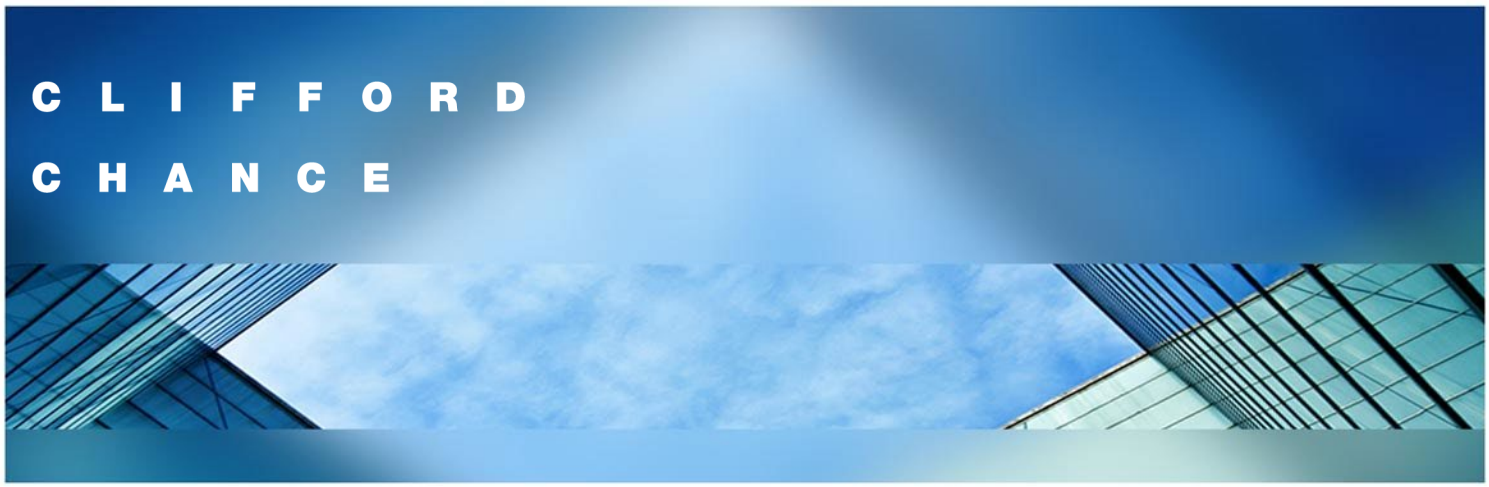


# SWEEPING AML REFORM LEGISLATION ENACTED AS PART OF THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021

On January 1, 2021, Congress passed into law the National Defense Authorization Act for Fiscal Year 2021, which includes the Anti-Money Laundering Act of 2020 (the "**Act**"), the most sweeping anti-money laundering ("**AML**") legislation since the enactment of the USA PATRIOT Act of 2001. The Act represents the culmination of years of legislative and policy work to reform, modernize and strengthen the US AML and countering the financing of terrorism ("**CFT**") regime. The Act follows and incorporates provisions from a number of recent legislative initiatives, including The Corporate Transparency Act of 2019 (H.R. 2513), The COUNTER Act of 2019 (H.R. 2514), and The Illicit Cash Act (S. 2563). The Act also largely carries out the 2020 National Strategy for Combating Terrorist and Other Illicit Financing prepared by the Department of the Treasury in consultation with the Departments of Justice, State, and Homeland Security, the Office of the Director of National Intelligence, and the staffs of the federal functional regulators. It also advances recent regulatory initiatives to re-examine the AML regulatory framework intended to upgrade and modernize the US AML regime to address emerging and evolving threats while providing financial institutions with additional flexibility in addressing these threats.[1]

---

[1] *See e.g., Anti-Money Laundering Program Effectiveness*, Advance Notice of Proposed Rulemaking, 85 Fed. Reg. 58023 (Sept. 17, 2020) (seeking comments on, inter alia, proposed regulatory amendments clarifying that covered financial institutions must maintain an "effective and reasonably designed" AML program, setting out definition and core elements of AML program "effectiveness," and establishing an explicit requirement for an AML risk-assessment).

