JONES DAY | One Firm Worldwide®

WHITE PAPER

May 2023

2022 Anti-Money Laundering and Sanctions Year in Review

In 2022, anti-money laundering ("AML") and sanctions controls were at the center of regulatory and enforcement activities in the United States and abroad. Globally, governments have continued to recognize the impact of AML legislation on the health and stability of their financial sector. In a continuing trend, digital assets remained a top enforcement priority in 2022, and authorities issued record-setting penalties in a number of high-profile cases.

Following Russia's invasion of Ukraine in February 2022, lawmakers immediately sought to enact comprehensive sanctions packages with the goal of limiting Russia's ability to participate in the global economy. These sanctions frameworks continue to evolve as regulators confront emerging issues. By the end of 2022, the European Union had released its ninth legislative sanctions package, with a 10th following in early 2023. Legislators and regulators have maintained focus on the virtual currency industry, including by taking action against illicit actors who use digital assets to circumvent sanctions controls.

This *Year in Review* explores these and other noteworthy legislative and enforcement developments related to AML and sanctions in 2022, considers the potential impact on financial institutions as a result of these developments, and explores the industry trends expected to continue throughout 2023.

TABLE OF CONTENTS

SANCTIONS

United States Adopts Sweeping Sanctions Measures

In the United States, sanctions developments for 2022 focused largely on Russia, Ukraine, and Belarus following Russia's invasion of Ukraine in early 2022 and the war that has followed. Since February 2022, acting in close consultation and alignment with many Western countries, the United States has significantly expanded existing restrictions on Russia, certain regions of Ukraine, and, to a lesser extent, Belarus. Broadly, these expanded restrictions include:

- Comprehensive sanctions on the "Donetsk People's Republic" and the "Luhansk People's Republic" regions of Ukraine, similar in purpose and scope to the sanctions imposed on Crimea following Russia's 2014 invasion of Crimea. As a result, U.S. persons are prohibited from engaging in or facilitating virtually all activities in or with these regions of Ukraine.
- The addition of more than 1,500 Russian and Belarusian individuals and entities to the Specially Designated Nationals and Blocked Persons ("SDN") List maintained by the Office of Foreign Assets Control ("OFAC"), including most of Russia's largest state-owned and private banks and financial institutions, hundreds of oligarchs and elected officials, and hundreds of individuals and entities across large swaths of Russia's economy, including in the defense, technology, electronics, mining, marine, energy, and media sectors.
- A broadly defined prohibition on "new investment" by U.S. persons in Russia. OFAC has defined "investment" as "the commitment of capital or other assets for the purpose of generating returns or appreciation." OFAC has clarified that new investment does not include "[e]ntry into, performance of, or financing of a contract, pursuant to ordinary commercial sales terms, to sell or purchase goods, services, or technology to or from an entity in Russia (*e.g.*, a payment of an invoice for goods, where payment is made within the contracted time period and such payment does not involve participation in royalties or ongoing profits)."
- A restriction on the provision by U.S. persons of certain professional services and certain quantum computing services to Russian entities or individuals.

In late 2022, OFAC also targeted certain Iranian companies it alleged to be supplying unmanned aerial vehicles to Russia to support Russia's ongoing invasion of Ukraine. News reports also indicate that certain Iranian officials have called on their government to restart negotiations aimed at reviving the Joint Comprehensive Plan of Action, but U.S. officials have reportedly downplayed the likelihood of resuming talks.

Virtual currencies also came into the spotlight as part of the U.S. government's enforcement of the vastly expanded sanctions related to Russia and Belarus in 2022. In March 2022, U.S. Attorney General Merrick Garland announced the launch of Task Force KleptoCapture, an interagency law enforcement task force dedicated to enforcing the "sweeping" sanctions enacted in response to Russia's unprovoked military invasion of Ukraine. The mission of the taskforce explicitly includes "[t]argeting efforts to use cryptocurrency to evade U.S. sanctions, launder proceeds of foreign corruption, or evade U.S. responses to Russian military aggression." In May 2022, the Congressional Research Service issued a report warning of the rising use of cryptocurrency for Russia-related sanctions evasion.

In May 2022, Jones Day authored a *White Paper* detailing the impact of these global sanctions.

European Union Adopts Sanctions Following the Invasion of Ukraine by Russia

Following the invasion of Ukraine by Russia, the European Union adopted an initial set of sanctions on February 23, 2022. Since then, the European Union has gradually strengthened these sanctions, and the latest measures were adopted on December 16, 2022. These sanctions are designed to limit access to European markets and financial services and include individuals and entities close to the Kremlin on asset freeze and EU entry ban lists. They were subsequently extended to entire sectors of the Russian economy, and the list of sanctioned persons has continued to grow. For example, the armament, finance, aviation, luxury goods, and energy sectors are now affected by import and export restrictions and/or price caps. Some Russian banks have also been disconnected from the "SWIFT" interbank network. Due to the

rapid evolution of these sanctions, the European Commission has published a consolidated sector-by-sector list of FAQs on the measures imposed.

Australian Government Imposes Sanctions Relating to Russia

During the course of 2022, the Australian government progressively imposed increasingly significant sanctions and controls relating to Russia and Belarus. Australia had imposed sanctions relating to Crimea and Sevastopol in 2014 that were extended in 2015, and these sanctions were then applied relating to Donetsk and Luhansk beginning March 28, 2022, by regulations made on February 24, 2022. The government announced that the delay in commencement was to give "opportunities for businesses that have had legitimate operations and business interests in Russia and in the affected territories of Ukraine to be able to make changes to their arrangements."

