the Currency ("OCC"), released a report on stablecoins, a digital asset designed to maintain a stable value relative to a national currency or other reference asset. [2] Among other regulatory issues, the PWG report discusses the inherent illicit finance risks associated with stablecoins and outlines the concerns they raise for compliance with the rules governing AML/CFT. Noting the ability of stablecoins to facilitate large cross-border transactions, the PWG report identifies potential vulnerabilities regarding the AML/CFT regulation of stablecoins in countries throughout the world. The report emphasizes the need for increased global cooperation in this regard and explains that Treasury will continue to promote the adoption of international AML/CFT standards worldwide. Notably, the report acknowledged the possibility

of building "strong AML/CFT protections . . . into the stablecoin" itself as a means of providing "greater transparency into illicit financial activity."

On November 8, FinCEN released an updated advisory on the use of the financial system to facilitate ransomware payments and associated money laundering activity. Noting "the increase of ransomware attacks in recent months against critical U.S. infrastructure," FinCEN's new advisory observes that "[m]ost ransomware schemes involve convertible virtual currency (CVC)," which the agency described as "the preferred payment method of ransomware perpetrators."[3] The advisory describes new trends associated with ransomware and related payments, including the increasing use of anonymity-enhanced cryptocurrencies, decentralized mixers, and "foreign CVC exchanges" to launder payments associated with ransomware attacks. FinCEN's advisory warns that individuals and entities hired by victims to facilitate ransomware payments may be required to register as money-services businesses and may have continuing BSA obligations. The updated advisory also provides a list of 12 "red flags" intended to assist financial institutions in identifying ransomware-related payments, and reiterates institutions' obligations to file suspicious activity reports ("SARs") for "both *attempted and successful* transactions, including both attempted and successful initiated extortion transactions."

On November 23, the Board of Governors of the Federal Reserve, the FDIC, and the OCC issued a joint statement announcing the completion of a series of interagency "crypto-asset policy sprints."[4] Through this initiative, the agencies sought to enable staff to better understand crypto-assets and the risks they present to regulated financial institutions, including those related to AML compliance. While the statement does not set forth detailed findings, it does identify several areas warranting further public clarity. In 2022, the agencies intend to issue guidance related to, among other things, the safekeeping and custodying of crypto-assets, facilitation of purchases and sales of crypto-assets, loans collateralized by crypto-assets, stablecoins, and holding crypto-assets on balance sheets.

On October 6, DOJ announced the launch of a new National Cryptocurrency Enforcement Team ("NCET"), which will investigate and prosecute the "criminal misuse of cryptocurrency" conducted by "virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors."[5] NCET builds on DOJ's release in late 2020 of the Cryptocurrency Enforcement Framework by the Attorney General's Cyber-Digital Task Force. According to DOJ's announcement, the new teams will work "collaboratively . . . to combine their expertise in financial systems, blockchain technology, tracing transactions, and applicable criminal statutes to address illegal activity involving cryptocurrency in a structured way."

2021 also saw several significant AML enforcement actions involving virtual currencies by DOJ and its partner agencies. In July, DOJ's Money Laundering and Asset Recover Section, or MLARS, assisted in the seizure of bitcoin valued at $2.3 million paid to the digital extortion group Darkside following the Colonial Pipeline attack. By using the Bitcoin public ledger, law enforcement was able to track the digital currency transfers to a specific Bitcoin address.

In August, an individual who allegedly ran a Darknet-based cryptocurrency "mixing" and "tumbling" service pleaded guilty to money laundering conspiracy and to operating an unlicensed money transmitting business. In pleading guilty, the defendant admitted to processing more than $300 million in bitcoin transactions over a seven-year period and agreed to forfeit 4,400 bitcoin worth more than $200 million at the time. The defendant separately agreed to pay a $60 million civil penalty to resolve a parallel enforcement action brought by FinCEN.

In September, Treasury's Office of Foreign Assets Control ("OFAC") sanctioned virtual currency exchange SUEX. SUEX allegedly facilitated criminal transactions involving at least eight ransomware variants, with 40% of its known transaction history involving unlawful activity. OFAC's designation of SUEX was the first sanctions designation against a virtual currency exchange.

State authorities have also been focused on AML compliance by institutions facilitating virtual currency transactions. In July, a leading online retail brokerage disclosed that it has entered into a settlement in principle with the New York Department of Financial Services ("DFS") to resolve alleged violations of New York AML laws, including an alleged "failure to maintain

and certify a compliant anti-money laundering program."[6] According to the company's disclosure, the company expects to pay a $30 million fine to resolve the investigation.

Sanctions Compliance Guidance for the Virtual Currency Industry

On October 15, 2021, OFAC issued, "Sanctions Compliance Guidance for the Virtual Currency Industry" ("Guidance").[7] This highly anticipated guidance, which came less than one month after OFAC's first-ever designation of a virtual currency exchange, details how companies that operate with virtual currency must comply with U.S. sanctions laws. OFAC, recognizing the various facets at play in the virtual currency industry, cast a wide net by making the Guidance applicable to all persons in this space, including administrators, exchangers, miners, wallet providers, and even users.

