MAYER | BROWN

January 2, 2021

Legal Update

The US National Defense Authorization Act for Fiscal Year 2021: What Financial Services Companies Need to Know

The William (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 ("NDAA," the "Act"), which was enacted into law on New Year's Day when the US Congress overrode President Trump's veto of the legislation, contains a broad range of policy reforms that will impact the financial services industry, including new beneficial ownership reporting rules long sought by the industry. The Act also substantially strengthens the federal government's anti-money laundering capabilities (including new authority over crypto-assets) and contains measures to address anti-competitive behavior by China. In addition, the Act establishes a 10-year statute of limitations for the Securities and Exchange Commission ("SEC") to seek disgorgement for violations of US securities laws.

The Act also contains numerous changes that will impact government contract requirements and important cybersecurity enhancement provisions (including a Government Accountability Office study on expanding cybersecurity insurance), which will be addressed in our separate Legal Updates, *The National Defense Authorization Act for Fiscal Year 2021: Procurement Policy and Requirements* and *The National Defense Authorization Act for Fiscal Year 2021: Cybersecurity Provisions*.

This Legal Update is divided into five sections:

1. The Anti-Money Laundering Control Act of 2020
2. The Corporate Transparency Act
3. SEC Disgorgement Statute of Limitations
4. China-Related Economic Provisions
5. Miscellaneous Provisions

Section 1. The Anti-Money Laundering Control Act of 2020

The Money Laundering Control Act of 2020 ("MLCA") constitutes an entire title of the NDAA and substantially strengthens the US government's anti-money laundering/combating the financing of terrorism ("AML/CFT") enforcement apparatus through enhanced analytical capabilities, a regular process of establishing national AML priorities, and clearer authority to regulate providers of virtual currency services. Specifically, the MLCA seeks to:

- Improve coordination and information sharing among the Financial Crimes Enforcement Network ("FinCEN"), the federal functional regulatory agencies, federal law enforcement agencies, national security agencies, the intelligence community, and financial institutions;

- Modernize AML/CFT laws to adapt both government and private sector abilities to respond to new and emerging threats;
- Encourage technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and terrorist financing;
- Reinforce the risk-based approach to AML/CFT compliance; and,
- Establish uniform beneficial ownership information reporting requirements, particularly with respect to shell companies. (Discussed in Section 2 below.)

NATIONAL AML/CFT PRIORITIES

Within 180 days of enactment of the Act, the Treasury Secretary, in consultation with the Attorney General and federal and state regulators, will be required to establish and make public national priorities to govern AML/CFT policy; 180 days following the establishment of such priorities, FinCEN, in conjunction with federal and state regulators, will be required to adopt regulations to ensure compliance. These priorities are to be consistent with the national strategy for CFT and other forms of illicit finance as mandated by section 261 of the Countering Russian Influence and Europe and Eurasia Act of 2017 and refreshed every four years. Examiners are required to evaluate whether financial institutions appropriately incorporate the priorities into their risk assessments and overall AML programs. The Act formally embraces risk assessment as a component of AML compliance programs.

CLARIFYING FINCEN'S AUTHORITY TO REGULATE VIRTUAL CURRENCY PROVIDERS

While the use and trading of virtual currencies are legal practices, the Act notes that terrorists and criminals, including transnational criminal organizations, seek to exploit vulnerabilities in the global financial system and increasingly rely on substitutes for fiat currency, including emerging payment methods (such as virtual currencies), to move illicit funds. As a result, the MLCA expands the Bank Secrecy Act ("BSA") definitions of "currency exchange" and "monetary instruments" to include value that substitutes for currency or funds, clarifying FinCEN's ability to regulate virtual currency and businesses engaged in the exchange of such instruments. In addition, the Act would subject dealers in art and antiquities to AML compliance under the BSA.

ENHANCED INFORMATION SHARING

MLCA provides for the establishment of a "FinCEN Exchange," which would promote enhanced information sharing among law enforcement and national security agencies, FinCEN, and financial institutions. The FinCEN Exchange would also promote innovation and the use of enhanced technology in required reporting. Any information shared with financial institutions participating in the Exchange could only be used for identifying and reporting on activities that may involve the financing of terrorism, money laundering, proliferation financing, or other financial crimes.