These sanctions prohibited, among other things:

- Export and import of armaments to and from Russia;
- Export of goods and services related to infrastructure in the transport, telecommunications, energy, oil, gas, and minerals sectors to the affected regions of Ukraine, as well as investments related to these sectors; and
- Import of any goods not verified by Ukrainian authorities from the affected regions of Ukraine.

The sanctions were extended during the year to ban the export of aluminum ores and products and certain luxury goods to Russia, and to prohibit imports of gold, oil, natural gas, coal, and other energy products.

On December 2, 2022, Australia adopted the price cap on seaborne Russian-origin crude oil agreed by the G7 countries, of $60 per barrel, and the Minister for Foreign Affairs issued a general permit authorizing the provision of financial assistance and financial services where they assist with, or are provided in relation to, the import of Russian oil at or below the price cap. This measure is designed to maintain a stable supply of oil to the global market while reducing the revenue Russia earns from oil.

Regulations were also introduced, effective February 25, 2022, to allow the Minister for Foreign Affairs to designate a person or entity for targeted financial sanctions, or declare a travel ban, if:

- The Minister is satisfied that the person or entity is, or has been, engaging in activity or performing a function that is of economic or strategic significance to Russia;
- The person or entity is a current or former Minister or senior official of the Russian government; or
- The person is an immediate family member of a person listed under the first and second bullets above.

Those regulations were then used to impose targeted financial sanctions and travel bans on Russian President Vladimir Putin, all members of Russia's Security Council, 339 members of the State Duma of the Federal Assembly of the Russian Federation, as well as other Russian individuals and military personnel.

Sanctions were also applied to a number of Russian organizations, including companies predominantly engaged in activities relating to military equipment or services, publicly owned or controlled Russian companies involved in the sale or transport of crude oil or petroleum products, and publicly owned or controlled Russian banks (in addition to organizations that had already been listed under the prior sanctions). The sanctions prohibit dealing in financial instruments (bonds, equity, transferable securities, money market instruments, or other similar financial instruments) issued by specified organizations, or providing loans or credit to them.

The Australian Transaction Reports and Analysis Centre ("AUSTRAC") announced on June 27, 2022, that it had established a dedicated intelligence team to monitor and triage financial reporting about Russian sanctions, including suspicious matter reporting and international funds transfer reporting, and use the reporting to produce actionable financial intelligence to assist the Australian Sanctions Office and Australian Federal Police to detect sanctions evasion.

ANTI-MONEY LAUNDERING

United States

AML Developments Related to Virtual Currencies

In 2022, the Department of the Treasury ("Treasury") announced its intent to pursue proposed amendments to Bank Secrecy Act ("BSA") regulations that would impose compliance requirements on certain transactions involving convertible virtual currency ("CVC") and digital assets with legal tender status ("LTDA"). In January 2022, the Treasury published its semiannual agenda of regulations that, among other things, included two rules proposed by the Treasury's Financial Crimes Enforcement Network ("FinCEN") from 2020 that remained pending. The first, FinCEN's October 2020 proposed rule to amend the BSA's "Travel Rule," would clarify the Travel Rule's application to CVC and LTDA. The second, FinCEN's December 2020 proposed rule on certain transactions involving CVC or LTDA, would impose BSA reporting and recordkeeping requirements on CVC or LTDA transactions above certain monetary thresholds that involve unhosted wallets or wallets hosted in a jurisdiction identified by FinCEN. The January 2022 agenda recognized that FinCEN's October 2020 proposed rule was in the "proposed rule stage," while FinCEN's December 2020 proposed rule was in the "final rule stage." The Treasury published another semiannual agenda in August 2022 indicating that both of the proposed rules remained pending.

In September 2022, DOJ stated in its report "The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets" that it supported issuing a final version of FinCEN's October 2020 proposed rule. DOJ reasoned that the final rule would be "a necessary step to meeting the objectives that the rule is designed to achieve—including mitigating the illicit finance risks posed by digital assets by preserving information about their transaction." DOJ also stated that it supported amendments to the BSA and its implementing regulations to clarify that their key AML provisions, including those requiring customer identification programs and the reporting of suspicious transactions to regulators, apply to non-fungible token ("NFT") platforms.

DOJ's September 2022 report also served to update the Department's October 2020 Cryptocurrency Enforcement Framework. Similar to the October 2020 Framework, the September 2022 report discusses: criminals' use of cryptocurrency to launder money and hide financial activity in other ways; criminals' use of virtual asset service providers ("VASPs") that do not comply with AML standards; and the AML compliance risks posed by practices meant to make it more difficult to trace or attribute transactions, such as by obfuscating the source of funds. In addition, the September 2022 report highlights the "distinct risks of criminal exploitation" associated with decentralized finance and NFTs, both of which had grown significantly since the publication of the October 2020 Framework.