Attorney Advertising: Prior results do not guarantee a similar outcome

Key AML reform initiatives implemented by the Act include mandating steps to streamline and enhance Suspicious Activity Report ("**SAR**") and Currency Transaction Report ("**CTR**") filing requirements under the Bank Secrecy Act ("**BSA**"), the creation of a federal beneficial ownership registry, enhancing coordination and information sharing between relevant regulatory and enforcement agencies, as well as between banks and between banks and law enforcement, and fostering responsible innovation, including the use of artificial intelligence and data analytics for AML compliance purposes. The Act also covers a number of other AML reform topics, including reinforcing the risk-based approach to countering money laundering and terrorist financing, addressing "de-risking," strengthening international cooperation, clarifying and updating the application of AML rules to digital assets, strengthening enforcement tools such as the scope of subpoena authority over foreign banks with US correspondent accounts, and increasing penalties for AML violations, providing new whistle-blower incentives and protection, and mandating a number of studies and reviews in view of further modernization and enhancements to the AML regulatory framework. We briefly discuss key aspects of the Act below.

## Enhancements to SAR and CTR Filing Requirements

One of the key AML reform policy goals has been the modernization of SAR and CTR filing requirements to address the usefulness and burden imposed on financial institutions by these requirements. In that regard, the Act requires the Secretary of the Treasury, in consultation with relevant federal enforcement and regulatory authorities, to conduct a formal review of the SAR and CTR filing requirements currently in effect within a year of the enactment of the Act and propose rulemaking, as appropriate, implementing changes to such reports to reduce any unnecessarily burdensome regulatory requirements and ensure that the information provided is highly useful in safeguarding the national security and financial system of the United States, combatting money laundering and financing of terrorism, and conducting related criminal or regulatory investigations, risk assessments or proceedings. The Act also amends existing statutory provisions requiring the filing of SARs to, among other things, mandate the establishment of streamlined, including automated, processes for the filing of noncomplex categories of reports that reduce burdens imposed on persons required to report and include standards ensuring that such streamlined reports relate to suspicious transactions relevant to potential violations of law.

Further, the Act requires the Attorney General, in consultation with the Secretary of the Treasury, federal law enforcement agencies, federal functional regulators, and other appropriate federal Agencies, to prepare an annual report setting out certain information about the use of data derived from reports filed by financial institutions pursuant to the requirements of the BSA, including, among other things, frequency with which reported data contains actionable information, number of legal entities and individuals identified in reported data, and information on the extent to which arrests, indictments, convictions, and other criminal or civil actions were taken using reported data. Among other things, these annual reports are to be used by the Secretary of the Treasury to assess the usefulness of BSA reports and assist the Financial Crimes Enforcement Network ("**FinCEN**") in considering revisions to such reporting requirements.

The Act also requires the Secretary of the Treasury, in consultation with federal and state enforcement and regulatory authorities, to conduct a review of the thresholds for filing SARs and CTRs and a make a determination as to whether such thresholds should be adjusted. The Secretary must conduct this review within a year from the enactment of the Act and propose rules, as appropriate, implementing its findings and determinations.

In addition, the Act requires FinCEN to publish semi-annual reports on threat pattern and trend information to provide guidance about the preparation and use of SARs and other reports filed by financial institutions. These reports must also contain information about the techniques used in money laundering or terrorist financing, and include corresponding trends data that can be adapted in algorithms/fed into machine learning, if appropriate.

## New CFT Program Requirements

Currently, financial institutions are required under the BSA and its implementing rules to implement an AML compliance program meeting minimum statutory and regulatory requirements and standards. With respect to CFT and sanctions compliance, guidance by the federal regulatory and enforcement agencies indicates that financial institutions should implement CFT compliance policies and procedures but, as a technical matter, there are no federal statutory provisions requiring financial institutions to adopt and implement a CFT compliance program. The Act would statutorily require covered financial institutions to establish risk-based CFT programs that meet minimum standards set by the Secretary of Treasury.

Although financial institutions generally already have CFT policies and procedures to ensure sanctions/CFT compliance and mitigate related compliance and enforcement risks, the specific CFT program requirements imposed by the Act will likely create a new regulatory compliance risk for financial institutions related to CFT program deficiencies and potential failure to meet the minimum regulatory requirements and standards for such programs. While in the past sanctions-related enforcement cases have generally been triggered by pervasive sanctions/CFT violations, the new CFT program requirements could potentially trigger enforcement actions for failure to meet minimum program requirements and standards, even in the absence of material sanctions/CFT violations. It is only a small consolation that the Act amends the current provisions requiring the implementation of minimum standards for AML programs by directing the Secretary of the Treasury to take into account, among other things, the financial burden that these CFT compliance requirements will impose on financial institutions.