The Guidance builds on OFAC's existing sanctions framework and best practices for designing compliance programs and screening both customers and transactions for potential sanctions nexuses in other contexts. This framework consists of five essential components: (i) management commitment; (ii) risk assessment; (iii) internal controls; (iv) testing and auditing; and (v) training. The Guidance advocates for a risk-based approach to sanctions compliance, with internal controls as a central component. For instance, geolocation tools and due diligence mechanisms—such as IP address blocking controls and know your customer ("KYC") procedures—are even more crucial in this context given the anonymity that often characterizes virtual currency transactions. The Guidance highlights that OFAC has taken enforcement actions against companies in the virtual currency industry because of their failure to prevent users in sanctioned jurisdictions from using their platforms, in part for failing to use geolocation information available to them.

In conjunction with the Guidance, OFAC updated its frequently asked questions ("FAQs") to provide additional interpretative guidance to virtual currency companies. For example, FAQ 646 clarifies that a U.S. person who identifies a virtual currency that should be blocked under sanctions rules must deny all parties access to it.[8] This can be accomplished in multiple ways, such as by blocking each virtual currency wallet in which the blocked person has an interest or by consolidating wallets containing blocked virtual currency.

Despite the challenges created by a rapidly evolving industry, the Guidance makes clear that virtual currency companies are expected to comply with the same sanctions rules that apply to fiat currency transactions, namely by identifying and preventing unauthorized or prohibited transactions. As virtual currency will undoubtedly remain a priority area of enforcement for OFAC in 2022, industry participants should heed the Guidance when designing and implementing their compliance programs.

JASTA Secondary Liability

In 2021, significant decisions by the Second Circuit Court of Appeals on the viability of aiding-and-abetting claims under the Anti-Terrorism Act ("ATA") raised the possibility that banks and other financial institutions may need to consider undertaking diligence beyond screening against OFAC's list of Specially Designated Nationals and Blocked Persons ("SDNs") and other such lists.

In 2016, the Justice Against Sponsors of Terrorism Act ("JASTA") expanded civil liability under the ATA to "any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism."[9] This requires proof of three elements: "(1) the party whom the defendant aids must perform a wrongful act that causes an injury, (2) the defendant must be generally aware of his role as part of an overall illegal or tortious activity at the time that he provides the assistance, and (3) the defendant must knowingly and substantially assist the principal violation."[10]

Following 2018 and 2019 decisions in the Second Circuit,[11] district courts had generally dismissed claims of secondary liability (i.e., for aiding and abetting or conspiring with a person who committed an act of international terrorism) against foreign banks. In two cases last year, however—*Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842 (2d Cir. 2021) and *Honickman v. BLOM Bank SAL*, 6 F.4th 487 (2d Cir. 2021)—that trend began to shift. By vacating the district court's dismissal in *Kaplan*, while affirming a dismissal in *Honickman*, the Second Circuit signaled that such claims may, at least in certain narrow circumstances, proceed beyond the pleading stage and into discovery, which could potentially mire banks in years of litigation before a ruling on the merits.

In *Kaplan,* the Second Circuit found that the complaint sufficiently alleged a claim for aiding and abetting under JASTA by, among other things, alleging "that the relevant customers of [the bank] were persons and entities who were in fact integral parts of Hizbollah, and that LCB knew this was so because Hizbollah repeatedly publicized those relationships on Hizbollah websites and in news media that included Hizbollah's own radio and television stations."[12] Notably, the *Kaplan* court rejected the district court's finding that the allegations were insufficient as to general awareness because the customers were not designated by the United States. The court explained that it would "defy common sense" to hold that the only way that a plaintiff could plead general awareness was by alleging that the customers were so designated.

In *Honickman*, however, the court made clear that the inquiry will be case specific and will require courts to determine whether the plaintiffs cite a sufficient number of sources to warrant discovery regarding the defendant's knowledge of the customer's connection to a Foreign Terrorist Organization ("FTO"). The court provided little guidance to lower courts attempting to make this determination, explaining only that the sources cited in the complaint must warrant an inference that the connection between the customer and the FTO were "public knowledge" at the time of the assistance.

District courts in the Second Circuit are now faced with the challenge of deriving governing principles from these decisions as they decide motions to dismiss in other cases alleging claims for secondary liability under JASTA. The outcome of these cases will provide further guidance to financial institutions regarding how to protect against potential litigation and liability.

EUROPEAN UNION

New European Union AML/CFT Legislative Package

In July 2021, the European Commission presented a new legislative package intended to strengthen existing AML/CFT rules stemming from the 5th AML Directive. The package contains four main legislative proposals, which are designed to improve the detection of suspicious transactions and activities and close loopholes used by criminals:

- A Regulation on AML/CFT that will contain directly applicable rules;
- The 6th AML Directive, which will replace Directive 2015/849/EU and will contain new rules applying to national supervisors and Financial Intelligence Units ("FIUs") in Member States;
- A Regulation creating an EU AML/CFT authority ("AMLA"), which will be the central authority coordinating national authorities to ensure a consistent application of EU rules by the private sector. This new AMLA will, in particular, establish a single integrated system of AML/CFT supervision across the European Union, directly supervise some of the riskiest financial institutions, monitor and coordinate national supervisors responsible for other financial entities and nonfinancial entities, and support cooperation among national FIUs; and
- Revision of Regulation 2015/847/EU on Transfers of Funds to trace transfers of crypto-assets.