Enforcement Activity Related to Virtual Currencies

In February 2022, DOJ charged the founder of BitConnect in the Southern District of California with wire fraud, international money laundering, and operating an unlicensed money transmitting business in connection with a cryptocurrency investment program and a cryptocurrency exchange with a proprietary coin offering. DOJ alleged that BitConnect's founder misled investors about the profitability of the company's purported proprietary technology and guaranteed returns by using investors' money to trade on the volatility of cryptocurrency exchange markets, all while operating a Ponzi scheme where earlier BitConnect investors were paid with later investors' money. DOJ also alleged that BitConnect operated as a money transmitting business through its digital currency exchange but had failed to register with FinCEN. This indictment followed the September 2021 guilty plea to wire fraud by BitConnect's head promoter, who was sentenced to 38 months in prison in September 2022.

In October 2022, as part of a global resolution, Bittrex, an online virtual currency exchange, settled with both FinCEN and OFAC. Bittrex allegedly operated for nearly two years without a sanctions compliance policy in place, conducted more than 116,000 transactions valued at over $260 million with entities and individuals located in jurisdictions subject to U.S. sanctions, and failed to report any suspicious activities for a period of more than three years, including suspicious transactions involving sanctioned jurisdictions. FinCEN imposed a $29.28 million civil monetary penalty against Bittrex for failing to maintain an effective AML program and failing to report certain suspicious activity. Meanwhile, OFAC announced a more than $24.28 million settlement, making it the largest-ever penalty levied by the agency in the virtual currency industry.

Danske Bank Pleads Guilty to Fraud on U.S. Banks in Parallel DOJ and SEC Actions

On December 13, 2022, Danske Bank pleaded guilty to bank fraud conspiracy and agreed to pay $2 billion to settle the yearslong investigation into its Estonian branch, Danske Bank Estonia. According to the plea, Danske Bank defrauded U.S. banks about Danske Bank Estonia customers and its AML controls to enable high-risk customers who lived outside Estonia, including in neighboring Russia, to access the U.S. financial system. On the same day, the bank settled a parallel SEC action for violating the antifraud provisions of section 10(b) of the Securities and Exchange Act of 1934.

Danske Bank acquired Danske Bank Estonia in 2007, but the branch maintained its own IT system and oversight procedures, including a program (the NRP) whereby approximately 10,000 high-risk, nonresident customers, including from Russia, could access the U.S. financial system with little controls or oversight. Between 2008–2016, Danske Bank Estonia processed more than $160 billion through U.S. banks on behalf of NRP customers. Following a whistleblower's report and internal audit, Danish authorities fined Danske Bank nearly $2 million for violating AML rules through the NRP in December 2017.

The United States initiated an investigation in 2018, by which time Danske Bank knew or should have known that some NRP customers were engaged in highly suspicious and potentially criminal transactions, including transactions through U.S. banks. According to the settlements, Danske Bank also knew or should have known that the Estonia branch's AML program and procedures did not meet Danske Bank's own standards and were not appropriate to meet the risks associated with the NRP, but did not disclose this information to investors.

Danske Bank's settlements highlight the significant monetary penalties for AML failures and misrepresentations but also demonstrate that U.S. authorities will seek to address this conduct through fraud statutes, expanding the scope of liability to banks without a U.S. branch or presence. Unable to rely on the BSA, DOJ charged the bank with conspiracy to commit bank fraud under 18 U.S.C. § 1349. Notably, the SEC was able to reach Danske Bank because, among other things, U.S. investors held approximately 18% of the bank's securities and, according to the SEC, Danske Bank made misrepresentations "for the benefit of" and "available to" actual and prospective U.S. investors via its corporate website.

U.S. Charges Foreign Manufacturer for Conspiring to Provide Material Support to Foreign Terrorist Organizations

On October 18, 2022, French building materials manufacturer Lafarge S.A. pleaded guilty to a charge that it made payments to terrorist groups, including ISIS and al-Nusrah Front ("AND"), amounting to a first-of-its-kind conviction.

In 2010, Lafarge constructed a cement plant in Northern Syria, which it operated through its long-defunct subsidiary Lafarge Cement Syria ("LCS"). After the Syrian Civil War began in 2011, Lafarge and LCS negotiated agreements to pay "armed factions" in the Civil War to protect LCS employees, to ensure continued operation of the plant, and to obtain economic advantage over local competitors. Lafarge purchased raw materials from ISIS-controlled suppliers and paid monthly "donations" to armed groups such as ISIS and ANF. To encourage ISIS to act in LCS's economic interest, LCS entered a "a revenue-sharing agreement" with the terrorist group being compensated based on the amount of cement sold by LCS.

According to the plea, Lafarge and LCS executives concealed their dealings with ISIS and ANF by requiring intermediaries to create shell businesses and submit invoices with false descriptions of services to LCS. The revenue-sharing agreement with ISIS required the purchaser to pay ISIS directly, while LCS gave the purchaser a discount. Executives used personal email addresses to discuss the arrangement and required that documents memorializing their agreement omit the name "Lafarge." Lafarge and LCS executives also backdated an intermediaries termination notice to coincide with the U.N. Security Council's resolution prohibiting business with ISIS and ANF. LCS evacuated and ISIS took possession of the plant in September 2014.

The total gain to all participants in the conspiracy—including LCS, the intermediaries, and the terrorists groups—totaled approximately $80.54 million, with nearly $6 million funneled to ISIS and ANF by LCS. Swiss Holcim acquired Lafarge in 2015, but Lafarge did not disclose its agreements with ISIS during premerger diligence. Because Lafarge did not operate in Syria at the time of the acquisition, Holcim did not conduct further diligence on Lafarge's activities in Syria. According to DOJ, Lafarge, LCS, and Holcim did not self-report the conduct and did not fully cooperate with the U.S. investigation.

