JONES DAY | One Firm Worldwide®

WHITE PAPER

January 2021

2020 Anti-Money Laundering Year in Review

2020 witnessed a flurry of anti-money laundering activity, with the issues and developments continuing to be global in scope. In the United States, suspicious activity reports, outlining transactions involving terrorism finance or other illegal activity, were leaked to the public. This sparked questions into the effectiveness of current anti-money laundering regime and suspicious activity report filing.

In the European Union, an action plan to prevent money laundering and terrorist financing was proposed, foreshadowing increased enforcement action and further regulation. The European Union also adopted a global human rights sanctions regime, highlighting the need for appropriate safeguards in compliance frameworks.

In Hong Kong, the test to determine the reasonableness of a person's belief regarding legitimacy of sources of funds was reformulated. Last year also witnessed multiple public pronouncements and penalties imposed in Singapore regarding anti-money laundering and countering the financing of terrorism, forcing companies to look into their compliance programs and the quality of their execution.

This Year in Review focuses on these developments as well as highlights other key trends in the sanctions and anti-money laundering arena from a global perspective. This Year in Review also provides insight into potential anti-money laundering and what these issues mean for financial institutions, and offers an outlook for the year ahead.

TABLE OF CONTENTS

UNITED STATES

Passage of the Anti-Money Laundering Act of 2020

Congress passed the National Defense Authorization Act ("NDAA"), which includes the Anti-Money Laundering Act of 2020 ("AMLA"), in December 2020.[1] Over a presidential veto, the Senate enacted the legislation. The AMLA is the first overhaul of U.S. anti-money laundering laws since the USA PATRIOT Act of 2001. It includes new reporting requirements for financial institutions and tasks regulators with reviewing and streamlining existing reporting requirements. Additionally, it creates new fines and penalties for violators of the Bank Secrecy Act ("BSA"), as well as new means for the public to cooperate with law enforcement.

The AMLA's 236 pages also include many other provisions that could be relevant to individual market participants. For example, it creates a whistleblower program for the Treasury. The AMLA also creates a Treasury Attaché program in the U.S. embassies to maintain relationships with non-U.S. counterparts abroad and establishes Financial Crimes Enforcement Network ("FinCEN") liaisons to maintain relationships with BSA officers and foreign counterparts, coordinate consistent supervisory guidance, and propose changes to regulations. The AMLA creates a pilot program for sharing of suspicious activity reports ("SARs") with financial institutions' foreign branches, subsidiaries, and affiliates, except those in China, Russia, and certain other jurisdictions. The AMLA also directs FinCEN to create and maintain a secure ultimate beneficial owner registry of legal entities.

Some other sections of the Act worth highlighting are Section 6002, which affirms risk-based programs but also establishes a "national priority" template for compliance. Section 6102 clarifies that virtual currency is within FinCEN's scope. Section 6305 establishes a mechanism for "no-action" relief by FinCEN. Section 6306 amends Section 5332 to codify a safe harbor for maintaining open accounts at the request of law enforcement. Section 6315 significantly toughens sanctions on Source of Wealth/Funds inquiry via stricter penalties. It remains to be seen how regulators will use the AMLA's legislative grants of authority to pursue further rulemaking related to anti-money laundering.

Correspondent Banking Issues and the Anti-Money Laundering Act of 2020

The sheer scope and breadth of the AMLA has gained considerable attention. One important aspect of the AMLA, however, seems to be flying under the radar: its expanded subpoena power over correspondent banking. Specifically, the new provisions significantly expand the U.S. government's subpoena and seizure powers, which will have a profound impact on foreign banks that maintain correspondent accounts in the United States.

There are three aspects of the change that are worth highlighting:

- First, Section 6308 expands the U.S. government's subpoena authority with respect to foreign banks with U.S. correspondent accounts to include "any records relating to the correspondent account or any account at the foreign bank," provided that such records are the subject of certain types of investigations or civil forfeiture action. The wording is much broader than the authority provided under the USA PATRIOT Act, or 31 U.S.C. § 5318(k)(3), which permits subpoena of records related to such correspondent account only. Noncompliance with any subpoena could potentially lead to the bank losing its access to the U.S. financial system.

- Second, the Act explicitly addresses foreign banks' potential objection to the subpoenas: conflicts with foreign secrecy or confidentiality law cannot be the sole basis to modify or quash such subpoenas

- Third, the U.S. government is permitted to serve a foreign bank's representative office in the United States by mail or fax, certainly not the most onerous standard.

Presumably, foreign banks may still be able to rely on constitutional due process defenses to challenge AML Act subpoenas. A potentially instructive case is Judge Engelmayer's pre-AMLA decision in *Vasquez v. Hong Kong & Shanghai Banking Corp., Ltd.*, No. 18 CIV. 1876 (PAE), 2020 WL 4586729 (S.D.N.Y. Aug. 10, 2020). There, Judge Engelmayer held that a nonresident bank's use of a New York-based correspondent bank account does not in itself constitute purposeful availment by the bank sufficient to confer personal jurisdiction under New York's long-arm statute. The court was focused on the directional arrow of the transfer and the correspondent bank's passive role in receiving the wire transfer.