The Act further provides for the establishment of three liaison programs within Treasury and FinCEN. The first liaison program, the Treasury Attaché program, will embed specialists in terrorist finance and money laundering in embassies and other locations around to world to liaise with their international counterparts to enhance efforts to combat money laundering and terrorist financing. The second liaison program will be domestically focused and be composed of FinCEN employees who would perform outreach to BSA officers at financial institutions and interact with examiners to promote consistency in AML/CFT compliance. The third liaison program designates FinCEN employees deployed internationally to engage in outreach and interact with officials of analogous foreign financial intelligence units. The Act also allocates $60 million for technical assistance to foreign countries to better develop their own AML/CFT compliance programs.

EVALUATION OF THE EFFECTIVENESS OF CURRENT BSA MANDATED REPORTING

The Attorney General is required to prepare a report, in consultation with federal and state regulators and law enforcement agencies, on the usefulness of information reported by financial institutions under the BSA. The report is to be prepared annually for the first five years following enactment and to be used by FinCEN to revise reporting provisions under the BSA. The Act also provides that when imposing suspicious activity report ("SAR") requirements, FinCEN is to consider items that include the national priorities established pursuant to the MLCA.

As part of improving BSA reporting, the Act instructs Treasury to permit streamlined reporting and automated reporting for noncomplex categories of reports and also to consider whether reporting thresholds should be adjusted. In addition, FinCEN is required to solicit feedback from law enforcement on the usefulness of information reported in SARs and, in turn, provide periodic summary reports to financial institutions on information provided in SARs that are found to be most useful for law enforcement. As part of such sharing, the Act requires FinCEN to semi-annually report on threat patterns and trend data. The semi-annual threat pattern reports are to focus on typologies, including data that may be adapted into algorithms concerning emerging money laundering threat patterns and trends. The Act also requires the Treasury Secretary to convene a team of relevant federal agencies as well as private sector experts on banking, national security, and law enforcement to meet periodically with the goal of countering illicit finance, including proliferation finance and sanctions evasion.

EXPLORATION AND UTILIZATION OF TECHNOLOGICAL INNOVATION

One difficulty financial institutions have encountered in identifying patterns of money laundering or terrorist financing is a reluctance by regulators to move away from established rules-based reporting protocols that undergird SAR and CTR reporting. To counter such reluctance, the Act includes several initiatives designed to spur the use of technology, including artificial intelligence in BSA compliance. The Act requires that the Bank Secrecy Act Advisory Group ("BSAAG")—a statutorily mandated body comprised of federal regulators, law enforcement officials, and state government, trade group, and financial institution representatives that advise Treasury on BSA compliance issues—to form a Subcommittee on Technology and Innovation to encourage technology and innovation in AML and CTF undertakings. The subcommittee is directed to reduce obstacles to innovation in current guidance and in examination practices. The Act also provides that FinCEN and financial institutions' regulators appoint BSA Innovation Officers, whose mission will be to provide outreach to state supervisors, financial institutions, trade associations and technology companies and vendors on innovative technologies that may further BSA compliance goals. Moreover, the Act requires the Treasury to issue a rule specifying the standards by which financial institutions are to test technology and innovative processes related to BSA compliance. Such processes can include the use of machine learning or other enhanced analytical processes. These standards are expected to include criteria for when and how new technologies should be risk-tested against existing approaches.

SHARING SAR INFORMATION

Over the years, FinCEN has provided guidance on the extent to which SAR information can be shared by financial institutions with their affiliates. In doing so, FinCEN has sought to balance confidentiality concerns with financial institutions' need to use the information in SARs to improve their surveillance and compliance operations. The Act authorizes FinCEN to establish a three-year pilot program that would permit a US financial institution to share information regarding filing SARs with foreign branches, subsidiaries, and affiliates. The program would generally not be permitted in certain jurisdictions, including China and Russia, unless specifically approved by the Treasury Department. Treasury could make two-year extensions of the initial three-year term after certifying to the House and Senate Banking Committees that such an extension is in the national interest.

