protiviti®
Face the Future with Confidence

Top of Mind Compliance Issues for 2021 – The AML Act of 2020

What to Expect and When

The main headline about the Anti-Money Laundering Act of 2020 (AML Act) has been that the United States finally moved to address a long-standing gap in its anti-money laundering (AML) regime by establishing a national registry of beneficial owners. Not reading beyond that headline, however, would be a mistake because the AML Act includes many other provisions that, taken collectively, could reshape the future of AML compliance in the United States.

The following sections summarise many of the key provisions of the AML Act that should be top of mind for management and compliance professionals. These are grouped by topic and do not necessarily track to the specific title of the law in which the provisions are included.

Applicability	Beneficial Ownership Registry
Risk-Based AML Compliance Programmes Shaped by Public Priorities	Whistleblower Programme
Strengthening and Modernising FinCEN and AML Regulations	Criminal Liability Related to Concealment of PEP or Special Measures Entity Involvement in Transactions
Improving Communications and Oversight	
Expanded Extraterritoriality	Additional Penalties for Non-Compliance

Applicability

The provisions of the AML Act are applicable to a "financial institution" as defined in the Bank Secrecy Act (BSA), with two amendments included in the AML Act:

- The definition of a person or business that "engages in the transmission of currency or funds" is modified to include the transmission of "value that substitutes for currency," making clear that it applies to the transmission of virtual currency.
- A person "engaged in the trade of antiques, including any adviser, consultant or any other person who deals in the sale of antiquities" is added to the definition.

Risk-Based AML Compliance Programmes Shaped by Public Priorities

The AML Act affirms that AML compliance programmes must be risk-based but adds that such risk-based programmes are to be guided in part by publicly announced AML priorities. The Secretary of the Treasury is required to announce the initial public priorities for AML compliance within 180 days (June 30, 2021) of the effective date of the AML Act and to update the priorities at least every four years thereafter, in consultation with the Attorney General, other federal and state regulators, and national security agencies.

Financial institutions will be expected to incorporate the public priorities into their AML risk assessments and regulators will review how effectively they do this. To account clearly for consideration of the public priorities, financial institutions will need to revise their AML risk assessment methodologies. Given the complexities and rapidly evolving threat environment for AML compliance, updating priorities every four years would seem to be a stretch. Time will tell whether the Treasury Department will announce public priorities on a more frequent basis or will look to financial institutions to determine how to modify or expand these priorities between updates.

Strengthening and Modernising FinCEN and AML Regulations

The AML Act includes many steps aimed at strengthening and modernising existing AML regimes. These include:

- Reinforcing the authority of the Financial Crimes Enforcement Network (FinCEN) to regulate virtual currency.
- Requiring FinCEN to issue regulations for implementing a three-year pilot programme (with a two-year extension at the Treasury Department's option) allowing financial institutions to share Suspicious Activity Reports (SARs) with foreign branches, subsidiaries and affiliates and not just with parent companies as currently permitted.
- Enhancing FinCEN's funding and authority related to, inter alia, hiring and retaining staff, coordinating with other federal regulators, conducting industry outreach domestically and internationally, and providing technical assistance.

- Explicitly allowing two or more financial institutions to share resources as described in prior interagency guidance.
- Requiring numerous assessments, reviews, reports and studies on a range of issues, including (in addition to those mentioned in other sections of this paper):
    - Consideration of a process for issuing FinCEN no-action letters.
    - Review of SAR and Currency Transaction Reporting (CTR) filing requirements.
    - Annual reporting by the Attorney General to the Treasury Department on the use of BSA data by law enforcement.
    - Semi-annual publication by FinCEN of threat patterns and trends.
    - Requiring FinCEN, within one year, to solicit public comment and review all BSA regulations.
    - A study by the Government Accountability Office (GAO) on human trafficking and how financial institutions can identify it.
    - A study by the GAO on the use of online marketplaces and online payment services, including virtual currencies and P2P payments and how such payments are used to facilitate human trafficking and drug trafficking and how virtual currencies and their underlying technologies can be used to combat trafficking.
    - A study by the Treasury Department on money laundering by the People's Republic of China, the related risks to the international financial system and a strategy for combating these risks.
    - A study by the DOJ and the Treasury Department on efforts by authoritarian regimes to exploit the U.S. financial systems.
    - Within one year and then annually for the ensuing four years, reporting by the Attorney General to Congress on deferred and non-prosecution agreements, along with the justification for each.
- Taking steps to advance innovation, including:
    - Establishing a subcommittee of the Bank Secrecy Act Advisory Group (BSAAG) to focus on innovation and technology.
    - Requiring FinCEN and the federal functional regulators each to appoint a BSA Innovation Officer who will coordinate outreach with the industry, law enforcement, state supervisors and others, including vendors.
    - Requiring the Treasury Department to issue a rule for testing new technologies.