This new legislative process will entail the creation of a Single EU Rulebook for AML/CFT that will harmonize rules across the European Union, in particular in the areas of customer due diligence, beneficial ownership, and cash payments. For instance, one new rule will set a limit of €10,000 on large cash payments across the European Union.

Regarding crypto-assets, the package also aims to include the entire crypto sector in the scope of EU AML/CFT rules, obliging all service providers to conduct due diligence on their customers, and to prohibit the provision of anonymous crypto-asset wallets.

The European Union will also create a gray list and a black list of countries presenting risks of money laundering and terrorist financing ("ML/TF"), reflecting similar FATF lists. The European Union will use these lists to choose and apply measures proportionate to the risks posed by a given country. Based on an autonomous assessment, the European Union will also be able to include non-FATF listed countries that threaten the European Union's financial system on these two lists.

This legislative package will be discussed by the European Parliament and the Council as part of a speedy legislative process. The future AMLA is expected to be operational in 2024.

EBA Highlights of Key ML/TF Risks Across the European Union

On March 3, 2021, the European Banking Authority ("EBA") published its biennial Opinion on risks of ML/TF affecting the European Union's financial sector. This Opinion is addressed to national competent authorities and contains recommendations to mitigate the identified risks.

In the first part of the Report, the EBA highlights both a number of cross-sectoral ML/TF risks that were identified in its previous Report as well as several new risks. Notably, the EBA identifies an increase in risks arising from virtual currencies, financial services and products provided by fintech companies, weaknesses in counter-terrorist financing systems and controls, de-risking, crowdfunding platforms, and the COVID-19 pandemic.

The second part of the Report contains specific recommendations for members of the banking, financial, and insurance sectors, including credit institutions, payment institutions, electronic money institutions, investment firms, collective investment undertakings/fund managers, and life insurance undertakings.

EBA Consultation on Draft Guidelines for AML/CFT Compliance Officers

On August 2, 2021, the EBA launched a public consultation on new Guidelines for the role, tasks, and responsibilities of AML/CFT compliance officers. The guidelines come in response to reports that existing regulations have not been implemented evenly nor applied effectively throughout the EU financial sector.

In particular, these Guidelines include provisions relating to eligibility requirements of AML/CFT compliance officers, their level of seniority, their powers and overall responsibilities (e.g., preparing policies and procedures, monitoring compliance, conducting customer due diligence, and reporting to the management body) and the role of the management body within the AML/CFT governance framework. These Guidelines, which also contain provisions applicable to groups of companies, will apply to entities falling within the scope of the current AML Directive. The public consultation period ended on November 2, 2021.

FRANCE

New French Order on the System and Internal Controls to Fight ML/TF

In January 2021, a new French Order (*arrêté*) on the system and internal controls to fight money laundering and terrorist financing was published in the Official Journal of the French Republic. This Order replicates some of the provisions of French Order of November 3, 2014, on the internal control of companies in the banking, payment services, and investment services sector subject to the supervision of the Prudential Supervision and Resolution Authority ("ACPR"). The new rule was also created to extend the existing requirements to more entities subject to French AML/CTF rules. This Order, in force since March 1, 2021, also incorporates under French law the obligation to appoint a person in charge of each the permanent control and the periodic control of the AML/CTF system.

Additional requirements relating to the outsourcing of AML/CTF functions were also introduced, including the obligation to inform the ACPR of any outsourcing and the obligation to include mandatory provisions in outsourcing arrangements.

Revised French ACPR Guidelines on Identification, Verification, & Knowledge of Customers

In December 2021, the ACPR published a revised version of its Guidelines on the identification, verification, and knowledge of customers. These revised Guidelines include the provisions of the 5th AML Directive and of the French Order (*arrêté*) of January 6, 2021, on the system and internal controls to fight money laundering and terrorist financing, notably with respect to the verification of the identity of customers and to new obligations relating to the beneficial ownership register.

SPAIN

Amendment Creates New Obligations for Virtual Asset Service Providers

In April 2021, the Council of Ministers amended Law 10/2010 on the prevention of money laundering and terrorist financing ("Spanish AML Act"). Under the amendment, virtual asset service providers ("VASPs") engaging in exchange services between virtual currencies and fiat currencies or wallet custody services are now obliged entities and must register with a newly created Registry at Bank of Spain ("BoS"). This obligation

applies to any VASPs providing any of these services in the Spanish market, either to professional or retail customers, and even if VASPs are not based in Spain.

In practice, this amendment requires any VASP providing services in Spain before April 27, 2021, to have completed registration at the VASP Registry by the end of January 2022. Breach of this registration obligation may trigger penalties of up to €10 million. To register, applicants must submit:

- A report on the honorability of the company and the directors of the company proving absence of criminal records, administrative offenses, or ongoing investigations;
- A copy of the AML Prevention Plan of the company, in the terms provided by BoS and the Spanish AML legislation; and
- A copy of a risk assessment document including the AML policies of the company, also within the terms provided by BoS.