ENHANCED COLLABORATION AMONG FINANCIAL INSTITUTIONS

The Act expands the ability of non-bank financial institutions to collaborate in terms of BSA compliance. The Act contemplates that two or more non-bank financial institutions would enter into collaborative agreements patterned on the Interagency Statement on Sharing Bank Secrecy Act Resources published by FinCEN and the federal bank supervisory agencies in October 2018. The Act instructs Treasury to engage in an outreach effort to advise financial institutions on how to structure collaborative arrangements.

CONSEQUENCES OF DE-RISKING

The MLCA also expresses the sense of Congress that financial de-risking that may trump potential AML/CFT risk can be harmful to underserved sectors of the economy. The General Accounting Office is instructed to study the issue and provide a report to the House and Senate Banking Committees within one year following enactment. The MLCA is also intended to improve AML and CFT "Communication, Oversight and Processes." This would be accomplished through enhanced coordination among federal regulatory, law enforcement, and national intelligence agencies.

ENHANCED FEDERAL COORDINATION

The Treasury Secretary is required to periodically invite state supervisors to participate in the federal interagency coordination process. The Act also calls for the establishment of a Subcommittee on Information Security and Confidentiality to be established as part of the BSAAG to advise Treasury on information security and the confidentiality implications of AML/CFT regulations.

The Act would require the federal functional regulators, FinCEN, and the IRS individually to appoint officials with a background in the BSA, federal information, or privacy laws as "Bank Secrecy Act Security Information Officers," who would have to be consulted with on BSA regulations affecting information security, information sharing under the BSA, and the development of new technologies that may strengthen information security or compliance with the BSA. In addition, FinCEN is required to establish an analytical hub, staffed with a cadre of experts capable of identifying, tracking, and tracing money laundering and terrorist financing networks. The analytical hub will work in conjunction with the federal functional regulators and state regulators to identify and analyze potential money laundering or terrorist financing schemes that examiners may identify during the examination process.

BSA NO-ACTION LETTERS

The Act requires FinCEN to assess the potential value of providing BSA no-action letters. The federal bank regulatory agencies occasionally provide periodic guidance on specific issues or practices in the form of industry letters, such as Supervision and Regulation "SR" letters published by the Federal Reserve. The SEC has a more established practice of providing no-action letters to securities industry participants who may not be certain whether a particular product, service, or action would constitute a violation of the federal securities laws. No-action letters are issued by SEC staff. In determining whether a similar no-action process would be beneficial in the context of AML/CFT compliance, the Act instructs the FinCEN Director to evaluate, among other things, whether a no-action letter process would help mitigate risk and the time that would be involved in coordinating responses to requests from the functional financial institution regulators. FinCEN is obligated to report the results of its assessment to the congressional banking committees within 180 days of enactment.

SAFE HARBOR FOR COOPERATING WITH LAW ENFORCEMENT

The Act provides a safe harbor for financial institutions that keep accounts open at the direction of law enforcement at the federal or state level. The safe harbor provision is intended to address a long-standing industry concern that the failure to close an account that has been the subject of SAR filings due to potentially illicit transactions could lead to examination criticism even when law enforcement agencies have requested that the account remain open so that they can track transaction patterns.

IMPROVED EXAMINER TRAINING

The Act requires federal regulatory agencies to develop annual training programs for examiners who perform AML/CFT compliance examinations. Training is to cover financial crime patterns, risk profiles and warning signs, the importance of AML to law enforcement, and drawbacks associated with de-risking.

ENHANCED SUBPOENA AUTHORITY OVER FOREIGN BANKS WITH US CORRESPONDENT ACCOUNTS

The Act increases the ability of Treasury and the Department of Justice ("DOJ") to subpoena records from non-US banks that maintain correspondent accounts with banks in the United States. The authority applies to alleged violations of criminal law, the BSA, and civil forfeiture actions. Foreign banks would have a right to enter an appearance in a US District Court to quash a subpoena, but subpoenas will not be quashed solely on the basis that they conflict with privacy protections in the bank's home country. Non-compliance with a subpoena can result in the assessment of fines that may equal twice the amount of the criminal proceeds involved, and Treasury can order US banks to close the affected correspondent account.