Lafarge's plea represents the first instance a company pleaded guilty to conspiring to provide material support to a foreign terrorist organization. Lafarge and now-defunct LCS will pay criminal fines of $90.78 million and a forfeiture of $687 million. The Lafarge case materializes the possibility of corporate liability for terrorist financing in the United States.

JASTA Secondary Liability

While 2022 continued to see district courts increasingly permit Anti-Terrorism Act ("ATA") claims to proceed beyond the pleading stage into discovery, there were also important countercurrents to this development. Despite several recent decisions favorable to defendants,[1] plaintiffs continue to create a greater risk for businesses operating in regions with active terrorist organizations (or having customers with ties to those regions).[2] Moreover, businesses operating in those regions now also face the prospect of criminal liability under the ATA.[3]

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" a designated Foreign Terrorist Organization ("FTO") who "committed, planned, or authorized an act of international terrorism."[4]

Spurred by the reasoning in circuit court decisions, district courts—with the recent exception of the Eastern District of New York dismissing plaintiffs' claims in *Wildman v. Deutsche Bank*[5]—have increasingly denied defendants' motions to dismiss, enabling ATA plaintiffs to pursue complex and costly discovery.[6] In 2021, the Second Circuit paved the way for certain JASTA claims to survive motions to dismiss.[7] In those decisions, the Second Circuit made clear that pleading a bank's "general awareness" of a customer's ties to terrorism did not require the customer's designation as an FTO, but rather could arise from certain public reporting, such as in the news media.[8] In 2022, the D.C. Circuit joined the Second Circuit in interpreting JASTA's aiding and abetting provision in *Atchley v. AstraZeneca UK Ltd.*, 22 F.4th 204 (D.C. Cir. 2022), and *Bernhardt v. Islamic Republic of Iran*, 47 F.4th 856 (D.C. Cir. 2022).

In *Atchley*, plaintiffs were injured in terrorist attacks committed by Jaysh al-Mahdi ("JaM"). Plaintiffs alleged that corrupt payments made by defendants—medical supply and manufacturing companies—to JaM in order to secure contracts with Iraq's Ministry of Health, financed JaM.[9] The D.C. Circuit held that the plaintiffs had sufficiently pled general awareness by pleading that defendants were "aware of reports extensively documenting both [JaM's] domination of the Ministry and its mission to engage in terrorist acts" and had sent their agents into the Ministry, which displayed weapons, "Death to America" slogans, posters of JaM leadership, and JaM's flag, and in which "armed terrorist fighters circulated openly."[10] The court also held that plaintiffs had sufficiently pled substantial assistance by plausibly alleging that defendants' significant financial support over several years "was important to the development" of JaM.[11]

In contrast, nine months later, in *Bernhardt*, the D.C. Circuit held that plaintiffs had failed to sufficiently plead a JASTA aiding and abetting claim against bank defendants that were alleged to have had financial dealings with intermediary banks with terrorist links.[12] The court held that, notwithstanding that some of these intermediary banks were sanctioned by OFAC, there were no plausible allegations that defendants were "generally aware" of these intermediaries' alleged connections to al-Qaeda. The court concluded that those alleged connections—that the intermediaries were nationalized Iranian banks, one of which was founded by a key financial contributor to al-Qaeda—were insufficient to establish that the intermediaries were so closely intertwined with terrorism that defendants were aware they were assuming a role in al-Qaeda's terrorist activities.[13] Petitions for rehearing *en banc* are currently pending in both *Atchley* and *Bernhardt*.

How district courts continue to assess motions to dismiss in light of developing Circuit and potential Supreme Court guidance will provide further insight regarding how to mitigate ATA litigation risks in the coming year.[14]

FinCEN Issues Final Rule Regarding Beneficial Ownership Reporting

As detailed in a Jones Day *Alert*[15] last fall, FinCEN issued a final rule in September 2022 under the Corporate Transparency Act's ("CTA") beneficial ownership information ("BOI") reporting provisions. The rule requires certain reporting companies, including domestic and foreign corporations and LLCs, domestic entities created by filings with a secretary of state (or similar), and foreign entities registered to do business in any U.S. jurisdiction, to report to FinCEN: (i) the beneficial owners

of the entity; and (ii) the company applicants of the entity. Other entities, such as banks, brokers, and accounting firms, are exempt from the rule under the terms of the CTA.

The rule provides that a beneficial owner is an individual who, directly or indirectly, either owns or controls at least 25% of the reporting entity or exercises substantial control over the reporting entity. The company applicant is the individual who directly files or controls the filing of the document that creates the entity with the secretary of state (or similar). The final rule takes effect on January 1, 2024.

At the close of 2022, FinCEN issued a Notice of Proposed Rulemaking ("NPRM") concerning access to and protection of reported BOI. The NPRM proposes how government officials, along with certain financial institutions and their regulators, would access and use BOI. A final rule is expected later in 2023.

European Union

Court of Justice of European Union Invalidates General Public Access to European Registers of Beneficial Ownership

Pursuant to article 30(5) of the European AML Directive, each Member State of the European Union must ensure that information on the beneficial ownership of companies and of other legal entities mentioned in the beneficial ownership register is accessible in all cases to any member of the general public. Member States can restrict such access only in exceptional circumstances and on a case-by-case basis—for example, where access would expose the beneficial owner to disproportionate risks.