All submissions must be drafted in Spanish, and BoS will have three months to analyze and approve or deny each application.

Further, pursuant to the reformed Spanish AML Act, VASPs are now subject to the Spanish AML legislation and thus will need to be registered at the AML Prevention Service of the Spanish Ministry of Finance, known as SEPBLAC. Among other obligations, VASPs will now be required to conduct KYC activities in accordance with EU legislation, record and monitor transactions, and ensure that the company's staff is trained in AML procedures.

GERMANY

German Crypto-Assets Transfer Regulation

The German Crypto-Assets Transfer Regulation of September 24, 2021. (*Kryptowertetransferverordnung* or "CATR"), in force since October 2021, implements the FATF's Travel Rule and introduces a wide range of enhanced customer due diligence measures aimed at ensuring the complete traceability of crypto-asset transfers.

In essence, the CATR obliges crypto-asset service providers ("CASPs") transferring crypto-assets on behalf of a buyer to transmit information on the name, address, and account number (e.g., public key) of the seller and the name and account number (e.g., public key) of the beneficiary simultaneously and securely to the CASP acting on behalf of the beneficiary. Moreover, the CASP acting on behalf of the beneficiary must ensure that it also receives and properly stores the originator and beneficiary information.

German Transparency Register and Financial Information Act. The Transparency Register and Financial Information Act of June 25, 2021 (*Transparenzregister- und Finanzinformationsgesetz* or "TRFI"), which entered into force in August 2021, amends the existing provisions of the German Anti-Money Laundering Act (*Geldwäschegesetz*). The amendment relates to the identification and verification of beneficial owners as part of the customer due diligence process.

In particular, the TRFI differentiates between the collection of beneficial owner information and its verification by obliged entities. The TRFI prescribes that obliged entities may collect beneficial owner-related information directly from their contract partner or any persons acting on its behalf only and that, at this stage, enquiries with a transparency register are not sufficient for the purpose of complying with the mandatory customer due diligence rules.

As to the verification of any information provided within the customer due diligence process, obliged entities must make enquiries with the transparency register only if they intend to establish a business relationship with a trust or a similar legal structure. In all other cases, they must verify the information by taking risk-based measures.

On October 28, 2021, the Federal Financial Supervisory Authority ("BaFin") published its revised Notes on the Interpretation and Application of the German Anti-Money Laundering Act (*Geldwäschegesetz*), in order to, among other things, reflect the changes introduced by the TRFI and provide clarifications in this respect.

ITALY

Legislative Decree No. 195/2021

Legislative Decree no. 195/2021 ("Decree") was published in the Official Gazette on November 30, 2021. The Decree implements the Directive (EU) 2018/1673 of the European Parliament and of the Council of October 23, 2018, on combating money

laundering by criminal law ("Directive"). The Directive established minimum rules concerning the definition of criminal offenses and sanctions in the area of money laundering.

The Decree entered into force on December 15, 2021, and amends parts of the Italian Criminal Code, including Articles 648 (handling of stolen goods), 648-bis (money laundering), 648-ter (use of money, goods, or benefits of illicit origin), and 648-ter.1 (self-laundering).

The amendments relate to the predicate offences of Art. 648 crimes—the Decree expands these offences to include contraventions and culpable crimes. The Decree has also added the crimes of stolen goods and self-laundering to the list of offences covered under Art. 9, paragraph 4, of the Italian Penal Code. Art. 9 allows for the prosecution of Italian citizens for certain crimes committed abroad, even in the absence of the relative condition of prosecution (e.g., a request by the Minister of Justice).

UNITED ARAB EMIRATES

Newly Established Executive Office of Anti-Money Laundering and Countering the Financing of Terrorism

In February 2021, the UAE Cabinet, chaired by His Highness Mohammed bin Rashid Al Maktoum (Vice President, Prime Minister, and Ruler of Dubai), established an Executive Office of Anti-Money Laundering and Countering the Financing of Terrorism ("Executive Office"). The Executive Office is charged with overseeing implementation of the National AML/CFT Strategy and National Action Plan, a program of reforms designed to bolster the United Arab Emirates' position as a center of international finance. The reforms are further intended to respond to the 2020 Mutual Evaluation Report issued by the FATF, which identified systemic deficiencies in the UAE AML/CFT regulatory framework.

In keeping with its mission, the Executive Office will serve as the primary body coordinating AML/CFT efforts, with responsibilities that include: (i) improving national and international coordination and cooperation on AML/CFT policy and operational issues; (ii) increasing information-sharing between national and international law enforcement agencies and the private sector; and, in conjunction with the Ministry of Foreign Affairs and International Cooperation, or "MoFAIC," and other relevant agencies, (iii) enhancing the United Arab Emirates' existing AML/CFT legislation and regulatory framework.