INCREASED PENALTIES FOR REPEAT OFFENDERS

To discourage repeat violations of the BSA, the Act provides for the imposition of additional penalties that would be based on three times the profit gained or loss avoided by the repeat offender or double the penalty amounts that would otherwise apply. In addition, those who are (i) convicted of crimes for which the maximum term of imprisonment is more than one year or (ii) found in civil proceedings to have willfully violated the BSA and where the violation facilitated money laundering or the financing of terrorism shall be barred from serving as a member of the board of directors of a US financial institution for 10 years. Additionally, persons convicted of BSA violations who were officers or directors of banks at the time the violation occurred must repay any bonus awarded during the calendar year. The Act adds a provision to the BSA that prohibits persons from misrepresenting or concealing information from a financial institution concerning the true ownership of assets or source of funds involved in a transaction. Violators can be sentenced up to 10 years in prison, fined $1 million, and subjected to asset forfeiture.

ENHANCED PROTECTIONS FOR WHISTLEBLOWERS

The Act also enhances whistleblower protections for those who come forward and provide Treasury, the DOJ, or the institution that is the target of a BSA crime with original information concerning the crime. Under the Act, whistleblowers who provide information that results in a successful enforcement of the BSA be awarded up to 30 percent of the amount that is collected in monetary sanctions. The Act also includes provisions that protect whistleblowers from retaliatory actions.

ANNUAL REPORTING TO CONGRESS ON DPAS AND NPAS

BSA violations are often resolved through the use of deferred prosecution agreements ("DPAs") or non-prosecution agreements ("NPAs") with the DOJ. The Act requires the Attorney General to report annually to the congressional judiciary and banking committees beginning the first year following enactment and each year thereafter for four years and provide a list of DPAs and NPAs entered into, modified, or terminated that year and an explanation of the justification for the action taken, the list of factors taken into account, and the level of coordination with other relevant agencies. The intent of the reporting requirement is to give Congress more insight into the circumstances that result in the government entering into or terminating agreements rather than prosecuting subjects of an investigation. It is possible that this added scrutiny could push the government to prosecute BSA cases rather than enter into settlement arrangements.

TAKEAWAYS

- FinCEN gains greater analytical capability and enforcement scope over virtual currency companies.
- Financial institutions have been waiting for greater regulatory encouragement in terms of utilizing machine learning and other analytical capabilities to identify money laundering and terrorist financing risk. It will be

interesting to see the extent to which the NDAA's push toward technological developments will help overcome regulatory reluctance in this area.

- The evolution of national AML/CFT priorities will help institutions adjust risk assessments and compliance program procedures, but the extent to which institutions incorporate the national priorities into their compliance programs may also raise the risk of increased examination scrutiny.
- Congressional scrutiny on the use of DPAs and NPAs and on the circumstances that result in the termination of these agreements could result in the DOJ imposing more rigorous requirements, including an increased reliance on independent monitors.

Section 2.The Corporate Transparency Act

The MLCA incorporates the Corporate Transparency Act ("CTA"), which aims to eliminate the use of US-incorporated shell companies for money laundering or terrorist financing schemes. The CTA notes that over 2,000 corporations and limited liability companies are formed annually under the laws of various states, most of which do not require information on beneficial owners at the time of formation. The CTA also points out that these corporations serve as convenient vehicles for malign actors to perpetrate a wide range of crimes. The CTA seeks to discourage the proliferation and use of shell companies through enhanced transparency of ownership information. States and tribal governments are banned by the CTA from permitting the organization of bearer share companies.