On November 22, 2022, the Grand Chamber of the Court of Justice of the European Union considered in Joined Cases C-37/20 whether the general public's access to information on beneficial ownership constitutes a serious interference with the fundamental rights to respect for private and family life and to the protection of personal data, as guaranteed by articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The court found that the directive does not limit the general public's access to information that is strictly necessary, nor is the access granted by the directive proportionate to the objective of general interest to prevent money laundering and terrorist financing. In addition, the possibility to restrict the general public access on a case-by-case basis does not, according to the court, demonstrate a proper balance between the objective of general interest and the fundamental rights at stake, or the existence of sufficient safeguards against the risks of abuse of personal data.

While the court's decision does not lead to the annulment of all national legislations transposing the AML Directive, it obliges all national judges to set aside national pieces of legislation transposing litigious article 30(5) of the AML Directive, if such legislation goes against the court's retroactive decision. For example, this judgment led several countries such as Luxembourg, Germany, Belgium, and the Netherlands to temporarily close down all general public access to their register of beneficial ownership. Other countries, such as France, have decided to maintain general public access while considering all the consequences of the judgment.

The impact of this decision on market participants should be limited as competent authorities, financial intelligence units, and natural or legal persons subject to AML rules (e.g. banking and financial institutions, auditors, notaries, etc.) will still have access to the registers of beneficial ownership.

European Central Bank Withdraws License of Austrian Credit Institution

The Tribunal of the European Union recently upheld a 2019 decision by the European Central Bank ("ECB") to withdraw the license of an Austrian credit institution. Given the continuous and repeated noncompliance with AML/CFT requirements, as well as internal governance, the ECB considered that the bank was no longer able to ensure sound risk management.

European Banking Authority Launches its New Database "EuReCA"

The European Banking Authority ("EBA") announced on January 31, 2022, the launch of its new database "EuReCA," intended to become a key tool in the fight against money laundering and terrorist financing, as it would allow the EBA to adapt its supervision to the reality on the ground.

In particular, the information contained in the database will make it possible to identify significant weaknesses in the European Union's financial institutions and to consolidate the measures imposed on failing actors at the European level.

EBA Guidelines on Remote Customer Onboarding Solutions and Role and Responsibilities of AML/CFT Compliance Officer

In its final guidelines dated June 14, 2022, the EBA provided guidance on the role and responsibilities of the compliance officer in the fight against money laundering and terrorist financing. In particular, the guidelines dictate that regulated institutions must designate a member of their management body responsible for the implementation of AML/CFT obligations, and specify the tasks and responsibilities of this person. The objective is to clarify the regulatory framework and to harmonize it at the European level.

On November 22, 2022, the EBA published its Guidelines on the use of remote customer onboarding solutions, which define the measures that credit and financial institutions must take to ensure compliance with applicable AML/CFT and data protection legislation. In particular, the EBA requires institutions to carefully design their remote onboarding policies and procedures, and provides details on the customer identification and verification mechanisms.

Report of European Supervisory Authorities on Withdrawal of Authorization for Serious Breaches of AML/CFT Regulations

The European Supervisory Authorities ("ESAs"), in a joint report published on May 31, 2022, discussed the issue of the withdrawal of license in cases of serious breaches of the AML/CFT regulations. The report calls for the effectiveness of the AML/CFT system to be a condition for the granting of authorization in all sectoral legislation. The report is also in favor of creating a ground for withdrawal of authorization in cases of serious breaches of the AML/CFT regulations. In this regard, the ESAs retain criteria to qualify such a breach, and specify that the withdrawal of a license should occur only as a last-resort measure and after a proportionality control.

Italy

New Decree No. 55 Setting Forth Provisions on Communication, Access, and Consultation of Data and Information on Beneficial Ownership

Legislative Decree no 231/2007 (Italian AML Law that has transposed the European AML Directive in Italy) provides for a register setting forth the information on beneficial ownership (*registro dei titolari effettivi*). On March 11, 2022, the Minister of Economy, together with the Minister of Industry, issued Decree No. 55 setting forth provisions on communication, access, and consultation of data and information on the beneficial ownership of companies with legal personality, private legal persons, trusts with tax-relevant legal effects, and legal institutions similar to trusts. The decrees on the operational rules for the functioning of this register have not yet been issued.

Increase to Limits on Transfer of Cash and Bearer Securities

Article 1, paragraph 384 of Law no. 197 of December, 29 2022 (the so-called Budget Law 2023) amended Article 49 of Legislative Decree no. 231/2007 by raising from €2,000 to €5,000 the limit on the transfer of cash and bearer securities ("*titoli al portatore*") in euro or foreign currency. This limit applies to transactions carried out for any reason between different parties, whether natural or legal persons. The limit of €5,000 applies as of January 1, 2023.

England

Financial Conduct Authority Fines Santander UK Plc £107.7 Million for Serious and Persistent Gaps in AML Controls

The Financial Conduct Authority ("FCA") found that a unit of Spain-based Banco Santander SA failed to properly oversee and manage its AML systems between December 2012 and October 2017, which significantly impacted the account oversight of more than 560,000 business customers. In particular, the bank had ineffective systems to adequately verify the information provided by customers about the business they would be doing. The bank also failed to properly monitor the money that customers reported would be going through their accounts compared with what actually was being deposited. These failures led to more than £298 million passing through the bank before it closed some identified litigious business banking accounts. Santander has not disputed the FCA's findings and agreed to settle, which means it has qualified for a 30% discount. Without the discount, the £107,793,300 financial penalty would have been £153,990,400.