New Specialized AML/CFT Courts

Following on the creation of specialized AML/CFT courts in several other emirates in late 2020, the Dubai courts, at the directive of His Highness Mohammed bin Rashid Al Maktoum, established a specialized new court that will focus on combatting money laundering and other financial crimes in August 2021. Sitting within the Dubai courts, the new court will have unique jurisdiction over all cases that involve or that appear to involve money laundering and other relevant financial crimes.

Creation of this new court is a clear reflection of Dubai's commitment to enhancing its AML/CFT enforcement framework and an important response to FATF's 2020 Mutual Evaluation Report, which identified prioritizing money laundering enforcement as a "priority action" among its recommendations.

New Official Guidelines

As part of ongoing efforts to enhance the UAE AML/CFT framework, key regulatory bodies issued updated AML/CFT guidelines over the course of the year.

In April 2021, the National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organisations Committee ("NAMLCFTC") (the primary body for policy making and issuing regulations to combat money laundering and terrorism financing) adopted new AML/CFT guidelines for financial institutions and designated nonfinancial businesses, and professions ("DNFBP") (e.g., brokerages, real estate companies, auditors, corporate service providers, law firms, and dealers of precious metals and gemstones). The guidelines are intended to raise awareness on the importance of adhering to anti-money laundering and financial crime legislation and highlight the risks and penalties associated with violations.

At the same time, NAMLCFTC approved six risk assessment reports relating to terrorism financing, trade-based money laundering, misuse of legal persons/abuse of the corporate veil, nonprofit organizations, lawyers, and the gold sector. The objectives of these reports are to identify relevant AML/CFT risks, align legislative and operational frameworks within the United Arab Emirates with existing risks, and enhance

cooperation among regulatory authorities. As such, these reports will be poised to serve as the basis for further legislative and regulatory guidance and reforms.

In June 2021, the UAE Central Bank issued new guidance that, in key part, sets out the Central Bank's expectations for the preparation and submission of SARs and suspicious transaction reports ("STRs")—filed through the goAML integrated digital platform with the Financial Intelligence Unit ("FIU")—and establishes maximum reporting timelines. This new guidance builds upon, and should be read in conjunction with, earlier AML/CFT procedures and guidelines issued by the Central Bank, with current legislation and regulations taking precedence.

As an initial matter, the guidance reminds UAE financial institutions that the obligation to file would be triggered where they have a reasonable suspicion that relevant funds may be related to crime, not only where there is actual knowledge of criminal activity. Moreover, there is no *de minimis* reporting threshold, and the Central Bank mandates reporting not only suspicious transactions but also suspicious activities, with any of the following constituting reportable suspicious activities:

- Customers being subject to adverse media reports;
- Customers refusing to respond, or reluctantly responding, to diligence inquiries at intake;
- Customers being designated on relevant sanctions-related prohibited or restricted parties lists; and
- Customers providing false documentation.

As such, the breadth of potentially reportable transactions and activities is substantial.

Importantly, UAE financial institutions are—and have been—required to report suspicious activities "without delay," with failure to do so triggering criminal sanctions. The new guidance now establishes maximum timelines for identifying and reporting suspicious activities, specifically:

- Within 20 days from an internal suspicious activity alert, an investigator must assess the alert, conduct any investigation that might be warranted, and submit a recommendation to the financial institution's money laundering reporting officer ("MLRO") regarding whether filing a SAR or STR is necessary;
- Within that same period, the MLRO must review the case report, consider the internal filing recommendation, and/or settle the financial institution's approach to the underlying activity; and
- Within an additional 15 days, the MLRO must, if doing so is warranted, file a SAR or STR with the FIU.

That timeline is further reduced where the SAR or STR is triggered by an inquiry from law enforcement, in which case the financial institution must assess and, if warranted, submit a SAR or STR within 24 hours. Notwithstanding these timelines, the guidance recognizes that certain "complex" circumstances may require more extensive assessment, and it provides for longer timelines if the financial institution submits timely notice to the FIU. However, in all cases, the reporting timelines set out in the guidance are intended as *maximum* timelines, with quicker reporting encouraged.

Following on the June 2021 guidance, the Central Bank has also issued further guidance to financial institutions and DNFBPs operating in certain high-risk sectors, including guidance for financial institutions providing services to cash-intensive businesses in September 2021 and guidance for licensed exchange houses in November 2021. Each such guidance sets out detailed diligence expectations for institutions operating in the relevant sector(s) and offers risk mitigation strategies designed to ensure compliance with existing AML/CFT requirements.

Taken as a whole, the AML/CFT guidance issued over the past year highlights the importance of establishing effective internal controls specifically attuned to existing risks as well as increasingly evolving regulatory requirements and expectations.

AUSTRALIA

AUSTRAC Issues Revised Rules to Reflect AML/CTF Act Reforms

On June 15, 2021, the Australian Transaction Reports and Analysis Centre ("AUSTRAC") issued an Instrument[13] that updates the existing AML/CTF Rules[14] to reflect the amendments to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) ("AML/CTF Act") passed by the Australian Parliament in December 2020.