- Requiring the Treasury Department to report to Congress within one year on the impact of technology on financial crimes compliance.
- Requiring the Treasury Department to convene a tech symposium periodically.

The results of the actions described above could have a significant impact on compliance efforts, thus financial institutions should monitor developments closely and take full advantage of opportunities to provide input and influence the future direction of AML compliance.

Improving Communications and Oversight

The AML Act contains a number of steps to improve communications and oversight; these include, but are not limited to:

- Requiring the Treasury Department to include state supervisors in discussions of BSA requirements.
- Establishing a subcommittee of BSAAG to advise on security and confidentiality implications of regulations and BSA examinations.
- Requiring FinCEN, each federal functional regulator and the IRS to appoint a BSA Security Officer for consultation related to security and information sharing.
- Requiring FinCEN to maintain staff with financial expertise to analyse AML and terrorist financing data.
- Requiring BSA examiners to undergo annual training.

These efforts to foster greater coordination; upskill and train FinCEN and bank regulatory staff, respectively; and improve public-private collaboration around security and confidentiality should be welcomed by the industry.

Expanded Extraterritoriality

The AML Act significantly extends the extraterritorial reach of the United States. Under the authority afforded by the USA PATRIOT Act, the U.S. could issue subpoenas to any foreign bank that maintains a correspondent account in the U.S. for records related to that correspondent account. Under the expanded authority included in the AML Act, the U.S. may issue subpoenas for any record related to a correspondent account or *any account of the foreign bank*, including records maintained outside of the United States if the records are the subject of an investigation involving, inter alia, a violation of a U.S. criminal law or a violation of the BSA. What this means, as an example, is that a foreign bank may be issued a subpoena for information related to the account(s) of one of its customers, even if no activity for that customer has been cleared through its USD correspondent account.

Foreign banks that receive a subpoena would be prohibited from notifying the account holder of the existence of the subpoena. Foreign banks can take steps to try to quash a subpoena, but

claiming a conflict with local privacy or confidentiality laws will not be considered a bona fide reason for not complying. Failure to comply may result in contempt sanctions and financial penalties and, in the extreme, the Treasury may direct U.S. financial institutions to terminate their correspondent relationships with a non-complying foreign bank.

Foreign banks with correspondent banking relationships in the U.S. will want to consider the additional exposure they may face because of this authority. While specific arguments for quashing a subpoena likely need to be fact-based, affected foreign banks would be wise to consult with counsel now to understand how best to manage possible subpoenas.

Beneficial Ownership Registry

In keeping with FATF Recommendations related to identifying and discouraging the use of shell companies, specifically Recommendation 24 "that countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities," the Corporate Transparency Act (which is included in the AML Act) requires FinCEN to maintain a national registry of beneficial owners. The registry will not be public and will only be available to (1) law enforcement under specified conditions, (2) a federal functional regulator, or (3) financial institutions with a customer's permission.

Reporting companies include entities formed under the laws of the U.S. or Indian Tribe and foreign entities registered to do business in the United States. These entities must report the following information on each beneficial owner (an entity or individual who directly or indirectly exercises substantial control over the entity or who owns or controls 25% or more of the entity's ownership interest, excluding minors, nominees, employees acting in their employment capacity, someone with a right of inheritance, and creditors):

- Full legal name
- Date of birth
- Current residential or business address
- Unique identifying number of an acceptable identification document

Exclusions to the definition of reporting company include publicly-traded companies, certain non-profits and government entities, certain financial institutions, and other entities that employ more than 20 full-time-equivalent employees, filed a federal income tax return with more than $5 million in sales or gross receipts, and maintain an operating presence in a physical office in the United States.

The Act establishes penalties of (1) not more than $500 per day for each day a violation continues, and (2) a criminal fine of not more than $10,000 and up to two years in prison for wilfully providing or attempting to provide fraudulent beneficial ownership information. It also

provides penalties for unauthorised disclosure or use of beneficial ownership information: (1) a civil penalty of not more than $500 per day for each day a violation continues, and (2) a criminal fine of $250,000 and up to five years in prison or, if the violation occurs while violating another U.S. law or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period, a fine of not more than $500,000 and up to 10 years in prison. The Treasury Department is required to conduct an annual audit to ensure access to beneficial ownership information is limited to those authorised and must report annually to the Senate Banking Committee and the House Financial Services Committee on the audit; the GAO must also audit the system. The Treasury Department is required to report periodically to Congress regarding any complaints on the beneficial ownership process and, through its Inspector General, for conducting investigations of any cybersecurity breaches of the registry.