FinCEN is mandated to establish a database through which individuals seeking to form non-exempt corporations and limited liability companies organized under state or tribal law or to register corporations organized outside the United States that seek to do business in the United States would be required to register and provide information on the beneficial owners of the underlying company. Information to be reported on beneficial ownership would include name, address, date of birth, and a unique identifier number (i.e., taxpayer identification number or a passport number). Beneficial owners are defined as those who control 25 percent of the shares of a company or persons who otherwise exercise substantial control over the entity (such as the chief executive officer or chief operating officer).

The registration requirement would go into force for newly formed entities upon the enactment of implementing regulations by FinCEN. Existing corporations would have up to two years in which to fulfill their registration obligations. In the event of a change in ownership, companies would have one year to update their information, although Treasury following consultation with the DOJ could shorten the period. Upon registration, individuals or corporate entities could request FinCEN to issue them a unique identification number that could be referenced in subsequent filings with the database. Those who report incomplete or inaccurate information could be subject to civil and criminal penalties.

A wide range of companies are exempt from having to comply with the registration requirements. Exempt companies include publicly traded and SEC reporting companies, Federal Deposit Insurance Corporation ("FDIC")-insured banks and savings associations, bank and savings association holding companies, mutual funds, registered investment advisers, credit unions, broker-dealers, exchanges or clearing agencies, futures commission merchants, introducing brokers, swap dealers, retail foreign exchange dealers registered with the Commodity Futures Trading Commission ("CFTC"), public accounting firms, financial market utilities, pooled investment vehicles, political organizations, trusts, and 501(c) organizations.

In addition to being available to law enforcement, information maintained in the database would be available to financial institutions for the performance of customer due diligence. In return for receiving access to information in the database, financial institutions would have to commit to protect the confidentiality of the information and to not use it for purposes other than related to AML and CFT compliance.

TAKEAWAYS

- Enhanced transparency into the ownership of shell company structures will afford greater visibility on the part of enforcement authorities and financial institutions, yet they will remain high-risk relationships for financial institutions.

Section 3. SEC Disgorgement Statute of Limitations

The NDAA would amend the Securities Exchange Act of 1934, as amended ("Exchange Act") to provide the SEC with the explicit authority to seek disgorgement in federal court of any unjust enrichment by violators of US securities laws. The Act provides for a five- or 10-year statute of limitations, depending on the securities law violation. In either case, the statute of limitations begins to run "after the latest date of the violation that gives rise to the action or proceeding in which the [SEC] seeks the claim occurs." Claims subject to the 10-year statute of limitations must involve conduct that violates:

- Section 10(b) of the Exchange Act;
- Section 17(a)(1) of the Securities Act of 1933;
- Section 206(1) of the Investment Advisers Act of 1940; or
- Any other provision of the securities laws for which scienter must be established.

The Act provides that the 10-year statute of limitations applies to any claims for equitable remedies, "including for an injunction or for a bar, suspension, or cease and desist order" the SEC may seek.

These provisions seek to address some of the challenges the SEC has faced since the US Supreme Court decided *Kokesh v. SEC* in June 2017. The Supreme Court in *Kokesh* held that the disgorgement remedy sought frequently by the SEC operates as a penalty, and disgorgement claims are subject to a five-year statute of limitations. The Court's decision has had a demonstrable, negative impact on the SEC's enforcement efforts, especially with respect to actions involving complex, long-running frauds, such as Ponzi schemes. The SEC Enforcement Division's 2019 Annual Report estimated that the adverse ruling in *Kokesh* "caused the [SEC] to forgo approximately $1.1 billion dollars in disgorgement in filed cases," noting that the dollar amount would have been much higher had the Enforcement Division not shifted priorities in response to *Kokesh*.

The Court revisited the question of the SEC's disgorgement authority in June 2020. The Court's decision in *Liu v. SEC* provided some clarity by explaining that disgorgement could be an equitable remedy, and not a penalty, depending on the circumstances. However, the SEC's Enforcement Division later expressed the view in its 2020 Annual Report that the Court's decision in *Liu* "also imposed some limitations and left open some questions." The Act's amendments to the Exchange Act should provide a statutory fix to the difficulties faced by the SEC since the *Kokesh* decision, which will allow the SEC to move forward with more certainty in its enforcement actions in federal court.