## Reinforcing the Risk-Based Approach to AML Compliance and Addressing De-Risking

One of the stated purposes of the Act is "*to reinforce that the anti-money laundering and countering the financing of terrorism policies, procedures, and controls of financial institutions shall be risk-based*." In that regard, amendments implemented by the Act to AML/CFT compliance program requirements explicitly state that the required AML/CFT programs should be risk-based and, consistent with the financial institution's risk profile, should ensure that more resources and

attention are directed towards higher-risk customers and activities. The Act also directs the Secretary of the Treasury, in consultation with federal regulatory and law enforcement agencies, to conduct a formal review of the BSA/AML regulations and guidance to, among other things, ensure their usefulness and effectiveness and identify any regulations or guidance that are redundant, outdated or do not promote a risk-based approach to AML/CFT compliance. These provisions build on a number of recent regulatory initiatives to reinforce the risk-based approach to AML/CFT compliance, including, for example, the April 15, 2020, update to the BSA/AML examination manual – the first revisions to the BSA/AML examination manual since 2014 – intended to clarify the risk-focused approach to AML examinations that is used by the federal banking regulators.[2] The reinforcement of the risk-based approach in the statute is helpful, because, while the risk-based principle has long been a cornerstone of BSA/AML compliance, examiners have not always adhered to that principle and have criticized institutions for not adopting procedures and controls deemed necessary without regard for the institution's risk profile.

Further, the Act acknowledges the "de-risking" phenomenon and its potential adverse impacts on transparency and transaction traceability which are crucial for ensuring the integrity of the international financial system, as well as the impact of de-risking on financial inclusion and alleviation of human suffering. The Act defines "de-risking" to mean "*actions taken by a financial institution to terminate, fail to initiate, or restrict a business relationship with a customer, or a category of customers, rather than manage the risk associated with that relationship consistent with risk-based supervisory or regulatory requirements, due to drivers such as profitability, reputational risk, lower risk appetites of banks, regulatory burdens or unclear expectations, and sanctions regimes*."

Tackling the de-risking phenomenon has proven to be particularly challenging and the Act does not provide any immediate solutions but it does mandate steps intended to alleviate the de-risking issues. In particular, the Act directs the Comptroller General of the United States to conduct an analysis and prepare a report identifying options for financial institutions to handle high risk transactions and accounts without compromising AML/CFT requirements. The Act also directs the Secretary of the Treasury, in consultation with state and federal regulatory agencies and other appropriate stakeholders, to conduct a formal review of BSA/AML regulations and guidance, relying substantially on the de-risking report prepared by the Comptroller General, and propose changes, as appropriate, to reduce any unnecessarily burdensome regulatory requirements. Within a year after the completion of the foregoing review, the Secretary would have to develop a de-risking strategy to reduce the adverse consequences related to de-risking.

## Beneficial Ownership Reporting Requirements

The lack of state requirements to collect beneficial ownership information at the time of company formation and after changes in ownership was among the more significant perceived gaps and vulnerabilities in the US AML/CFT framework. The

[2] *See also Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision* (available at: https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-81a.pdf).

lack of such requirement hindered the ability of regulated entities to mitigate risks[3] and law enforcement's ability to swiftly investigate entities created to hide ownership. FinCEN's Customer Due Diligence Rule,[4] which became effective in May 2018, addressed some of these issues but had various exceptions and was dependent in part on self-disclosure regarding beneficial owners from the company. The Act contains provisions imposing mandatory beneficial ownership reporting requirements (dubbed "The Corporate Transparency Act") that establish "secure, nonpublic database" within FinCEN for beneficial ownership information intended to help financial institutions and enforcement and regulatory agencies identify entity beneficial owners. Covered entities (each called a "reporting company") must submit a report to FinCEN identifying "each beneficial owner" as well as "each applicant with respect to that company" by their: (i) full legal name; (ii) date of birth; (iii) current residential or business street address; and (iv) unique identifying number (e.g., passport number, FinCEN identifier). If there is a change in beneficial ownership, the reporting company must report such change to FinCEN within one year.

These obligations apply to any corporation, limited liability company, or "other similar entity" that is: (i) created by filing with a domestic secretary of state (or equivalent); or (ii) a foreign entity that registered to do business in the United States by filing with a domestic secretary of state (or equivalent). Importantly, the bill excludes a number of entities from the definition of a "reporting company," including, *inter alia*, banks and bank holding companies, registered investment companies and other financial institutions registered with the U.S. Securities and Exchange Commission ("**SEC**") or the Commodity Futures Trading Commission, issuers that are registered or required to file certain reports under the US securities laws, and governmental entities. Such entities are thus exempt from the beneficial ownership reporting requirements.