The Instrument amends the AML/CTF Rules to reflect the following reforms to the AML/CTF Act:

- The requirement that financial institutions conduct due diligence assessments before entering into, and for the duration of, any correspondent banking relationship that will involve a vostro account;
- The requirement that a reporting entity complete the applicable customer identification procedures, including verification of identity, before providing any designated service to a customer; and
- The expanded set of circumstances in which a reporting entity may rely on the applicable customer identification procedures undertaken by a third party.

Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021

On December 2, 2021, the Australian Parliament passed the Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021 (Cth) ("Autonomous Sanctions Amendment Act"). The Autonomous Sanctions Amendment Act introduces Magnitsky-style laws into Australia as part of the global movement to impose targeted sanctions on individuals and entities.

Prior to the passage of the Autonomous Sanctions Amendment Act, the Australian sanctions regime contained in the Autonomous Sanctions Act 2011 (Cth) ("Autonomous Sanctions Act") was limited to country-specific sanctions. The Autonomous Sanctions Amendment Act amends the Autonomous Sanctions Act to introduce new "thematic" sanctions based on conduct of concern by individuals or entities, including the proliferation of weapons of mass destruction, threats to international peace and security, malicious cyber activity, serious violations or serious abuses of human rights, activities undermining good governance or the rule of law (including serious corruption), and serious violations of international humanitarian law.

The Autonomous Sanctions Amendment Act establishes a specific decision-making process in relation to thematic sanctions listings. Before making a thematic sanctions listing decision, the Australian Minister for Foreign Affairs is required to consult with and obtain agreement in writing from the Commonwealth Attorney-General to ensure listing decisions take account of all relevant foreign policy and other national interest considerations.

MAINLAND CHINA

Anti-Money Laundering Legislation in China

On June 1, 2021, the People's Bank of China ("PBOC") released the Anti-Money Laundering Law ("Draft Amendments") to seek public comments. The Draft Amendments are expected to be reviewed by the National People's Congress ("NPC") in 2022. On April 15, 2021, PBOC released the Measures for the Supervision and Administration of Combating Money Laundering and Financing for Terrorism by Financial Institutions ("Measures"), which took effect on August 1, 2021. The Measures replaced the prior Measures for the Supervision and Administration of Combating Money Laundering by Financial Institutions (2014) and adopted several major changes. These changes expand the scope of organizations subject to AML requirements to include insurance agents and insurance brokers, loan companies, and nonbanking payment institutions. Further, organizations must utilize a risk-based approach and implement policies, procedures, and internal controls commensurate with the organization's AML/CFT risks.

China Releases Blocking Rules

On January 9, 2021, China's Ministry of Commerce ("MOFCOM") released Rules on Counteracting Unjustified Extra-Territorial Application of Foreign Laws and Other Measures ("Rules"). To implement the Rules, the Chinese government has designated a joint committee called the "Working Mechanism," which will include relevant Chinese ministries and be chaired by MOFCOM. MOFCOM may issue a prohibition order ("Prohibition Order") to the effect that a Foreign Legislation or Measure will not be accepted or observed, after the Working Mechanism has considered the relevant factors. The Rules also provide that where a person complies with foreign laws and measures prohibited by a Prohibition Order, "and thus infringe[s] upon the legitimate rights and interests" of Chinese Persons, the affected Chinese Persons may file a civil lawsuit in the Chinese courts and seek compensation.

China Enacts Anti-Foreign Sanctions Law

On June 10, 2021, the NPC Standing Committee passed the Anti-Foreign Sanctions Law ("ASL") in response to certain

restrictive measures imposed by other countries on Chinese citizens and organizations ("Chinese Persons"). Under the ASL, the Ministry of Foreign Affairs and other relevant ministers of the State Council ("competent ministries") have the discretion to identify, on a new sanctions list named the Countermeasure List ("CL"), any foreign individuals and organizations that are involved in making, deciding, and implementing discriminatory restrictive measures on foreign countries, and other individuals and organizations related to those already identified on the CL, including their spouses and direct lineal family members.

In addition to the new sanctions list, Article 12 sets a broad prohibition on "implementing or assisting in the implementation of discriminatory restrictive measures taken by foreign countries against Chinese citizens and organizations." Importantly, when an organization or individual continues to implement a blocked foreign discriminatory restrictive measure, the ASL allows Chinese Persons to "institute a lawsuit with the Chinese courts in accordance with the law, requesting the said organization or individual to cease the infringement and compensate for the losses."

China's New Data Laws Restrict Cross-Border Data Transfers

China's new Data Security Law ("DSL"), which became effective on September 1, 2021, imposes certain restrictions on a company's ability to transfer data out of China without the prior approval of Chinese authorities. Article 36 of the DSL provides that organizations and individuals in China, including multinational companies with operations in China, must seek approval from competent Chinese authorities in connection with providing data stored in China to any foreign judicial or law enforcement authority.

Similarly, the new Personal Information Protection Law ("PIPL"), which took effect on November 1, 2021, provides that personal information processors must seek approval from competent Chinese authorities in connection with providing personal information stored in China to any foreign judicial or law enforcement authority. In addition, the PIPL also sets a number of procedural restrictions in the context of transferring data outside of China even if the transfer is not in response to an information request from foreign judicial or law enforcement authority.