France

AML/CFT Failures Do Not Entitle the Victim of Fraudulent Act to Obtain Damages

In a September 21, 2022, decision, the Commercial Chamber of the French Supreme Court (*Cour de cassation*) ruled on the following question: Does the failure of a financial institution to comply with its AML/CFT obligations entitle the victim of a fraudulent act to obtain damages?

The Commercial Chamber answered in the negative: The obligations of vigilance and declaration imposed on financial institutions are intended to fight money laundering and terrorist financing only. The victims of fraudulent acts cannot, therefore, claim damages from the failing financial institution because of noncompliance with these obligations.

Assets Frozen Under International Sanctions Cannot Be Transferred or Seized

The French Supreme Court, in two decisions dated September 7, 2022, addressed the ability of litigants to seize frozen assets. The matter involved a Kuwaiti group that had seized assets belonging to a Libyan investment fund, worth approximately €1 billion, in execution of an arbitration award rendered in Cairo. As these assets were frozen by a European decision, the question arose as to the effectiveness of the seizure. The Court of Cassation was able to rely on a recent decision of the European Court of Justice and confirm that no enforcement measures can be taken against frozen funds or economic resources. Thus, assets frozen under international sanctions cannot be transferred or seized. This decision was eagerly awaited in view of the European sanctions against Russian oligarchs.

Spain

Amendments to Act 10/2010 on the Prevention of Money Laundering and Terrorist Financing

On September 28, 2022, Law 18/2022 on the Creation and Growth of Companies amended Act 10/2010 (the "Act") in its second final provision to include provisions focusing on personal data protection. The amendment incorporates certain relevant regulations already included in the latest European AML directives that Spanish legislation has yet to implement.

Specifically, the changes are as follows:

- Section 3 of Article 2 of the Act is amended by including among the persons excluded from the obligation to comply with the regulations of the Act, provided that the risk of money laundering or terrorist financing is low: (i) electronic money institutions; (ii) payment institutions; and (iii) individuals and legal entities referred to in Royal Decree-Law 19/2018 of November 23, 2018, on payment services and other urgent measures in financial matters;
- Letter a) of Section 1 of Article 12 of the Act, which regulates business relationships and non-face-to-face operations, is modified, clarifying that in all cases in which the electronic signature used does not meet the requirements of a qualified electronic signature, it will still be mandatory to obtain, within a period of one month from the beginning of the business relationship, a copy of the ID; and
- Obliged subjects that belong to the same category (e.g., credit institutions, jewelers, or insurers, among others) are allowed to create common systems of information, storage, and documentation collected, for complying with the obligations established in the Act. These obliged parties will be jointly responsible for the processing of the data in this system and, therefore, will acquire new obligations, such as the need to: (i) inform the Commission for the Prevention of Money Laundering about the setting-up of the common system; (ii) inform the interested parties about the communication of the data to the system, if applicable; or (iii) respond to the exercise of rights set out in Articles 15 to 22 of EU Regulation 2016/679 of the Parliament and of the Council of 27 April 2017 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Mainland China

Anti-Money Laundering Legislation in China

China's draft amendments to the Anti-Money Laundering Law were submitted to the National People's Congress ("NPC") in 2022 and are now under further revision. The Amendments are intended to modernize the AML regulatory framework, strengthen the information-sharing mechanism, and specify individuals' obligations and responsibilities.

Inactive Enforcement of Unreliable Entity List Provisions and Blocking Rules

As briefed in our 2020 *Year in Review*, China's Ministry of Commerce ("MOFCOM") released Provisions on the Unreliable Entity List, which set up a MOFCOM-led work mechanism to evaluate and designate foreign entities on the so-called Unreliable List. The designated entities will be subject to certain restrictive measures. MOFCOM, however, has not made any such designations to date.

Similarly, MOFCOM has not issued any prohibition orders to the effect that a foreign legislation or measure will not be accepted or observed in China under MOFCOM's Rules on Counteracting Unjustified Extra-Territorial Application of Foreign Laws and Other Measures (i.e. the Ministry's blocking rules). We briefly introduced the details of the blocking rules in the 2021 *Year in Review*.

China Enforces Anti-Foreign Sanctions Law

As reported in our 2021 *Year in Review*, the Anti-Foreign Sanctions Law was enacted by the NPC in response to certain restrictive measures imposed by other countries on Chinese citizens and organizations.

Over the last two years, China has sanctioned more than 70 foreign individuals and entities of the United States, European Union, United Kingdom, Canada, and Lithuania due to their actions that are thought to be against China's national sovereignty, security, and development interests. Specifically, China's Ministry of Foreign Affairs ("MOFA") imposed six rounds of sanctions in 2021 and three rounds of sanctions in 2022. These sanctions measures usually include asset freezing, transaction prohibition, and visa or border entry denial.

Most of those sanctions are imposed on foreign government officials, congress or parliament members, and think tanks and their directors. For example, on July 23, 2021, MOFA imposed sanctions on six U.S. individuals including a former U.S. Commerce Secretary and one U.S. entity, responding to the release of "Hong Kong Business Advisory" by three U.S. agencies and OFAC's designations of seven Chinese senior officials on the SDN List.