The reporting obligations are also retroactive: any reporting company formed or registered before the effective date of the law must report the information detailed above to FinCEN "*in a timely manner, and not later than 2 years after the effective date*" of the Treasury's forthcoming regulations, which must be promulgated no later than one year after the enactment of the Act.

FinCEN will retain beneficial ownership information for each reporting company for no less than 5 years after the date of dissolution of the reporting company and generally shall keep such information confidential. FinCEN is authorized to disclose confidential beneficial ownership information only pursuant to protocols established by regulations that protect the security and confidentiality of such information to law enforcement and appropriate regulatory agencies, as well as a financial institution subject to customer due diligence requirements with the consent of the reporting company.

In contrast to a previous version of this portion of the Act, about which Clifford Chance wrote here, penalties attach upon "willful" (rather than "knowing") violation of the beneficial ownership disclosure requirements. Any person who willfully: (i) provides or attempts to provide false or fraudulent beneficial ownership

---

[3] Covered financial institutions are generally required to identify and verify the identities of beneficial owners of legal entity customers at the time of account opening and defined points thereafter.

[4] *See Customer Due Diligence Requirements for Financial Institutions*, 61 Fed. Reg. 29398 (May 11, 2016).

information, or (ii) fails to report complete or updated beneficial ownership information, is liable for a civil penalty of not more than $500 per day that the violation continues and may be fined not more than $10,000, and/or may be imprisoned for no more than 2 years. A limited safe harbor provision allows a person who previously submitted inaccurate information to cure the defect within 90 days of submission if they also submit a report containing the corrected information. The penalty provisions state only that a person "shall be liable to the United States" for the respective civil penalties, and it is unclear which enforcement agency will be responsible for investigating violations and assessing such penalties. The placement of these provision and the surrounding language indicate, however, that, in addition to criminal enforcement authorities, the Secretary of the Treasury/FinCEN itself may enforce the beneficial ownership reporting requirements.

## Interagency and Public-Private Information Sharing and Cooperation

Information sharing and collaboration among financial institutions and between the government and the private sector is essential for the effectiveness and efficiency of the AML regime. While PATRIOT Act Sections 314(a) and 314(b) have provided information sharing mechanisms, enhancing the use of interagency and public-private partnerships for information sharing and cooperation has been a longstanding focus of AML regulatory reform efforts, considering that such information sharing and cooperation is crucial for the effectiveness of the AML regime. In that regard, the Act incorporates certain important information sharing and cooperation mechanisms and tools outlined below that promise to improve transparency and insight into money laundering and terrorist financing typologies and structures and should facilitate AML/CFT efforts and increase cooperation among relevant law enforcement and regulatory agencies and the private sector.

*FinCEN Exchange*. The Act establishes a so-called "FinCEN Exchange," within FinCEN, to facilitate a "*voluntary public-private information sharing partnership*" between FinCEN and law enforcement agencies, national security agencies, and financial institutions. The Act permits the Director of FinCEN (the "**Director**") to share such information shared through the FinCEN Exchange in his or her sole discretion; the information can be shared with the "appropriate" federal functional regulator,[5] provided the information is shared in such a way as to "ensure the appropriate confidentiality of personal information," (and also in compliance with all other "applicable" federal laws). More detailed guidance on what confidentiality procedures should be implemented are promised in the ensuing regulations.

*FinCEN Domestic Liaisons*. The Act establishes within FinCEN an Office of Domestic Liaison to, among other things, perform outreach to BSA officers at financial institutions, coordinate with regulatory agencies, promote coordination and consistency of AML supervisory guidance, and act as liaison between financial institutions and their state and federal regulators with respect to BSA information sharing matters.

[5] This defined term has the meaning ascribed to it in the Gramm-Leach-Bliley Act, and includes any federal regulator that examines a financial institution for compliance with the Bank Secrecy Act. § 6003(3).

*Sharing Information on Usefulness of SARs*. The Act requires FinCEN, to the extent "practicable," to periodically solicit feedback from BSA compliance officers at a cross-section of reporting financial institutions regarding SARs filed and discuss observed trends in suspicious activity and to share such feedback with relevant state and federal regulatory agencies. The Act also requires FinCEN to make periodic disclosures, to the extent "practicable," to each financial institution, in summary form, of information about SARs filed that "proved useful" to federal or State criminal or civil law enforcement agencies. These disclosures will also include information from the Department of Justice ("**DOJ**") regarding its review and use of SARs filed by the institution, as well as any trends in suspicious activity observed by DOJ.