These restrictions have the potential to further complicate companies' compliance efforts regarding anti-money laundering.

CROSS-BORDER

On October 14, 2021, the G7 published 13 guiding principles for countries planning to implement central bank digital currencies ("CBDCs"). Although no G7 member has yet issued a CBDC, the report discusses generally applicable public policy considerations. Principle 6 addresses illicit finance, suggesting that "[a]ny CBDC needs to carefully integrate the need for faster, more accessible, safer and cheaper payments with a commitment to mitigate their use in facilitating crime."[15] Principle 6 further recommends that all members in a "CBDC ecosystem," including private-sector entities, have clearly defined roles and responsibilities for AML/CFT. The guidance also discussed important considerations for balancing these objectives—specifically the need to prevent illicit finance without compromising user privacy or inclusion.

On October 28, 2021, the FATF published updated guidance on virtual assets and VASPs. The publication builds on prior guidance issued by the FATF in 2018 and 2019 regarding AML risks and other issues raised by virtual assets. In summary, the FATF's updated October 2021 guidance: (i) clarifies what FATF refers to as "expansive"[16] definitions for virtual assets and VASPs; (ii) explains in further detail how FATF standards apply to stablecoins; (iii) addresses how countries should approach unique AML risks presented by peer-to-peer virtual asset transactions not conducted on an intermediated exchange; (iv) updates guidance regarding licensing and registration requirements for VASPs; and (v) discusses information sharing and cooperation standards for regulatory authorities that supervise VASPs in each country. The FATF's publication also provides further guidance regarding application of the "Travel Rule" to virtual assets and VASPs. This update comes as FinCEN's October 2020 proposed amendments to the United States' Travel Rule—which, among other things, clarify the rule's application to virtual assets and VASPs—remain pending.[17]

SANCTIONS

Expanded Scope: New Geographies and Sectors

In the United States, geopolitical developments in 2021 brought continued sanctions focus on Russia, China, and Hong Kong, and a renewed focus on Belarus and Burma. The new administration continued to devote attention to the perceived increase in civil–military fusion in China, while ongoing sanctions-related negotiations with Iran provided few regulatory developments.

In 2021 OFAC also entered new territory with its first-ever designation of a virtual currency exchange. In addition, in late 2020 and early 2021, OFAC entered into settlement agreements with two digital wallet companies relating to the failure of such companies to prevent users located in comprehensively sanctioned countries from accessing the companies' products and services.

Hong Kong Business Advisory

On July 16, 2021, the U.S. Departments of State, Commerce, Homeland Security, and the Treasury jointly issued a business advisory highlighting risks associated with actions taken by the Chinese Government and the Government of the Hong Kong Special Administrative Region ("SAR"), a global financial hub, with the potential to "adversely impact" U.S. companies operating in the Hong Kong SAR ("Business Advisory"). U.S. entities with significant or strategic operations in Hong Kong should review the Business Advisory as well as the Hong Kong-related sanctions and, if appropriate, prepare contingency or business disruption plans that consider the possibility of key business partners, financiers, or customers becoming the subject of sanctions.