COVID-19 Pronouncements From FinCEN and NYDFS

Faced with unprecedented challenges to AML compliance in the work-from-home era, the FinCEN began in March and April 2020 to release notices to financial institutions regarding the impact of the COVID-19 pandemic on BSA and anti-money laundering obligations. Varying from customer identification guidance to regularity of board of directors meetings reviewing AML processes, FinCEN recognized that financial institutions may face reasonable delays in meeting BSA obligations. This indicated that FinCEN expected to be contacted by financial institutions that are likely to be delayed in filing SARs and encouraged financial institutions to evaluate and responsibly implement innovative approaches to meet such obligations. The notice also explained that Paycheck Protection Program ("PPP") loans made to existing customers would not require re-verification under the BSA, unless the financial institution's compliance program required such re-verification. The notices emphasized that the need for risk-based compliance with the BSA remained otherwise unaltered. Since March 2020, the New York Department of Financial Services ("NYDFS") has similarly released administrative accommodation guidance for financial institutions related to the COVID-19 pandemic.

FinCEN also published advisories on illicit conduct prevalent in the pandemic response and noted potential indicators of cybercrime, cyber-enabled crime, and consumer fraud observed during the COVID-19 pandemic. In July 2020, FinCEN advised financial institutions to be aware of remote identity process risks, including digital manipulation of identity documentation, as well as phishing scams referencing payments related to the CARES Act and business email compromise schemes that try to convince companies to redirect payments to new accounts using pandemic-related changes in business operations as the reason. FinCEN also advised financial institutions to be aware of imposter scams, where the actor poses as an official or representative from the IRS or CDC to coerce the target to provide funds or information, and money mule schemes. As ever, FinCEN emphasized that SAR reporting in conjunction with due diligence is crucial to identifying and stopping these financial crimes.

FinCEN Advisories and Warnings Regarding Technology Risks, Human Trafficking Red Flags, and Jurisdictional Deficiencies

In September 2020, FinCEN warned banks about their crypto exposure and the risks associated with virtual currency. FinCEN warned that examiners will be looking into banks' policies and procedures to mitigate risk. In October 2020, FinCEN issued an advisory to alert financial institutions to trends and indicators of ransomware and associated money-laundering activities. FinCEN stated that there has been an increase in encrypting system files and demanding ransom, ransom payment demanded in the form of bitcoin, and "fileless" ransomware that is written into the computer's memory as opposed to into a file on the hard drive. FinCEN advised financial institutions to remain diligent and cautious of ransomware attacks, including raising the notion that payment of ransom may generate its own AML consequences.

FinCEN also issued, in October 2020, an advisory to supplement the "2014 FinCEN Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking—Financial Red Flags." The supplemental advisory listed the four typologies of human trafficking and behavioral indicators of victims of human trafficking that should be incorporated in SAR filings. It also noted that the identifying and verifying of beneficial owners of legal entities, as required by the FinCEN Customer Due Diligence Rule, information sharing among financial institutions, and the filing of SARs could help combat human smuggling and trafficking.

FinCEN also issued multiple advisories this year regarding the Financial Action Task Force's list of jurisdictions with strategic deficiencies. These jurisdictions were, as of November 2020: Albania, The Bahamas, Barbados, Botswana, Burma (Myanmar), Cambodia, Ghana, Jamaica, Mauritius, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen, and Zimbabwe. This jurisdiction list may affect U.S. financial institutions' obligations and risk-based approaches with respect to the relevant jurisdictions.

FinCEN and Federal Banking Agencies' BSA Enforcement Statements

On August 18, 2020, FinCEN issued guidance clarifying its approach to enforcement actions for BSA violations. The guidance sought to provide transparency into FinCEN's considerations and deliberations when it identifies potential violations of the BSA.

BSA obligations generally apply only to financial institutions, such as commercial banks, credit unions, broker-dealers, and pawnbrokers, among several others. However, nonfinancial trades or businesses may also be subject to BSA requirements,

albeit in more limited circumstances. FinCEN's enforcement powers reach both financial institutions and nonfinancial trades or businesses, and may take several forms. FinCEN may issue a warning letter; seek equitable remedies, settlements, or civil money penalties; refer the matter to a law enforcement agency; or take no action at all in response to a BSA violation. In deciding whether to take any such action, FinCEN considers the extent to which the entity complied with specific BSA obligations as well as the adequacy of its AML program. Some of the factors involved in this deliberation include: the nature, seriousness, impact, and pervasiveness of the violation; history of similar violations; financial gain or other benefit resulting from the violation; actions taken to remedy and disclose the violation; and the quality and extent of cooperation with FinCEN.

In May 2020, FinCEN continued its use of Geographic Targeting Orders, requiring the collection and reporting of information on residential real estate transactions in the amount of $300,000 or more in various counties of nine states, including California, Illinois, and New York.

Leak of the FinCEN Files

In September 2020, a large number of SARs were made public, following a 2019 leak from the U.S. Treasury Department's FinCEN intelligence unit. The so-called "FinCEN Files" comprise more than 2,600 documents largely consisting of privileged SAR communications between banks and U.S. authorities. Under many national money laundering systems, banks and regulated institutions are required to file SARs when they identify suspicious transactions or conduct that could be indicators of money laundering or terrorist financing activity. The filing of a SAR is not necessarily indicative of any wrongdoing or illegal activity, and the standard of suspicion that triggers a filing is—by design—generally low. The aim of SAR regimes is to provide key intelligence to regulatory and criminal authorities, as banks themselves are not equipped to investigate these matters beyond the early-warning SAR stage. However, the scale and nature of the transactions identified in the leaked SARs has raised public questions about the adequacy of international anti-money laundering and anti-terrorist financing regimes.