*Authorization of Information Sharing with Foreign Affiliates*. The Act amends 31 U.S.C. § 5318(g) to require the Secretary of the Treasury to promulgate rules implementing a pilot program for sharing SARs information with the foreign branches, subsidiaries, and affiliates of a financial institution (the "**Pilot Program**"). Currently, SARs confidentiality provisions generally prohibit the sharing of SARs with foreign branches, subsidiaries, and affiliates. Among other things, the Pilot Program would permit financial institutions with a SAR reporting obligation to share relevant information, including that a SAR has been filed, with its foreign branches, subsidiaries and affiliates in certain jurisdictions "for the purpose of combating illicit finance risks." A financial institution may not share information on SARs with its foreign branches, subsidiaries, or affiliates in: (i) China; (ii) Russia; or (iii) a jurisdiction that is designated as a state sponsor of terrorism, subject to US sanctions, or determined by the Secretary to be unable to reasonably protect the security and confidentiality of such information. Exceptions to the exception (i.e., circumstances where information sharing is permissible with a foreign counterpart in either Russia or China) may be made by Treasury on a case-by-case basis, if within the national security interest of the United States. These information sharing authorizations should enable US financial institutions to better manage AML/CFT compliance risks on an enterprise-wide basis but they come with some additional risk exposure – the Act also allows Treasury to implement rules holding a foreign affiliate of a US financial institution liable for disclosure of information related to SARs under this section.

*Collaborative Arrangements Among Financial Institutions*. The Act explicitly authorizes and endorses collaborative arrangements between two or more financial institutions, as described in the 2018 Interagency Statement on Sharing Bank Secrecy Act Resources.[6] These collaborative arrangements allow financial institutions to pool resources to manage their BSA/AML obligations, and the Act extends permission to do so "in order to more efficiently comply with" BSA/AML requirements. As specified in the Interagency Statement, this authorization does not apply to collaborative arrangements formed for the purpose of sharing information under Section 314(b) of the PATRIOT Act. A financial institution is not entirely left adrift, however, in how to implement these collaborative arrangements; the Act promises that Treasury and appropriate regulators will perform an outreach program to provide financial institutions with best practices guidance.

[6] *See* https://www.fincen.gov/news/news-releases/interagency-statement-sharing-bank-secrecy-act-resources.

*Encouraging Interagency and Public-Private Consultation and Cooperation*. The Act also requires the Secretary of the Treasury to: (i) invite state banking regulators, as appropriate, to participate in interagency consultation and coordination with federal banking regulators regarding the promulgation of AML rules; and (ii) convene a supervisory team of relevant federal agencies, private sector experts in banking, national security, and law enforcement, and other stakeholders to examine strategies to increase cooperation between the public and private sectors for purposes of countering illicit finance, including proliferation finance and sanctions evasion.

*BSA No-Action Letter Issuance Process*. The Act requires an assessment of whether FinCEN should establish a formal process for the issuance of BSA/AML no action letters, including an analysis of whether a formal no-action letter process would help or mitigate or accentuate illicit finance risks. The Secretary of the Treasury shall prepare a report to Congress containing the findings and determinations made in carrying out the foregoing assessment and shall propose, as appropriate, rules implementing such findings and determinations.

## International Cooperation & Information Sharing

In addition to enhancements to domestic information sharing and cooperation, the Act also contains a number of provisions designed to foster information sharing and cooperation with foreign AML/CFT regulatory and enforcement authorities. The Act directs the Secretary of the Treasury to work with foreign counterparts, the Financial Action Task Force, the International Monetary Fund, the World Bank, the Egmont Group of Financial Intelligence Units, the Organization for Economic Co-operation and Development, the Basel Committee on Banking Supervision, and the United Nations, to promote stronger AML frameworks and enforcement of AML laws.

To promote information sharing with foreign AML/CFT regulatory and enforcement authorities, the Act generally provides protection from disclosure of information exchanged with foreign law enforcement, financial intelligence units and other AML/CFT authorities, but carves out from such protection the provision of such information to Congress and the US courts in an action commenced by the United States. Further, the Act includes funding for the provision of technical assistance to foreign countries and foreign financial institutions that promotes compliance with international AML/CFT standards and best practices. The Act also requires the appointment of no fewer than 6 "Treasury Financial Attachés" and no fewer than 6 FinCEN "Foreign Financial Intelligence Unite Liaisons" that, among other things, shall be co-located in a US embassy or similar facility and shall establish and maintain relationships with foreign counterparts in furtherance of AML/CFT information sharing and cooperation.