On the other hand, China's sanctions on foreign commercial companies and business persons are rare so far. The only such example is MOFA's sanctioning of Boeing Defense and Raytheon Technologies and their senior executives in response to an arms sales to Taiwan.

Australia

AUSTRAC Releases Financial Crime Guides

On April 21, 2022, the Australian Transaction Reports and Analysis Centre ("AUSTRAC") released two financial crime guides to help financial services businesses identify, prevent, and report ransomware attacks and the criminal abuse of digital currencies. The guides aim to help businesses understand the ways in which ransomware operates and digital currencies are used to facilitate crime.

The guide "Preventing the Criminal Abuse of Digital Currencies" provides lists of financial and behavioral indicators that can be used to review profiling and transaction monitoring programs, to target, detect, and disrupt transactions associated with financial crime and money laundering through digital currencies. The guide "Detecting and Reporting Ransomware" provides lists of indicators for financial services business to assess whether a customer might be either a victim of ransomware or a ransomware cybercriminal.

On October 28, 2022, AUSTRAC released a financial crime guide on "Preventing Trade-Based Money Laundering in Australia." This guide is aimed at assisting government agencies and financial services providers to understand and identify how the trade of goods and services can be used to move illicit money into and out of Australia. The guide explains the techniques that can be used by importers and exporters, and also provides a list of customer behavioral and financial indicators, noting that financial services providers should use a combination of such indicators, in addition to knowledge of their business, to monitor, mitigate, and manage risk associated with any unusual activity.

AUSTRAC Releases Guidance to Ensure Greater Access to Financial Services

On December 9, 2022, AUSTRAC released guidance to banks and superannuation funds on "Assisting Customers Who Don't Have Standard Forms of Identification." The guidance is intended to promote greater access to financial services by

supporting individuals from diverse backgrounds and in difficult circumstances who may not have the traditional forms of documentation required to prove their identity.

The guide notes that Australia's AML/CTF rules allow for alternative ways to verify a customer's identity if standard identification documents cannot be produced, and provides information about alternative identification options and how these options can be applied to classes of vulnerable individuals. This guidance aims to assist financial institutions in balancing flexible approaches to customer identity processes with the need to maintain due diligence required by anti-money laundering laws.

AUSTRAC Releases National Risk Assessment on Proliferation Financing in Australia

On December 14, 2022, AUSTRAC released Australia's first national proliferation financing risk assessment. "Proliferation financing" is when a person makes available an asset, provides a financial service, or conducts a financial transaction that is intended to facilitate the proliferation of weapons of mass destruction. The assessment found that Australia is primarily targeted by state-based or linked procurement networks; however, there has also been activity by non-state actors that may pose an increasing threat as new technologies become more available to the general public.

The assessment identifies the most significant proliferation financing threats as including:

- Use of Australian financial services and infrastructure to procure dual-use goods and evade sanctions;
- Use of Australia-based corporate structures, or Australian or third-country nationals, or designated nonfinancial businesses and professions, to facilitate proliferation financing and evade sanctions; and
- Exploitation of Australian citizens to source and export sensitive technologies and knowledge for "actors of proliferation concern."

Multinational

In June 2022, the Financial Action Task Force ("FATF") published a report updating on the implementation of its 2019 guidance (and 2021 updated guidance) on virtual assets and VASPs. The report found, among other things, that "[t]he vast majority of jurisdictions have not yet fully implemented" the FATF's recommendations setting global AML/CFT standards for virtual assets and VASPs. The report concluded that in 2021, "jurisdictions have made only limited progress" in introducing the FATF's "Travel Rule."

On March 4, 2022, the FATF amended existing Recommendation 24, which requires countries to "prevent the misuse of legal persons" for money laundering/terrorist financing and maintain "adequate, accurate and up-to-date" beneficial ownership information. The amended rule explicitly requires countries to adopt a multiprong and risk-based approach in addressing the risks of legal persons in their countries. Countries must evaluate the risk posed not only by legal persons in their country, but also "by foreign-created persons which have sufficient links with their country." The FATF expects countries to act expeditiously in adopting these new standards.

On April 19, 2022, the FATF announced the release of its "Report on the State of Effectiveness and Compliance with the FATF Standards." The report found significant strides in global technical compliance—from 36% in 2012 to 72% in 2022—but it also highlighted the "many countries" that have yet to take effective action. In the announcement, FATF outlined three changes it plans to make in its 5th Round of assessments: "1. a significantly shorter mutual evaluation cycle, so that countries get assessed more frequently[;] 2. greater emphasis on the major risks and context to ensure that countries focus on the areas where the risks are highest[;] and 3. a results-orientated follow-up assessment process, which will focus on specific actions to tackle money laundering, terrorist financing and the financing of weapons of mass destruction."

Throughout the year, FATF engaged in continued efforts to explore the integration of technology into AML/CFT frameworks. In May 2022, the agency published a confidential report that explores how law enforcement can use technology to

investigate money laundering and terrorist findings. On June 11, 2022, the FATF hosted a "Conference on Digital Transformation," inviting leaders in the AML/CFT space as well as experts in digital fields to discuss how they might utilize new technologies toward AML/CFT work. The mission of the conference was to explore how digitally driven AML efforts and privacy/data protection might be simultaneously achieved.