The SARs in the FinCEN Files are dated between 1999–2017 and reflect only a small proportion of total SARs filed in this period. The leak is significant because generally financial institutions must keep SARs confidential, and SARs, unless leaked, are not subject to public view. The leaked documents show payment flows of more than US$2 trillion through international banking networks, which were considered to be suspicious by one or more of the involved financial institutions. The SARs relate to various types of suspicious activity, including transactions involving suspected money laundering, terrorism finance, sanctions evasion, organized crime, and financial fraud. The leak also raises questions about the speed with which transactions are being reported and the quality of the information provided to regulators in SAR filings.

Several national and global AML regulators reacted to the leak of the files by urging broader global adoption of the Warsaw Convention, which requires national financial intelligence units to honor overseas requests to halt suspicious transactions at an earlier stage and prevent criminal exploitation of the global financial system. Such adoption of the Convention would require local banks to review any client relationships with counterparties identified in the SARs as well as reminding regulated institutions of their SAR filing obligations. FinCen also noted that the unauthorized disclosure of SARs filed in the United States is a national security-related crime.

It remains to be seen how the leak of the FinCEN Files will impact on global payment flows and bank behavior. It is likely that the number of SARs filed (in countries which have this reporting obligation) will increase and that regulators will increasingly focus on the quality and speed of reporting by financial institutions.

FinCEN's Safe Harbor Protections for Institutions Reporting Information

On December 10, 2020, FinCEN introduced via a new Fact Sheet guidance on Section 314(b) of the USA PATRIOT Act. Section 314(b) grants institutions safe harbor from civil liability when reporting information to one another related to money laundering and terrorist activity. The Fact Sheet rescinds earlier guidance (FIN-2009-G002) and an administrative ruling (FIN-2012-R006), while expanding protections that create additional information-sharing opportunities for institutions.

The FinCEN Fact Sheet also includes a broader range of protected information that institutions may share and provides that institutions only need a "reasonable basis" to believe that the suspicious activity relates to money laundering or terrorist activity. The Fact Sheet states that there is no prohibition

on sharing personally identifiable information, nor is there any required format on the medium that institutions may use to share information. The Fact Sheet also expands the types of entities eligible for Section 314(b) safe harbor, by including nonfinancial institutions that operate associations of financial institutions that may now participate in the information-sharing program—e.g., compliance service providers. In addition, unincorporated associations governed by contract, among a group of financial institutions, are also eligible for safe harbor.

Although institutions are not required to participate under Section 314(b), FinCEN strongly encourages information sharing. Participating entities should register with FinCEN's Secure Information Sharing System and reference FinCEN's user guides to learn the mechanics of the reporting process.

FinCEN's Proposed Rules Regarding AML Effectiveness and Wire Thresholds

Apart from the AMLA, in September 2020, FinCEN proposed new rulemaking seeking to establish that all covered financial institutions subject to an anti-money laundering program requirement must maintain an "effective and reasonably designed" anti-money laundering program, including processes to report information that has a "high degree of usefulness" to government authorities. The proposal also included amendments to streamline SARs on continuing activity, enhance information-sharing mechanisms, and communicate national AML priorities, among other potential amendments.

This proposed rule seeks to reform many different aspects of a financial institution's anti-money laundering programs by defining national AML priorities and creating a regulatory expectation of resource allocation by institutions to address those priorities.

Commentators have suggested that the setting of national priorities may impinge on any particular bank's risk-tailored approach and force "tick the box" compliance rather than strengthening risk-based efforts. Additionally, absent further clarification, many have suggested that the "high degree of usefulness" definition, while laudable, is ineffective guidance and should be supplemented with more targeted guidance. How this complements the AMLA is a big question for 2021.

In October 2020, FinCEN, the Federal Reserve Board, and the Department of the Treasury proposed a rule to reduce the threshold for when financial institutions are required to collect and retain information on fund transfers and transmittal of funds. The proposed rule would reduce the threshold from $3,000 to $250 for fund transfers and transmittals of funds that begin or end outside the United States The proposed rule would also clarify the meaning of "money" as used in these same rules to ensure that the rules apply to domestic and cross-border transactions, involving convertible virtual currency. The proposed rule would clarify that these rules apply to domestic and cross-border transactions involving digital assets that have legal tender status.

Commentators have suggested that the proposed rule unfairly targets cross-border transactions and that without evidence-based relation to actual improper conduct would needlessly increase compliance costs at international banks without targeting specific risk-based misconduct. These proposed rules are open to comment and have yet to be finalized.

FinCEN's Clarification of Due Diligence Expectations for Charities and Nonprofit Customers and Encouragement of Innovative Technology Adaptation to Combat Money Laundering

In November 2020, FinCEN, in coordination with the federal banking agencies, released a fact sheet clarifying BSA due diligence expectations for charities and nonprofit customers. The fact sheet highlighted the importance for banks to ensure their customers can transmit funds through legitimate and transparent channels during the COVID-19 pandemic. The fact sheet also reminded banks to apply a risk-based approach to customer due diligence requirements for these charities and nonprofit organization customers.

In December 2020, FinCEN further released a statement encouraging banks and credit unions to use innovative approaches, such as adapting new technologies, in order to combat money laundering and terrorism financing. Notably, FinCEN stated that financial institutions will need to adapt their efforts to the ever-evolving tactics of money launderers and other illicit actors.