## Enhanced Subpoena Authority over Foreign Banks with US Correspondent Accounts

Currently, Section 319(b) of the PATRIOT Act (31 U.S.C. § 5318(k)) authorizes the Secretary of the Treasury and the Attorney General to "*issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of*

*funds into the foreign bank*." Further, the existing PATRIOT Act provisions authorize the Secretary of the Treasury or the Attorney General to require the termination of any correspondent relationship with a foreign bank if the foreign bank fails to comply with a summons or subpoena issued under such authority. The Act contains a number of provisions that enhance this administrative subpoena authority.

More specifically, the Act amends 31 U.S.C. § 5318(k) to authorizes the Secretary of the Treasury or the US Attorney General to subpoena any records, including records stored outside the United States, relating to the correspondent account or any account at the foreign bank that are the subject of: (i) a US criminal investigation; (ii) any investigation of AML violations; (iii) a civil forfeiture action; or (iv) an investigation related to special measures authorized under Section 311 of the PATRIOT Act (31 U.S.C. § 5318A) with respect to jurisdictions, financial institutions, or international transactions of primary money laundering concern. This is a significant expansion on the type and scope of records the Secretary of Treasury or Attorney General could request through their existing subpoena authority under Section 319(b) of the PATRIOT Act, which was previously limited to records related to the correspondent account. The Act also amends Section 319(b) of the PATRIOT Act to specify how a foreign bank must produce records pursuant to a Section 319(b) subpoena and that an assertion that compliance with the subpoena would conflict with foreign confidentiality or privacy law shall not be the sole basis for quashing or modifying such as subpoena. The Act also strengthens the enforcement tools under Section 319(b) to compel compliance with a subpoena issued under that section.

## Whistleblower Incentives and Protection

Among the most impactful provisions of the Act are likely to be the substantial amendments and enhancements to the existing whistleblower protections and whistleblower awards provided for under the BSA (31 U.S.C. § 5323, 5328). In contrast to the existing provisions that cap the potential whistleblower award at $150,000 or 25% of the net amount of the fine, penalty, or forfeiture collected, whichever is less, the Act provides that a whistleblower who voluntarily provides original information leading to a successful enforcement action may receive up to 30% of the monetary sanctions eventually imposed if the sanction exceeds $1 million. The amount of the award is determined by the Secretary of the Treasury, considering the following criteria: (i) the significance of the information provided; (ii) the degree of assistance provided by the whistleblower and any legal representative of the whistleblower; (iii) the Treasury Department's interest in deterrence; and (iv) any other relevant factors the Secretary of the Treasury may establish. There is no minimum award guarantee under the statute to a whistleblower that provides information leading to a successful enforcement action, but the Treasury appears to have discretion to provide for a minimum award by regulation. In addition, the Act's amendments implement stronger whistleblower protections, including, among other things, creating a private right of action for whistleblowers who have suffered retaliation.

The new whistleblower incentives and protections established by the Act are in many respects similar to the whistleblower provisions of the Securities Exchange Act of 1934 enacted by the Dodd-Frank Act of 2010 and administered by the SEC.

In recent years the SEC has announced numerous whistleblower awards under these provisions, ranging from hundreds of thousands to over 100 million dollars (available at: https://www.sec.gov/whistleblower/pressreleases), providing a clear indication of the potential sweeping impact that the new whistleblower incentives are likely to have in the AML enforcement space.

## Strengthening of BSA/AML Enforcement Tools and Penalties

The Act adds another four tools to an enforcer's toolkit significantly increasing the scope of possible penalties for BSA/AML violations as outlined below.

First, the Act piles on hefty additional penalties for repeat violators of the BSA. If a person has previously violated a provision of the BSA or a rule issued thereunder, the Secretary of the Treasury may, "if practicable," impose an *additional* civil penalty of not more than: (i) three times the profit gained or loss avoided by such person as a result of the violation; or (ii) two times the maximum penalty with respect to the violation. This discretionary civil penalty can stack on top of the criminal or civil fines permitted under 31 U.S.C. §§ 5321, 5322. This new additional penalties authority magnifies exponentially the risks that financial institutions are facing, particularly considering the long string of record-breaking draconian fines levied against financial institutions for AML violations. A small comfort: this stacking provision is fully prospective. For purposes of determining whether a person has previously violated the BSA, that determination is limited to violations occurring after the Act's date of enactment. That said, this provision dramatically alters the risk calculus for financial institutions with respect to AML compliance.