Section 4. China-Related Economic Provisions

The NDAA includes numerous provisions intended to deter illegal and anti-competitive Chinese behavior, position the United States for strategic competition, and protect US assets from theft, improper use, or access by the Chinese government. The China-related provisions reflect Congress' consensus concern that certain actions by China present threats to US national security. Congress' position on these issues and the new measures being put in place through the NDAA signal that the focus on China will continue beyond the end of the Trump administration. The China provisions fall into several broad categories. The China-related government contract provisions are addressed in our separate Legal Update, *The National Defense Authorization Act for Fiscal Year 2021: Procurement Policy and Requirements*.

PROTECTING FEDERAL INVESTMENTS IN DEFENSE-SENSITIVE INTELLECTUAL PROPERTY

The Act tasks the President with creating a whole-of-government strategy to deter industrial espionage and cyber theft by China and demonstrate the resolve of the United States to defend its interests in cyberspace. The Act requires the strategy to include an assessment of China's actions to direct parties, including its surrogates or state-sponsored nongovernmental entities, to engage in industrial espionage or cyber theft.

ADDRESSING CHINA'S USE OF WORLD BANK ASSISTANCE

The Act establishes the pursuit of China's graduation from World Bank assistance as the official policy of the United States. Until China's graduation from assistance is achieved, the US policy will be to prioritize the funding of projects in China that contribute to the global public good. The Conference Report for the Act notes that the World Bank's International Bank for Reconstruction and Development ("IBRD") has loaned China an average of $2 billion a year, totaling more than $7.8 billion, even though China surpassed the bank's income threshold for lending in 2016. China has the world's second-largest economy and yet, through World Bank assistance, is able to obtain below-market rates for projects using IBRD loans. According to the Conference Report, China's access to this source of funds has allowed it to subsidize projects (such as those through its One Belt One Road initiative) in other countries that result in the displacement of US infrastructure projects and export opportunities.

The Act also includes a provision to increase transparency on Chinese lending. The Secretary of the Treasury is required to instruct the United States Executive Director at the World Bank to voice and vote at each international financial institution to secure greater transparency with respect to the terms and conditions of financing provided by the Chinese government to other member states that belong to that institution, consistent with the rules and principles of the Paris Club. This provision, combined with graduating China from World Bank assistance, is designed to limit China's ability to undercut global competition for projects by offering low-cost loans that are subsidized by leveraging World Bank assistance offered to China.

STUDIES AND REPORTING REQUIREMENTS ON CHINESE ECONOMIC AND SECURITY PRACTICES

The Act directs federal agencies to commission or undertake specific studies and reports on China's activities. The fact that Congress is seeking reports and strategies in these areas signals that there is bipartisan consensus that these issues may impact US national security interests and Congress may take more concrete action to address these issues in the future. Study and report provisions include:

- DoD is directed to commission an independent comparative analysis of efforts by China and the United States to recruit and retain researchers in national security-related and defense-related fields, with a particular focus on the "talent programs" used by China to recruit and retain researchers in fields related to national security.
- The Director of NIST is directed to conduct a study and provide recommendations on China's policies and influence in the development of international standards for emerging technologies (e.g., 5G wireless standards).
- The National Space Council is required to submit a report to Congress assessing the ability of the United States to compete with foreign space programs and in the emerging commercial space economy. This section would also require the President to submit a strategy to Congress that identifies market, regulatory, and other means to address unfair competition from the People's Republic of China based on the report's findings.

EXPANDING "CHINESE MILITARY COMPANIES" LIST AND REPORTING REQUIREMENTS

The Act would expand on and amend existing authority to restrict transactions and dealings involving entities designated as "Communist Chinese Military Companies" ("CCMC") under Section 1237 of the NDAA of 1999 ("Section 1237 List") in several respects.