Federal Regulatory Agencies' Issuance of Hemp/Cannabis Guidance and Supervisory Guidance Codification

In June 2020, FinCEN issued guidance for financial institutions offering services to medical-marijuana and hemp-related

businesses. The guidance outlined how financial institutions can conduct due diligence and the type of information and documentation to be collected to comply with Bank Secrecy Act requirements. The guidance clarified that financial institutions must conduct customer due diligence and collect basic identifying information for all customers, including hemp-related businesses. The guidance also stated examples of suspicious activity to be mindful of for hemp-related businesses, including hemp production in a jurisdiction where hemp production remains illegal, the customer appears to use the hemp-related business as a front to launder money, or the customer attempts to conceal involvement in marijuana-related business activity. Going forward, the issue of how a financial institution deals with hemp-related businesses may become more prevalent as more states debate the legality of marijuana and cannabis products.

In November 2020, the Office of the Comptroller of the Currency, Federal Reserve Board, Federal Deposit Insurance Corporation, National Credit Union Administration, and Bureau of Consumer Financial Protection proposed regulation that would codify the Interagency Statement Clarifying the Role of Supervisory Guidance, published in September 2018. The Interagency Statement provided that supervisory guidance does not create binding, legal obligations. Supervisory guidance includes interagency statements, advisories, bulletins, policy statements, questions and answers, and frequently asked questions. The Interagency Statement clarified that this supervisory guidance can contain examples the agencies generally consider consistent with safety-and-soundness standards, but the guidance is not an enforceable legal obligation. The proposed regulation seeks to codify this use of supervisory guidance and become binding on the agencies. The proposed regulation could help ease the compliance burden on financial institutions and lessen regulatory uncertainty. However, the proposed regulation could also open the door to confusion regarding the role of guidance as a source of examination deficiency, which was specifically preserved by the Interagency Statement.

AUSTRALIA

Settlement of AUSTRAC Proceeding Against Westpac Banking Corporation

In November 2019, the Australian Transaction Reports and Analysis Centre ("AUSTRAC") issued civil penalty proceedings against Westpac Banking Corporation alleging that it had breached the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 ("AML/CTF Act") on more than 23 million occasions. These breaches included: (i) failing to report International Funds Transfer Instructions on more than 19.5 million occasions; (ii) failing to appropriately assess and monitor AML/CTF risks associated with the movement of money into and out of Australia through its correspondent banking relationships; (iii) failing to maintain an AML/CTF Program in accordance with the AML/CTF Act; and (iv) failing to carry out appropriate customer due diligence including in relation to suspicious transactions associated with possible child sex exploitation in South East Asia. On September 24, 2020, AUSTRAC and Westpac announced that they had agreed to settle the proceedings, with Westpac agreeing to pay a penalty of $1.3 billion.

This is the largest civil penalty of any kind in Australian corporate history. The settlement of the AUSTRAC proceedings against Westpac underlines the significant financial risks for corporations operating in Australia that do not have effective AML/CTF controls and reporting procedures. The Australian Federal Government has provided a $104 million funding boost and an additional 67 new staff to AUSTRAC in their 2020/2021 budget. Financial institutions should review their AML/CTF controls and reporting procedures to ensure they are in compliance.

Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020

The Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020 ("AML/CTF Amendment Act") was passed on December 17, 2020. The AML/CTF Amendment Act amends the AML/CTF Act to introduce a range of measures to strengthen Australia's capabilities to address AML/CTF risk, including by reforming requirements relating to correspondent banking. The AML/CTF Amendment Act introduces a prohibition on financial institutions from entering into a correspondent banking relationship with a financial institution that permits its accounts to be used by a shell bank—banks with no physical presence in their country of incorporation. Further, the AML/CTF Amendment Act imposes a requirement on reporting entities (generally entities that provide financial, gambling, bullion, or digital currency exchange services, as listed in the AML/CTF Act) to conduct due diligence assessments upon entry into and throughout the life

of correspondent banking relationships (replacing the current requirement to undertake a preliminary risk assessment, which then informs whether a due diligence assessment is necessary). This increased burden has been justified on the basis that correspondent banking relationships are vulnerable to AML/CTF risk, particularly when reporting entities are in correspondent banking relationships with institutions located in jurisdictions with weak AML/CTF laws.

The AML/CTF Amendment Act also provides efficiencies for reporting entities, including by expanding the circumstances in which reporting entities may rely on customer identification and verification procedures undertaken by third parties such as other reporting entities or foreign entities (subject to appropriate AML/CTF regulation and supervision).

The changes to correspondent banking and identification procedures, which are introduced by the AML/CTF Amendment Act, come into effect by June 18, 2021, unless proclaimed earlier.

UNITED KINGDOM, EUROPEAN UNION, MIDDLE EAST

European Union Action Plan on Preventing Money Laundering and Terrorist Financing

In May 2020, the European Commission proposed an action plan to intensify the fight against money laundering and terrorist financing. The plan builds on certain key pillars: (i) effective implementation of existing rules; (ii) a single EU rule book on AML/CTF; (iii) bringing about EU-level supervision; (iv) a support and cooperation mechanism for financial intelligence units; and (v) enforcing EU-level criminal law provisions.

The Commission aims to put in place a system of harmonized standards and to establish an EU-level supervisory entity working in close cooperation with the relevant local, i.e., state-level, supervisory authorities. The single rulebook is intended to address the many divergences across EU Member States of the implementation of the current AML framework.

It is expected that an EU-level supervisory entity will further the Commission's efforts to promote harmonization and prevent supervisory fragmentation. While this new supervisor will have the ability to review internal policies and controls of supervised entities to ensure effective implementation, as of now, the debate as to the scope of this entity's remit is continuing. It could include supervision both within and outside the financial sector but may be limited to monitoring risks in financial institutions. We expect that its creation will result in increased enforcement actions.