Second, the Act provides for additional criminal fines under Section 5322, by adding a clause *requiring* a court to fine a defendant in the amount equal to the profit gained "by reason of" the relevant BSA violation "in addition to *any other fine under this section*." In theory, a court could therefore: (i) issue the applicable criminal penalties in the current version of Section 5322; (ii) levy an additional criminal fine of the profit gained by such a violation (as determined by the court); *and*, if the defendant is a repeat offender, (iii) pile on the discretionary civil penalty outlined above.

Third, in concert with the mandatory court-issued fine of profit gained, the Act also adds that if the guilty party is an individual who was a "partner, director, officer, or employee" of a financial institution at the time, they must repay any bonus paid to them by the financial institution during either the calendar year in which the violation occurred, or the calendar year following such violation. The Act does not specify how to determine which year's bonus must be repaid. Again, both this provision and the provision outlined in the prior paragraph are *mandatory*, not discretionary – the law as currently drafted states that the person "shall" pay.

Fourth, an individual who commits an "egregious violation" of the BSA will be banned from serving on the board of directors of any US financial institution for 10 years after the entry of a judgment. An egregious violation is a defined term and means that the individual is convicted of a BSA-related felony or found guilty of a willful civil violation that facilitated money laundering or the financing of terrorism. An important caveat: this portion of the Act is currently ambiguously drafted as an "and." While ambiguous, the prudent approach is to assume that the drafters

intended the bar to apply to individuals who *either* are found guilty of a related felony, *or* are liable for an eligible civil offense (not necessarily both).

In addition, the Act requires the Attorney General to submit to Congress an annual report listing all deferred prosecution agreements and non-prosecution agreements relating to BSA/AML violations entered into, amended, or terminated during the relevant year. The report must be more fulsome than a simple list and must include (i) the justification for entering into, amending, or terminating the agreement; (ii) the list of factors that were taking into account; and (iii) the extent of coordination between the Attorney General, Treasury, and other regulators before taking such action.

## Criminal Prohibitions on Concealing Material Facts in a "Monetary Transaction"

The Act adds two new criminal prohibitions on concealing material facts in "monetary transactions" (defined broadly to cover financial transactions involving monetary instruments, including, among other things, deposits, withdrawals, and funds transfers). For criminal liability to attach under these provisions, the person must knowingly conceal (or attempt to conceal) a "material fact" concerning the monetary transaction ("material fact" is not a defined term in the Act.)

First, if the person knowingly conceals a material fact concerning the *ownership or control* of assets involved in a monetary transaction, criminal penalties apply only if: (i) the person or entity who owns or controls the assets is a politically exposed person ("**PEP**") or relative/close associate of a PEP; and (ii) the aggregate value of the assets involved in one or more monetary transaction is at least $1 million.

Second, if the person knowingly conceals a material fact concerning the *source of funds* involved in a monetary transaction, criminal penalties apply if: (i) the transaction involves an entity found to be of primary money laundering concern under Section 311 of the PATRIOT Act (31 U.S.C. § 5318A); and (ii) the transaction violates the special measures prescribed under that section.

Corresponding penalties are steep, though both new prohibitions are phrased as "ands" – both conditions must be met for criminal liability to attach – and therefore will likely apply infrequently. Any person convicted of either new prohibition, or conspiracy to commit the same, "shall" be imprisoned for a maximum of 10 years, fined a maximum of $1 million, or both. Moreover, the Act specifically provides for mandatory criminal forfeiture of "any property involved in the offense and any property traceable thereto," as well as discretionary civil forfeiture.

## Fostering Innovation, FinTech and RegTech Provisions

The Act builds on a number of recent initiatives intended to foster innovation and use of AI and other technologies (RegTech) for AML compliance purposes.[7] Several provisions in the Act address the need to tailor and implement compliance efforts and innovative tools, such as machine learning and other enhanced data analytics tools that are sufficiently capable of tracking complex transactions and

[7] *See e.g., Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (December 3, 2018) (available at: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf); *OCC Interpretive Letter No. 1166* (Sept. 27, 2019) (concerning automated generation of SAR narratives); and FinCEN's Innovation Hours Program launched in May 2019 (*see* https://www.fincen.gov/resources/fincens-innovation-hours-program).

identifying AML and CFT-related risks. For example, the Act amends 31 U.S.C. § 5318 to require the Secretary of the Treasury to issue a rule specifying standards against which financial institutions should, on a risk-basis, test their technology and technology internal processes.