Existing reporting companies formed or registered before the effective date of the regulations promulgated by FinCEN to implement this provision must report beneficial ownership within two years of the effective date of the regulations; newly formed reporting companies after the effective date of the promulgated regulations must report beneficial ownership at the time of formation. There will need to be regulations implementing the registry and the current Customer Due Diligence (CDD) rule will need to be modified to bring it in line with the registry requirements. It is expected that rulemaking will take at least 18 months and then the registry will need to be operationalised, so it is likely to take several years before the programme is up and running.

In the intervening period, financial institutions will want to monitor the FinCEN rulemakings and consider the impact on their own operations of being able to leverage the registry, including policy and procedure changes that will be necessary and staff training that will need to occur.

Whistleblower Programme

The AML Act's revised whistleblower programme, which is modelled after the whistleblower programme in the Sarbanes-Oxley Act, increases the potential award amount for information reported to the Department of Justice and/or the Treasury Department related to BSA violations and enhances protections for whistleblowers. Under the AML Act, whistleblowers are eligible for an award equal to 30% of the penalties where the information leads to enforcement actions with penalties exceeding $1 million; this compares to the previous award formula of either $150,000 or 25% of the related penalties, whichever was less. Whistleblowers may report anonymously through an attorney but must disclose their identity before any award is made.

Critics say there is a problem with the anti-retaliation section of the whistleblower programme, i.e., employees at banks that are covered under the Federal Deposit Insurance Act or Section 214 of the Federal Credit Union Act (relating to insured credit unions) are excluded from the anti-retaliation provisions of the revamped programme. Effectively, this means all employees at

insured banks and credit unions would be forced to seek protection under older anti-retaliation laws which some would argue have not worked well in practice.

Financial institutions should monitor rulemaking and, simultaneously, review and update, as warranted, their internal whistleblower programmes in an effort to detect and address potential violations to mitigate the risks of whistleblower reports to the Department of Justice and/or Department of Treasury.

Criminal Liability Related to Concealment of PEP or Special Measures Entity Involvement in Transactions

The AML Act criminalises the concealment, falsification, misrepresentation, or the attempt to conceal, falsify or misrepresent, from or to a financial institution the source of assets involved in a monetary transaction if:

- The person or entity that owns or controls the assets is a politically exposed person (PEP), or any immediate family member or close associate of a PEP, and the value of the assets is equal to or greater than $1 million; or
- The transaction involves an entity identified as a primary money laundering concern by FinCEN and the transaction violates the prohibitions or conditions on opening or maintaining correspondent accounts or payable through accounts.

The penalty for non-compliance is up to 10 years in prison and $1 million in fines, including the forfeiture of any property involved in or traceable to the transaction.

Additional Penalties for Non-Compliance

Finally, new AML legislation rarely comes without new penalties and the AML Act is no exception. New penalties include the following:

- Repeat BSA violators are subject to discretionary penalties up to the greater of (i) three times the profit (or loss avoided) from the violation, or (ii) two times the maximum penalty with respect to the violation.
- Persons convicted of a BSA violation must be fined the amount gained as a result of the violation and, if the person is an officer of a financial institution, the person must also return any bonus earned during the period in question.
- Individuals found to be "egregious violators" of the BSA, e.g., individuals with a federal criminal conviction or a wilful civil violation that led to the facilitation of money laundering or terrorist financing, may be barred from serving on the board of a U.S. financial institution for 10 years.

Summary

The AML Act envisions a world where there is enhanced collaboration among regulators, where there is improved transparency and information sharing among governmental bodies and the financial services industry, where innovation is encouraged, and where AML compliance is more efficient and effective. But that world is still a number of years in the future and will require numerous rulemakings to implement the AML Act as well as the commitment of the industry to provide input throughout the process.

About Our AML Compliance Solutions

Protiviti's AML Leadership Team includes former financial institution regulators, former financial institution compliance officers, fraud and forensic specialists, and AML technology system experts. We draw on our previous industry experience to help compliance officers, board members, and all three lines of defence to respond to situations of noncompliance, to improve processes and controls, and to provide ad hoc support.

At Protiviti, we understand the AML challenges faced by financial services organisations. Our solutions are designed to help your company exceed regulators' expectations. We enable clients to take a disciplined approach to managing AML/sanctions risk and provide sustainable solutions.