As detailed in our recent Legal Update on the Section 1237 List, Executive Order 13959 of November 12, 2020, broadly prohibits US persons from engaging in certain securities-related transactions involving designated CCMCs. The Executive Order implements Section 1237 of the 1999 NDAA, which requires the Secretary of Defense to identify Chinese military-controlled entities operating in the United States and authorizes the use of sanctions authorities to restrict transactions and dealings involving such entities.[1]

The Act expands on the existing statutory language to: (1) enhance the reporting obligations of the Secretary of Defense through the end of 2030, (2) establish *Federal Register* publication requirements, (3) relax and inject flexibility into the consultation process, and (4) update relevant definitions while expanding the range of companies that can be listed as "Chinese Military Companies."[2]

Pursuant to the Act, the DoD List, which currently includes 35 Chinese companies, must be updated by April 15, 2021, and annually thereafter until December 31, 2030. Furthermore, the Secretary of Defense must submit an updated DoD List in classified and unclassified form—along with an explanation for any changes—to the Committees on Armed Services of the Senate and the House of Representatives and must publish the unclassified portion of the DoD List in the *Federal Register*. The requirement to update the DoD List on an ongoing basis continues to apply.[3]

The Act also does away with the requirement to consult with the Attorney General, the Director of Central Intelligence, and the Director of the Federal Bureau of Investigation. Instead, the Secretary of Defense may now consult with the head of "any appropriate Federal department or agency."[4]

Finally, the term "Communist Chinese Military Company," which was previously defined as anyone named on two Defense Intelligence Agency documents that are not publicly available (the "DIA reports") as well as "any other person that is *owned* or *controlled* by the People's Liberation Army and is engaged in providing commercial services, manufacturing, producing, or exporting," has now been shortened to "Chinese Military Company." Furthermore, its definition has been significantly expanded to include any entity that is: (i)(A) directly or indirectly owned, controlled, or beneficially owned by, or in an official or unofficial capacity acting as an agent of or on behalf of, the People's Liberation Army or any other organization subordinate to the Central Military Commission of the Chinese Communist Party; or (B) identified as a "Military-Civil Fusion Contributor" to the Chinese defense industrial base; and (ii) engaged in providing commercial services, manufacturing, producing, or exporting.[5]

Notably, the concept of "Military-Civil Fusion Contributor" reflects a significant expansion and is defined broadly to include: (A) entities knowingly receiving assistance from the Government of China or the Chinese Communist Party through science and technology efforts initiated under the Chinese military industrial planning apparatus; (B) entities affiliated with the Chinese Ministry of Industry and Information Technology, including research partnerships and projects;(C) entities receiving assistance, operational direction or policy guidance from the State Administration for Science, Technology and Industry for National Defense; (D) entities or subsidiaries defined as "defense enterprise[s]" by the State Council of the People's Republic of China; (E) entities residing in or affiliated with a military-civil fusion enterprise zone or receiving assistance from the Government of China through such enterprise zone; (F) entities awarded with receipt of military production licenses by the Government of China, such as a Weapons and Equipment Research and Production Unit Classified Qualification Permit, Weapons and Equipment Research and Production Certificate, Weapons and Equipment Quality Management System Certificate, or Equipment Manufacturing Unit Qualification; (G) entities that advertise on national, provincial, and non-governmental military equipment

procurement platforms in the People's Republic of China; and (H) any other entities the Secretary of Defense determines is appropriate.[6]

EXTENDING AND MODIFYING PROHIBITIONS ON COMMERCIAL EXPORT OF CERTAIN COVERED MUNITIONS ITEMS TO THE HONG KONG POLICE FORCE.

The Act extends and amends the existing prohibition on the commercial export of covered munition items to the Hong Kong Police Force contained in the 20019 appropriations bill (the "HK Covered Munition Act").[7] The HK Covered Munition Act prohibited the issuance of licenses to export certain types of crowd control items, including tear gas, pepper spray, rubber bullets, foam rounds, bean bag rounds, pepper balls, water cannons, handcuffs, shackles, stun guns, and tasers. The Act amends the name of the HK Covered Munition Act and makes clarifying revisions to note that the export ban extends to "covered munitions and crime control items." However, the NDAA amendments appear to be only clarifying in nature, as the definition of "covered munitions and crime control items" in the NDAA maintains the same list of items covered by the HK Covered Munition Act with no modifications. The export ban on covered munitions and crime control items has now been extended until December 31, 2021.