Beneficial Ownership Disclosure

Corporates need to be aware of recently expanded ownership disclosure obligations. The fourth Anti-Money Laundering Directive[2] further calibrated the framework for beneficial ownership disclosure. Particularly, it requires legal entities—corporations and partnerships—to provide the relevant ownership disclosure registry with relevant information on their beneficial owners.

In general, the pertinent rules, as transposed into Member State law, require corporations to disclose their beneficial owners, i.e., natural persons who: (i) directly or indirectly (a) hold more than 25% capital interest in the corporation or (b) control more than 25% of the voting rights; or (ii) exercise control over the corporation in a comparable fashion.

In ownership structures where corporate entities are shareholders of corporations, on the level of the immediate corporate shareholder, the decisive factor to determine beneficial owner status is the exercise of "controlling influence" by a natural person. To determine these, including in multi-tier structures, legal entities need to be aware that they have to request the required information from their beneficial owners and known holders of capital interests.

Consequently, corporates should consider properly documenting such information requests, including any responses thereto. This will provide valuable evidence in connection with any potential examination or enforcement proceeding relating to compliance with the transparency rules. Breaches are subject to significant fines.

European Union Banks' Joint Transaction-Monitoring and Information-Exchange Initiative

In order to improve the effective monitoring of suspicious transactions in the Netherlands, five prominent Netherlands-based banks (ABN AMRO, ING, Rabobank, Triodos, and the Volksbank) have set up a collective transaction-monitoring initiative, Transaction Monitoring Netherlands ("TMNL"). The initiative, formally established in July 2020, will function as an

addition to the banks' individual transaction-monitoring activities. Its aim is to provide a better and more complete overview of unusual patterns in payment traffic than individual banks can identify. TMNL will receive encrypted information on incoming and outgoing payment transactions of the participating banks and will monitor those transactions collectively. If TMNL detects suspicious activity, it will notify the concerning bank(s), which in turn can file a SAR with the Dutch Financial Intelligence Unit. TMNL will start its phased monitoring of transactions in the upcoming months, and it expects to be able to share first results with the participating banks in the first half of 2021. TMNL will start with the monitoring of commercial transactions. It is still unknown if and when transactions of private clients will be the subject of joint monitoring by TMNL.

Similar initiatives have also been taken up in other jurisdictions. In Sweden, the five biggest banks have created the Swedish Anti-Money Laundering Initiative, SAMLIT, with the aim of easily sharing information on methods, suspicious transaction patterns, and new types of crime with each other and the National Financial Police. The initiative started as a pilot project in May 2020, with the goal of being fully launched in 2021. In Belgium, the banking sector is calling for similar initiatives. At a national parliamentary hearing on the FinCEN Files in November 2020, Belgium's largest banks (BNP Paribas Fortis, Belfius, ING, and KBC) and Febelfin (the Belgian federation of the financial sector) requested the legislator to adopt a legal framework allowing an intra-bank sharing platform but also asked for a greater cooperation with the CTIF-CIF (the Belgian Financial Intelligence Processing Unit). Earlier this year, these banks have developed "Kube," a blockchain-based program in which relevant Know Your Customer information, such as the composition of the board of directors, the articles of incorporation, and the authorized capital, is shared automatically.

ASIA-PACIFIC

China

Anti-Money Laundering Measures in China

On September 15, 2020, the People's Bank of China ("PBOC") released Implementing Measures for Protecting Financial Consumers' Rights and Interests ("Implementing Measures"),[3] which aim to regulate the conduct of financial institutions and protect customers' data and privacy. The Implementing Measures try to strike a balance between protection of customers' rights and AML-related requirements. For example, Article 29 (2) provides that when financial customers are unable or refuse to provide necessary information for financial institutions to conduct an AML background check, the latter may take restrictive measures against relevant customers according to China's Anti-Money Laundering Law ("AMLL") and refuse to provide financial services.

Another major AML development involves PBOC's ongoing efforts to modernize the AMLL, which initially took effect on January 1, 2007. According to PBOC, modernization of the AMLL will be centered on, among others, expanding criminal sanctions, detailing administrative regulation rules, and introducing stricter regulatory measures against beneficiaries of money laundering violations. PBOC will release a draft to seek public comments in the near future.

China's Provisions on the Unreliable Entity List

On September 19, 2020, China's Ministry of Commerce ("MOFCOM") released Provisions on the Unreliable Entity List ("Provisions").[4] A working mechanism was established in accordance with the Provisions and chaired by MOFCOM. The working mechanism can put certain foreign entities, including financial institutions, on the Unreliable Entity List ("UEL"), after it completes an investigation and comprehensively considers a variety of factors. The working mechanism enjoys a wide range of investigative powers, including requests for information from foreign entities, reviewing and copying documents and materials, etc.

Once put on the UEL, a foreign entity may be subject to one or more restrictive measures specified in Article 10 of the Provisions, including investment restrictions in China; restrictions related to personnel's entry, work, stay, or residence in China; and monetary fines. The listed foreign entities may be granted a grace period to correct their conduct at the discretion of the working mechanism and may request their removal from the UEL. So far, no foreign entities have been listed on the UEL.

Hong Kong

FTSB's Proposed Regulation of Virtual Asset Service Providers and Dealers in Precious Metals and Stones

In view of the increased volume in trading in virtual assets and precious metals and stones in Hong Kong and their potential

money laundering and terrorism financing risks, the Hong Kong Financial Services and Treasury Bureau ("FSTB") issued a public consultation paper on November 3, 2020, outlining a proposed licensing regime for virtual asset service providers ("VASPs") and a two-tier registration regime for dealers in precious metals and stones ("DPMS") in order to implement the recommendations of the Financial Action Task Force.