On September 13, 2022, the FATF and INTERPOL held a joint conference to reinforce global asset recovery. The aims of this collaboration are: "(1) [i]ncreasing the visibility and priority of asset recovery at national level; (2) sending a clear signal that [FATF is] acting to cripple organized crime syndicates; and (3) better protect[ing] society and contribut[ing] to sustainable economic growth."

AUTHORS

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 at 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

Michael P. Gurdak
Washington
+1.202.879.5470
mpgurdak@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/Sydney
+61.3.9101.6820/+61.2.8272.0561
tlestrange@jonesday.com

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

Daniel Moloney
Melbourne
+61.3.9101.6828
dmoloney@jonesday.com

Lindsey M. Nelson
Washington
+1.202.879.3735
lmnelson@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

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

Alexander J. Wilson
New York
+1.212.326.8390
awilson@jonesday.com

Qiang Xue
Hong Kong/Beijing
+852.3189.7298/+86.10.5866.1111
qxue@jonesday.com

D. Grayson Yeargin
Washington
+1.202.879.3634
gyeargin@jonesday.com

ADDITIONAL CONTACTS

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

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

Jean-Guillaume de Tocqueville
Paris
+33.1.56.59.39.39
jgdetocqueville@jonesday.com

Kaarli H. Eichhorn
Brussels/London
+32.2.645.14.41/+44.20.7039.5959
keichhorn@jonesday.com

Dorothy N. Giobbe
New York
+1.212.326.3650
dgiobbe@jonesday.com

Aidan Lawes
London
+44.20.7039.5700
alawes@jonesday.com

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

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

Nadiya Nychay
Brussels
+32.2.645.14.11
nnychay@jonesday.com

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

Elizabeth A. Robertson
London
+44.20.7039.5204
erobertson@jonesday.com

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

Liz Saxton
London
+44.20.7039.5162
esaxton@jonesday.com

Schuyler J. Schouten
San Diego/Washington
+1.858.314.1160/+1.202.879.3844
sschouten@jonesday.com

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

Ben Witherall
Singapore
+65.6233.5532
bwitherall@jonesday.com

Special thanks to associates Sicily Maleva Kiesel, Zoë Lensing, Christina Mastrucci Lehn, Stephanie M. Pryor, Charles Smith, Darya Vakulenko, David Wu, and law clerks Beckie S. Alch and William P. Quaranta for their assistance with this White Paper.

ENDNOTES

1 *See Wildman v. Deutsche Bank*, No. 21-cv-04400, 2022 WL 17993076 (E.D.N.Y. Dec. 29, 2022); *Freeman v. HSBC Holdings, PLC*, No. 19-3970, 2023 WL 105568, at *3, *7–8 (2d Cir. Jan. 5, 2023); *Bernhardt v. Islamic Republic of Iran*, 47 F.4th 856 (D.C. Cir. 2022). Prior to the *Atchley* decision in the D.C. Circuit, a magistrate judge issued a report and recommendation in favor of dismissal in another JASTA case. *Cabrera v. Black & Veatch Special Projects Corps*., No. 19-cv -03833, 2021 WL 3508091 (D.D.C. Jul. 30, 2021) (stayed pending *Atchley v. AstraZeneca UK Ltd.*, 22 F.4th 204 (D.C. Cir. 2022) and awaiting decision on *en banc* review).

2 Plaintiffs have also increasingly targeted a greater number of industries with JASTA claims, including, but not limited to, medical supply and manufacturing companies, telecommunications companies, contractors, and social media companies. *See, e.g.*, *Atchley v. AstraZeneca UK Ltd.*, 22 F.4th 204 (D.C. Cir. 2022); *Schmitz v. Ericcson*, No. 22-cv-2317 (D.D.C. filed Aug. 4, 2022); *Cabrera v. Black & Veatch Special Projects Corps*., No. 19-cv-3833 (D.D.C. filed Dec. 27, 2019); *Gonzalez v. Google LLC*, 2 F.4th 871 (9th Cir. 2021).

3 *See* "First Corporate Anti-Terrorism Act Prosecution Marks Expansion of U.S. Counterterrorism Efforts," Jones Day *Commentary* (October 2022) (detailing first guilty plea by Lafarge S.A. for corporate material support for terrorism).

4 18 U.S.C. § 2333(d)(2).

5 No. 21-cv-04400, 2022 WL 17993076 (E.D.N.Y. Dec. 29, 2022).

6 *See, e.g., King v. Habib Bank Ltd.*, No. 20-cv-4322, 2022 WL 453789 (S.D.N.Y. Sept. 28, 2022) (denying defendant's motion to dismiss claims of aiding and abetting and conspiracy under JASTA).

7 *See, e.g.*, *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842 (2d Cir. 2021).

8 *Kaplan*, 999 F.3d at 862.

9 *Atchley*, 22 F.4th at 212–13.

10 *Id.* at 221.

11 *Id*. at 224.

12 *Bernhardt*, 47 F.4th at 868.

13 *Id.* at 868–69.

14 Petition for Writ of Certiorari, *Twitter, Inc. v. Taamneh*, No. 21-1496 (U.S. Mar. 10, 2022).

15 *See* Jones Day *Alert*, "FinCEN Issues Final Rule for Beneficial Ownership Reporting" (October 2022).