AUTHORS

Sean T. Boyce
Dubai
+971.4.709.8416
sboyce@jonesday.com

Steven T. Cottreau
Washington
+1.202.879.5572
scottreau@jonesday.com

Michael R. Fischer
Frankfurt
+49.69.9726.3943
mrfischer@jonesday.com

Marco Frattini
Milan
+39.02.7645.4001
mfrattini@jonesday.com

James E. Gauch
Washington
+1.202.879.3880
jegauch@jonesday.com

Patrizia Gioiosa
Milan
+39.02.7645.4001
pgioiosa@jonesday.com

Philippe Goutay
Paris
33.1.56.59.39.39
pgoutay@jonesday.com

Fahad A. Habib
San Francisco
+1.415.875.5761
fahabib@jonesday.com

Henry Klehm III
New York
+1.212.326.3706
hklehm@jonesday.com

Tim L'Estrange
Melbourne
+61.3.9101.6820
tlestrange@jonesday.com

Iván Martín-Barbón
Madrid
+34.91.520.3939
imartinbarbon@jonesday.com

Daniel Moloney
Melbourne
+61.3.9101.6828
dmoloney@jonesday.com

Brian C. Rabbitt
Washington
+1.202.879.3866
brabbitt@jonesday.com

Ronald W. Sharpe
Washington
+1.202.879.3618
rsharpe@jonesday.com

Francesco Squerzoni
Milan
+39.02.7645.4001
fsquerzoni@jonesday.com

Jayant W. Tambe
New York
+1.212.326.3604
jtambe@jonesday.com

Vinicio Trombetti
Milan
+39.02.7645.4001
vtrombetti@jonesday.com

Qiang Xue
Beijing
+86.10.5866.1111
qxue@jonesday.com

ADDITIONAL CONTACTS

Brett P. Barragate
New York
+1.212.326.3446
bpbarragate@jonesday.com

Mark A. Biggar
Cleveland
+1.216.586.7023
mbiggar@jonesday.com

Amy H. Burkart
Boston
+1.617.449.6836
aburkart@jonesday.com

Michael R. Butowsky
New York
+1.212.326.8375
mrbutowsky@jonesday.com

Kelly A. Carrero
New York
+1.212.326.8391
kacarrero@jonesday.com

Sophie Chevallier
Paris
+33.1.56.59.46.83
schevallier@jonesday.com

Michael P. Conway
Chicago
+1.312.269.4145
mconway@jonesday.com

Roman E. Darmer
Irvine
+1.949.553.7581
rdarmer@jonesday.com

Robert J. Graves
Chicago
+1.312.269.4356
rjgraves@jonesday.com

Frédéric Gros
Paris
+33.1.56.59.38.32
fgros@jonesday.com

James T. Kitchen
Pittsburgh
+1.412.394.7272
jkitchen@jonesday.com

Aidan Lawes
London
+44.20.7039.5700
alawes@jonesday.com

Florian Lechner
Frankfurt
+49.69.9726.3939
flechner@jonesday.com

Claudia Leyendecker
Düsseldorf
+49.211.5406.5500
cleyendecker@jonesday.com

James P. Loonam
New York
+1.212.326.3808
jloonam@jonesday.com

Locke R. McMurray
New York
+1.212.326.3774
lmcmurray@jonesday.com

Edward J. Nalbantian
London / Paris
+44.20.7039.5145 / +33.1.56.59.39.23
enalbantian@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Jessica L. Panza
Chicago
+1.312.269.4365
jpanza@jonesday.com

Jeff Rabkin
San Francisco / Silicon Valley
+1.415.875.5850 / +1.650.739.3954
jrabkin@jonesday.com

Richard M. Rosenblatt
Atlanta
+1.404.581.8695
rmrosenblatt@jonesday.com

Andrew L. Rotenberg
London
+44.20.7039.5159
arotenberg@jonesday.com

Lauri W. Sawyer
New York
+1.212.326.3898
lwsawyer@jonesday.com

Eric Snyder
Washington / New York
+1.202.879.3912 / +1.212.326.3435
esnyder@jonesday.com

Neal J. Stephens
Silicon Valley
+1.650.687.4135
nstephens@jonesday.com

Harriet Territt
London
+44.20.7039.5709
hterritt@jonesday.com

Rick van 't Hullenaar
Amsterdam
+31.20.305.4223
rvanthullenaar@jonesday.com

Ben Witherall
Singapore
+65.6233.5532
bwitherall@jonesday.com

The following lawyers assisted in the preparation of this White Paper*: Matthew C. Enriquez, Emily Goldberg Knox, Nikolay S. Kutsarov, Zoë Lensing, Rachel G. Miller, Stephanie M. Pryor, Isabel G. Roney, Matthew Rubenstein, Charles Smith, Juan Antonio Solis, David Wu, and law clerks Leah Murphy, Roger Lu, and Alexander J. Gonzalez.*

ENDNOTES

1 Review of Bank Secrecy Act Regulations and Guidance, 86 Fed. Reg. R 71201 (Dec. 15, 2021).

2 President's Working Group on Financial Markets *et al.*, *Report on Stablecoins* 19 (2021).

3 FinCEN, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* 1-2 (2021).

4 Press Release, Bd. of Governors of the Fed. Rsrv. *et al.*, "Joint Statement on Crypto-Asset Policy Sprint Initiative 1" (Nov. 23, 2021).

5 Press Release, Dep't of Just., "Deputy Attorney General Lisa O. Monaco Announces Cryptocurrency Enforcement Team" (Oct. 6, 2021).

6 Robinhood Mkts., Inc., Prospectus (Form S-1/A) (July 19, 2021).

7 Office of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Dec. 15, 2021).

8 Office of Foreign Assets Control, "Frequently Asked Questions" (Dec. 15, 2021).

9 18 U.S.C. § 2333(d)(2).

10 *Linde v. Arab Bank, PLC*, 882 F.3d 314, 329 (2d Cir. 2018) (quotation marks omitted) (quoting *Halberstam v. Welch*, 705 F.2d 472, 487 (D.C. Cir. 1983)).

11 *Linde v. Arab Bank, PLC*, 882 F.3d 314, 329 (2d Cir. 2018); *Siegel v. HSBC North America Holdings*, 933 F.3d 217 (2d Cir. 2019).

12 *Kaplan,* at 862.

13 *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument* 2021 (No 1) (Cth).

14 *Anti-Money Laundering and Counter-Terrorism Financing Rules* 2007 (No 1) (Cth).

15 G7, Public Policy Principles for Retail Central Bank Digital Currencies ("CBDCs") 10 (2021).

16 Financial Action Task Force, Virtual Assets and Virtual Asset Service Providers 5 (2021).

17 Threshold for the Requirement to Transmit Information on Funds Transfers and Transmittals of Funds that Begin or End Outside the United States, and Clarification of the Requirement to Transmit Information on Transactions Involving CVCs and Digital Assets, 85 Fed. Reg. 68,005 (proposed Oct. 27, 2020) (to be codified at 31 C.F.R. pt. 1010).