The FSTB proposed to define "Virtual Asset" as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes."[5] Under the proposal, any person seeking to conduct the regulated business of virtual asset trading platforms in Hong Kong will be required to apply for a license from the Securities and Futures Commission ("SFC") subject to the meeting of a fit-and-proper test.[6] At the initial stage, only professional investors with adequate financial resources, knowledge, and experience will be considered for the granting of a license.[7] Further, licensed VASPs are subject to the AML/CTF requirements in relation to customer due diligence and recordkeeping under Schedule 2 of the Amended Money Laundering Ordinance ("AMLO") and other regulatory requirements for investor protection purposes.

Likewise, DPMS seeking to engage in cash transactions at or above HK$120,000[8] during their course of business are required to register with the Commissioner for Customs and Excise and are subject to the AML/CTF requirements under Schedule 2 to the AMLO, in addition to meeting a fit-and-proper test for registration under the dedicated category.[9]

Upon commencement of operation of the proposal and the expiration of the proposed 180-day transitional period,[10] any person carrying on VASP activities without a proper license will commit a criminal offense and be subject to the penalty, upon conviction, of a fine of HK$5 million and imprisonment for seven years.[11] The FSTB intends to introduce a bill into the Legislative Council in 2021.[12]

The proposal provides the much-needed regulatory clarity and establishes rigorous benchmarks, which in turn will boost investor confidence.

SFC Launched Consultation on Proposed Amendment to Its AML/CTF Guideline

On September 18, 2020, the SFC launched a three-month consultation on proposals to amend its Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations) and the Prevention of Money Laundering and Terrorist Financing Guideline. The SFC's proposed changes include measures to incorporate the Financial Action Task Force's ("FATF") Guidance for a Risk-based Approach for the Securities Sector ("Securities Sector Guidance") published in October 2018.[13]

The proposed amendment seeks to facilitate the securities industry's implementation of AML/CTF measures using a risk-based assessment approach through enacting a range of measures as set out in FATF's Securities Sector Guidance. Under the proposed amendment, Licensed Corporations ("LCs") are required to consider the quantitative and qualitative data in its risk assessment and to use a list of four specific risk factors—product/service/transaction risk, country risk, customer risk, and delivery/distribution channel risk.[14] LCs are also required to undertake an institutional risk assessment at least once every two years.[15]

The SFC also proposed the implementation of a range of due diligence requirements in relation to cross-border correspondent relationships. The requirements apply to situations when Hong Kong LCs and registered institutions provide services relating to dealing in securities, futures contracts, or leveraged foreign exchange trading to an institution outside Hong Kong.[16] In terms of Customer Due Diligence ("CDD"), the SFC proposed simplified and enhanced procedures to, among other things, evaluate information provided by a customer regarding the destination of the funds involved in the transaction and to pay investment proceeds to the customer's bank account from which the funds for investment were originally transferred.[17]

The SFC proposed to supplement the existing list of examples of red-flag risk factors that will permit LCs to ascribe a lower risk and to adopt simplified due diligence.[18] Examples of such risk factors include, among other things, a customer's correspondence address that is associated with other apparently unrelated accounts, customers that exhibit no concern over the transaction costs or fees, and the making of large transactions immediately before news or a significant announcement is issued.

In relation to third-party deposits (i.e., customers using third parties to pay for or to receive investment proceeds), the SFC proposed to incorporate contents from circulars previously issued on May 31, 2019.[19]

The proposals will be subject to a three-month public consultation, and the SFC invited submission of comments by December 18, 2020.[20] Taking into account the comments received, the SFC will issue a consultation conclusions paper together with the finalized guidelines.

HKSAR v. Harjani Haresh Murlidhar

On December 5, 2019, the Court of Final Appeal Decision handed down a unanimous decision in *HKSAR v Harjani Haresh Murlidhar* [2019] HKCFA 47, which reformulated the test in determining whether a person has reasonable grounds to believe that the money in question is tainted under section 159A of the Crimes Ordinance (Cap 200) and section 25(1) of the Organized and Serious Crimes Ordinance (Cap 455) (collectively, "Money Laundering Offenses"). The reformulated approach involves a two-stage analysis: a (i) what facts or circumstances, inclusive of the personal knowledge of the defendant, were indeed known to the defendant that may have affected his belief as to whether the money was tainted; and (ii) whether any reasonable person who shares the defendant's knowledge will be bound to believe that the money was tainted. If the answer to the second question is in the affirmative, the defendant will be considered as having the mental element that could land a conviction under the Money Laundering Offenses.[21] This latest landmark decision reminds businesses to remain vigilant on the legitimacy of the source of funds.

Singapore

Increased Regulation from the Monetary Authority of Singapore

In the past year, the Monetary Authority of Singapore ("MAS") has demonstrated an increased emphasis on regulating the control frameworks that financial institutions have in place for managing the risks of money laundering and terrorism financing. In August 2020, MAS released an information paper to summarize the findings from its inspection of selected banks to assess the robustness of their enterprise-wide risk assessments for money laundering and terrorism financing. In September 2020, MAS issued a guidance paper that sets outs its expectations for effective controls to manage these risks at private banks. And in July 2020, MAS issued a consultation paper on a proposed Omnibus Act that would require, among other things, digital token service providers to establish an AML/CTF compliance function in Singapore.