Further, the Act establishes within the BSA Advisory Group a Subcommittee on Innovation and Technology (the " **Subcommittee**") to advise the Secretary of the Treasury and other stakeholders on promoting technological innovation in regards to AML/CFT. The Subcommittee will also focus, "to the extent practicable," reducing regulatory burdens to employing innovative technology in AML/CFT compliance. The Act also requires appointment of an Innovation Officer at FinCEN and each federal functional regulator to (i) provide outreach to law enforcement agencies, state banks supervisors, financial institutions, and other stakeholders, including technology companies and service providers, regarding "innovative methods, processes, and new technologies that may assist in compliance with" BSA requirements; (ii) provide financial intuitions and other stakeholders with technical assistance and guidance for implementing "responsible innovation" and technology consistent with BSA requirements; and (iii) "if appropriate" consider public-private partnerships related to innovative technology and/or create metrics of success for innovation and technology.

In addition, the Act establishes a Financial Crimes Tech Symposium to "promote greater international collaboration to prevent and detect financial crimes and suspicious activities" and focus on ways new technology can help monitor and prevent illicit activities. The Act also requires the Director of FinCEN to brief the Senate Committee of Banking, Housing, and Urban Affairs and the House's Committee on Financial Services on the use of emerging technologies, including, among other things, FinCEN's use of innovative technologies such as AI, digital identify technologies, and distributed ledger technologies, and also the efficiency of FinCEN's current use of such technology and the potential to better leverage these technologies in support of FinCEN's analysis and enforcement activities. The briefing will also include any policy recommendations regarding cooperation with the private sector in regards to implementing new technologies in AML/CFT compliance programs.

The Act also requires FinCEN to maintain a FinCEN Analytical Hub of financial experts to identify, track, and trace money laundering and terrorist-financing networks in support of criminal and civil investigations.

Finally, the Act includes provisions codifying the application of the AML framework to entities facilitating virtual currency transactions. In particular, the Act amends the definition of "financial institution" in 31 U.S.C. § 5312(a) to include entities engaged in the transmission of "currency, funds, or value that substitutes for currency". Further, the Act carries this definition across to the registration requirement for money services businesses ("**MSBs**"), making it clear that entities facilitating virtual currency transactions must register with FinCEN as MSBs and are required to implement AML/CFT compliance programs. These provisions essentially codify previous FinCEN guidance addressing MSB registration for entities facilitating virtual currency/cryptocurrency transactions (see our discussion here).

## Conclusion

As discussed above, the Act implements sweeping reforms to the US AML/CFT regime. It is the most comprehensive AML legislation in nearly 20 years and the result of years-long effort to modernize, strengthen, and streamline the BSA/AML regulatory framework and bring into focus risk-based compliance and enforcement priorities. Because many of the Act's mandates require additional reporting, study, and rulemaking, with certain such requirements occurring under prescribed timelines, the rollout of many of the reform measures implemented by the Act will take time. In the wake of these developments, financial institutions and other stakeholders should monitor the rollout of the AML/CFT regime reform to stay updated on the evolving AML/CFT regulatory requirements. Financial institutions should also prepare to closely assess their AML/CFT compliance programs, policies, and processes and take steps as necessary to align with new requirements and standards.

## CONTACTS

**David DiBari**
Managing Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

**Megan Gordon**
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

**Michelle Williams**
Partner

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

**Celeste Koeleveld**
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

**Steven Gatti**
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

**Daniel Silver**
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

**Philip Angeloff**
Counsel

T +1 202 912 5111
E philip.angeloff
@cliffordchance.com

**Catherine Ennis**
Counsel

T +1 202 912 5009
E catherine.ennis
@cliffordchance.com

**Laura K. Hamilton**
Associate

T +1 202 912 5900
E laura.k.hamilton
@cliffordchance.com

**Holly Bauer**
Associate

T +1 202 912 5132
E holly.bauer
@cliffordchance.com

**Steve Nickelsburg**
Partner

T +1 202 912 5108
E steve.nickelsburg
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

© Clifford Chance 2020

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.