Section 5. Miscellaneous Provisions

KLEPTOCRACY ASSET RECOVERY REWARDS PILOT PROGRAM

The Act establishes the Kleptocracy Asset Recovery Rewards Pilot Program at the Department of Treasury for the purpose of paying rewards to individuals who provide information that assists in "retraining, seizing, forfeiting or repatriating stolen assets linked to foreign government corruptions." To qualify for the reward, an individual must provide information that leads to (1) the restraining or seizure, forfeiture, or repatriation of stolen assets "in an account at a U.S. financial institution (including a U.S. branch of a foreign institution), that come within the United States, or that come within the possession or control of any United States person." Absent a presidential waiver, the total amount of reward payments is capped at $25 million in any calendar year. The pilot program is authorized for three years.

COMBATING RUSSIAN MONEY LAUNDERING ACT

The Act incorporates the Combating Russian Money Laundering Act, which expands the Treasury Secretary's authority to address Russian illicit financing by authorizing the Treasury Secretary to prohibit or impose conditions on the transmittal of funds by domestic financial institutions or domestic financial agencies in cases where such funds are used by specified entities or in specified transactions under Section 5318A(b) of Title 31 that are a primary money laundering concern in connection with Russian illicit finance. The Treasury Secretary is also required to report to Congress not later than one year after the enactment of the Act on whether any new regulations, statutes, or other measures are needed to identify, prevent, and combat money laundering linked to Russia.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Andrew Olmem
+1 202 263 3006
aolmem@mayerbrown.com

Tamer A. Soliman
+1 202 263 3292
tsoliman@mayerbrown.com

Thomas J. Delaney
+1 202 263 3216
tdelaney@mayerbrown.com

Christina M. Thomas
+1 202 263 3344
cmthomas@mayerbrown.com

Margaret-Rose Sales
+1 202 263 3414
msales@mayerbrown.com

Tiffany L. Smith
+1 202 263 3882
tsmith@mayerbrown.com

Endnotes

[1] Section 1237 authorizes the President to exercise a broad range of powers set forth in section 203(a) of the International Emergency Economic Powers Act ("IEEPA") to investigate, regulate, and impose prohibitions against Chinese military companies, whenever such companies conduct any commercial activity in the United States. In practice, the IEEPA powers are frequently used to impose comprehensive or targeted sanctions against individuals and entities under various US sanctions programs. Under Section 1237, the Secretary of Defense was required to publish within 90 days from enactment of the FY1999 NDAA (and update as appropriate on an ongoing basis) a list of Chinese military companies operating in the United States after consultation with the Attorney General, the Director of Central Intelligence, and the Director of the Federal Bureau of Investigation. However, the first list of Chinese military companies ("DoD List") was not released until June 24, 2020. The DoD List has since been supplemented and an Executive Order was issued on November 12, 2020, barring American investments on listed Chinese military companies. (See our previous Legal Update on this subject.)

[2] FY2021 NDAA at § 1260H.

[3] FY2021 NDAA at § 1260H(b).

[4] *Id.* at § 1260H(c).

[5] *Id.* at § 1237(b)(4) (emphasis added). The two lists are VP–1920–271–90 and PC–1921–57–95, published by the Defense Intelligence Agency ("DIA") in September 2990 and October 1995, respectively, and any update of those publications. The Defense Intelligence Agency is a DoD agency that "provide[s] military intelligence to warfighters, defense policymakers and force planners in the Department of Defense and the Intelligence Community, in support of U.S. military planning and operations and weapon systems acquisition." *See* DIA website here: https://www.dia.mil/About/; FY2021 NDAA at § 1260H(d)(1).

[6] *Id.* at § 1260H(d)(2).

[7] "An Act to prohibit the commercial export of covered munitions items to 15 the Hong Kong Police Force." approved November 27, 16 2019 (Public Law 116–77; 133 Stat. 1173).