Consistent with its public pronouncements on these issues, MAS has imposed multiple penalties on financial institutions in 2020 for failing to establish, maintain, and regularly update their AML/CTF controls and procedures. In July 2020, MAS revoked the Capital Markets Services License of Apical Asset Management Pte. Ltd. due to its discovery of "severe deficiencies in … AML/C[TF]" controls in its inspection of the company. In the same month, MAS imposed a SG$1.1 million penalty on Asiaciti Trust for inadequate safeguards against money laundering and terrorism financing.

Financial institutions doing business in Singapore should expect more of the same in the coming year and prepare accordingly. First, they should review the learnings identified in MAS's publications on these issues and update their controls wherever gaps are identified. Second, they should subject their AML/CTF controls to regularly scheduled independent audits to assess their effectiveness. Finally, they should demonstrate an enterprise-wide commitment to managing these risks by evaluating and incentivizing performance based on the quality of AML/CTF execution, establishing clear accountability for the execution of AML/CTF controls, and proactively conducting enterprise-wide risk assessments to better understand their money laundering and terrorism financing risk exposure.

Taiwan

Development of Anti-Money Laundering Regulations for Virtual Banking

Taiwan enacted its Money Laundering Control Act ("AML Act") in 1996 and has significantly strengthened its AML regime in recent years, including amending the AML Act in November 2018. The amended legislation brought Taiwan's AML controls in line with global standards. In late 2019, the Asia/Pacific Group On Money Laundering upgraded Taiwan to the "regular follow-up" category from the "enhanced follow-up" category. Following this achievement, virtual banks are expected to launch in Taiwan soon, which will further AML compliance and combat the financing of terrorism. Virtual banks have the advantage of building their systems from the ground up to cross-reference structured data in an ecosystem that connects the financial supply chain with the compliance value chain. In contrast, the traditional banking sector, including the well-developed offshore banking units sector, presents the greatest risks of money laundering. How AML regulations will be implemented in cryptocurrency platforms and virtual

banking in Taiwan will be something worth paying attention to in the future.

CROSS-BORDER

Digital Currencies and Their Impact on AML Regulations

There have been significant steps in the last few years to bring digital currencies and associated services and service providers within the scope of global AML standards and national enforcement activity. 2020 continued that trend.

At the start of the year, MAS updated its regulatory framework for digital payments via the new Payment Services Act 2019, which brought digital currency business businesses and exchanges based in Singapore under existing anti-money laundering and counterterrorist-financing rules and imposed new licensing requirements. All EU Member States were required to implement the Fifth Money Laundering Directive, which required EU cryptocurrency exchanges and custodian wallet providers to face the same broad AML/CTF regulations that are applied to financial institutions in the European Union, including obligations to perform customer due diligence and submit SARs to relevant authorities. The new EU regulations also required providers of exchange services and wallet providers to register with national regulators. Some Member States, including the United Kingdom and Germany, enhanced these core requirements further.

At the end of 2020, the European Union took a further step toward developing a comprehensive and harmonized framework for digital assets when it introduced a draft regulation for Markets in Crypto Assets ("MiCA"), which will cover digital currencies, stablecoins, e-money tokens, and utility tokens. MiCA will directly apply in all EU Member States and will regulate: (i) the public offering of crypto assets; (ii) the admission of crypto assets to trading on a trading platform; (iii) the licensing of crypto asset service providers; and (iv) the implementation of market abuse rules for crypto asset businesses.

In the United States, FinCEN issued a $60 million civil money penalty against Larry Dean Harmon, the founder, administrator, and primary operator of Helix and Coin Ninja, convertible virtual currency "mixers" or "tumblers," for violations of the BSA and its implementing regulations. In its penalty notice, FinCEN repeated and expanded on its 2013 Guidance—that exchangers and administrators of convertible virtual currency are money transmitters under the BSA. As such, they have an obligation to register with FinCEN; to develop, implement, and maintain an anti-money laundering compliance program; and to meet all applicable reporting and recordkeeping requirements. FinCEN issued further clarification in 2019 that providers of mixers and tumblers of convertible virtual currencies are likely also to be treated as money transmitters and therefore subject to these requirements. The added feature of concealing the source of the transaction does not change that person's status under the BSA.

Finally, highlighting some of the particular complexities that global businesses can face from coordinated cyberattacks, various global regulators highlighted concerns that companies that are subject to ransomware attacks, and that choose to pay the relevant cryptocurrency "ransom," will be committing money laundering offenses, compounding the difficulties those companies may face as a result of the hacking.

Tax Transparency Prosecutions and Initiatives

Emphasizing that the U.S. prosecutorial appetite for tax evasion cases remains high, in the largest-ever U.S. criminal tax charge, the Department of Justice in October 2020 charged the CEO of a *Fortune* 500 company of money laundering, among a series of other counts, perpetrated through decades-long efforts to hide beneficial ownership. The scheme allegedly concealed roughly $2 billion of capital gains from the IRS.

Continuing the global initiative to reach what are perceived aiders and abettors of tax misconduct, the European Union implemented Directive 2011/16 in relation to cross-border tax arrangements, known as the DAC6 Directive. DAC6 applies to cross-border tax arrangements that meet one or more specified characteristics (hallmarks) and mandates a reporting obligation for these tax arrangements. Failure to comply with DAC6 could lead to significant sanctions under local law in EU countries. Similarly, Argentina and Mexico in late 2020, as part of OECD's broader efforts to combat tax evasion, also announced plans to implement disclosure regulations similar to those found in the DAC6 Directive. These disclosure regulations generally require intermediaries, including lawyers, accountants, and tax advisors, to report certain cross-border tax arrangements considered to create "tax advantages," although that phrase is largely vaguely defined.

LAWYER CONTACTS

To learn more about Jones Day's experience in counseling companies and individuals that have received an allegation of corruption or have become the subject of government investigation, please visit our website.

AUTHORS

Sergio Alvarez-Mena
Miami
+1.305.714.9759
salvarezmena@jonesday.com

Jason Chen
Taipei
+886.2.7712.3204
jchen@jonesday.com

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

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

Ulf Kreppel
Frankfurt
+49.69.9726.3930
ukreppel@jonesday.com

Nadim Khan
Dubai
+971.4.709.8404
nkhan@jonesday.com

Lisa M. Ledbetter
Washington
+1.202.879.3933
lledbetter@jonesday.com

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

Samuel Ngo
Hong Kong
+852.3189.7233
sngo@jonesday.com

Stephen J. Obie
New York
+1.212.326.3773
sobie@jonesday.com

Lanier Saperstein
New York
+1.212.326.3845
lsaperstein@jonesday.com

Zachary Sharpe
Singapore
+65.6233.5506
zsharpe@jonesday.com

Harriet Territt
London
+44.20.7039.5709
hterritt@jonesday.com

Rick van ,t Hullenaar
Amsterdam
+31.20.305.4223
rvanthullenaar@jonesday.com

Peter J. Wang
Hong Kong / Shanghai
+852.3189.7211 / +86.21.2201.8040
pjwang@jonesday.com

Nick Wittek
Frankfurt
+49.69.9726.3917
nwittek@jonesday.com

Qiang Xue
Beijing
+86.10.5866.1111
qxue@jonesday.com

ADDITIONAL LAWYER CONTACTS

United States

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

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

Amy 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

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

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

Robert da Silva Ashley
New York
+1.212.326.7886
rdasilvaashley@jonesday.com

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

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

Jay Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

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

Henry Klehm III
New York
+1.212.326.3706
hklehm@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

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

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

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

Mark W. Rasmussen
Dallas
+1.214.220.3939
mrasmussen@jonesday.com

Heith D. Rodman
Atlanta
+1.404.581.8356
hdrodman@jonesday.com

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

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

Eric Snyder
New York
+1.212.326.3435
esnyder@jonesday.com

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

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

Middle East/Asia

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

Ben Witherall
Singapore
+65.6233.5532
bwitherall@jonesday.com

Europe

Renato Antonini
Brussels
+32.2.645.119
rantonini@jonesday.com

Liam Bonamy
London
+44.20.7039.5261
lbonamy@jonesday.com

Sophie Chevallier
Paris
+33.1.56.59.46.83
schevallier@jonesday.com

Patrizia Gioiosa
Milan
+39.02.7645.4001
pgioiosa@jonesday.com

Philippe Goutay
Paris
+33.1.56.59.39.39
pgoutay@jonesday.com

Frédéric Gros
Paris
+33.1.56.59.38.32
fgros@jonesday.com

Karin Holloch
Düsseldorf
+49.211.5406.5500
kholloch@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

Javier López Antón
Madrid
+34.91.520.3939
jlopezanton@jonesday.com

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

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

Liz Saxton
London
+44.20.7039.5162
esaxton@jonesday.com

Francesco Squerzoni
Milan
+39.02.7645.4001
fsquerzoni@jonesday.com

Vinicio Trombetti
Milan
+39.02.7645.4001
vtrombetti@jonesday.com

Australia

Daniel Moloney
Melbourne
61.3.9101.6828
dmoloney@jonesday.com

Special thanks to associates Ankit Bahri, Corey M. Byrne, Helen Jiang, Jeff Lin, Angelina N. Moore, Matthew J. Razzano, Michael B. Shammo, Daniel Shum, David Sverdlov, and law clerk David Wu for their assistance with this White Paper.

ENDNOTES

1 *See also* Jones Day *Commentary*, "Congress Passes Major U.S. Anti-Money Laundering Reforms," Dec. 2020.

2 Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015.

3 The official publication of the Implementing Measures (in Chinese).

4 *See* the official press release in Chinese.

5 Para. 2.6 of the FTSP Consultation Paper (Scope and Coverage).

6 Para. 2.5 of the FTSP Consultation Paper.

7 Para. 2.18 of the FTSP Consultation Paper (Regulatory Requirements).

8 Para. 3.1 of the FTSP Consultation Paper (Regulation of Dealers in Precious Metals and Stones)

9 Para. 1.13(b) of the FTSP Consultation Paper (Legislative Proposals).

10 Para. 2.22 of the FTSP Consultation Paper (Exemption and Prohibition).

11 Para. 2.28 of the FTSP Consultation Paper (Sanctions).

12 Para. 5.2 of the FTSP Consultation Paper (Next Steps).

13 Paragraph 6 (P.6) of the SFC Consultation Paper.

14 Paragraph 19 (P.9) of the SFC Consultation Paper.

15 Paragraph 17 (P.8) of the SFC Consultation Paper.

16 Paragraph 30 (P.11) of the SFC Consultation Paper.

17 Paragraph 45 (P.15) of the SFC Consultation Paper.

18 Paragraphs 47-52 (P.16-17) of the SFC Consultation Paper (Red-flag indicators of suspicious transactions and activities).

19 Paragraph 53-55 (P.17) of the SFC Consultation Paper (Third-party deposits and payments).

20 Paragraph 76 (P.22) of the SFC Consultation Paper (Seeking Comments).

21 Paragraph 26 of the CFA Judgment.

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

© 2021 Jones Day. All rights reserved. Printed in the U.S.A.