Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated June 9, 2021

U.S. Efforts to Combat Money Laundering, Terrorist Financing, and Other Illicit Financial Threats: An Overview

The United States maintains a multifaceted policy regime for tackling anti-money laundering (AML), combating the financing of terrorism (CFT), and countering other forms of illicit financial threats. Key issues for the 117th Congress may include oversight of the U.S. government's robust legal, regulatory, enforcement, and diplomatic AML/CFT effort—with special focus on the Biden Administration's implementation of significant changes to the AML/CFT regime that were enacted as part of the FY2021 National Defense Authorization Act (NDAA; P.L. 116-283).

Background

Misuse of the international financial system, including for the purposes of money laundering and terrorist financing, can result in significant economic, political, and security consequences at both national and international levels. *Money laundering*, which broadly refers to the process of disguising financial assets so they can be used without revealing their underlying illicit source or nature (e.g., proceeds of fraud, corruption, and contraband trafficking), is globally ubiquitous. *Terrorist financing*, a key global security concern, refers to the process of fundraising, through both licit and illicit means, and financially sustaining terrorist groups. Other illicit financial threats span a wide range of concerns, including proliferation finance, tax evasion, sanctions evasion, and the financial facilitation of malign threat actors.

Despite robust AML efforts in the United States, policymakers face challenges in their ability to counter money laundering effectively, including the diversity of illicit methods to move and store ill-gotten proceeds through the international financial system (e.g., trade-based money laundering and misuse of anonymous shell companies); the introduction of new and emerging threats (e.g., cyber-enabled financial crimes); the ongoing use of old methods (e.g., bulk cash smuggling); gaps in legal, regulatory, and enforcement regimes, including uneven availability of international training and technical assistance for AML purposes; the rise of new payment technologies, such as cryptocurrency; and costs associated with financial institution compliance with global AML laws.

Legal Framework

In the United States, the legislative foundation for domestic AML regulation originated in 1970 with the Bank Secrecy Act (BSA; P.L. 91-508) and its major component, the Currency and Foreign Transactions Reporting Act. Amendments to the BSA and related provisions in the 1980s and 1990s expanded AML policy tools available to combat crime—particularly drug trafficking—and prevent criminals from laundering their illicitly derived profits.

Key elements to the BSA's AML legal framework, which are codified in Titles 12 (Banks and Banking) and 31 (Money and Finance) of the *U.S. Code*, include requirements for customer identification, recordkeeping, reporting, and compliance programs intended to identify and prevent money laundering. Substantive criminal statutes in Titles 31 and 18 (Crimes and Criminal Procedures) of the *U.S. Code* prohibit money laundering and related activities and establish civil and criminal penalties and forfeiture provisions. Federal authorities have also applied administrative forfeiture, nonconviction-based forfeiture, and criminal forfeiture tools to combat money laundering.

In response to the September 11, 2001, terrorist attacks, Congress expanded the BSA's AML policy framework to incorporate additional provisions to combat the financing of terrorism through the USA PATRIOT Act (P.L. 107-56). This provided the executive branch with greater authority and additional tools to counter the convergence of illicit threats, including the financial dimensions of organized crime, corruption, and terrorism. Most recently, the Anti-Money Laundering Act of 2020 (Division F of the FY2021 NDAA) provided for a wide-ranging update to the BSA and establishes a system in which many small and medium-sized legal entities must disclose information about their beneficial owners to the U.S. Department of the Treasury.

Regulatory Framework

The BSA's AML framework is premised on banks and other covered financial entities filing a range of reports with Treasury's Financial Crimes Enforcement Network (FinCEN) when their clients engage in suspicious financial activity, large cash transactions, or certain other financial behavior. The accurate, timely, and complete reporting of such activity to FinCEN flags situations that may warrant further investigation by law enforcement. Other reports must be submitted to FinCEN by individuals transporting large amounts of cash internationally, persons with certain foreign financial accounts, and nonfinancial entities conducting large cash transactions. In December 2020, FinCEN proposed a new rule on cryptocurrency and digital asset transaction reporting and recordkeeping requirements similar to those for currency transactions.

Federal financial institution regulators—including the Federal Reserve, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency—conduct oversight and examine entities under their supervision for compliance with BSA/AML requirements. These regulators are responsible for the safety-and-soundness examinations of the institutions they supervise and generally conduct

BSA examinations concurrently with those routine inspections. When there is cause to do so, however, any of the regulators may carry out a special BSA examination. Enforcement actions for AML violations may result in civil and/or criminal penalties. Other federal agencies with AML regulatory responsibilities include the Securities and Exchange Commission and the Commodity Futures Trading Commission. The Internal Revenue Service also enforces compliance with BSA requirements, particularly for nonbank financial institutions not regulated by other federal agencies, such as money service businesses, casinos, and charities.

International Framework

Given the global nature of the international financial system and the transnational criminal activity that attempts to exploit it, the United States and other countries have engaged in a variety of international efforts designed to improve global AML responses and build international cooperation and information sharing on AML issues, including through formal bilateral requests for mutual legal assistance on financial crime investigative matters. Multiple international organizations contribute to international AML cooperation through global standard setting, cross-border information sharing, AML assessment and monitoring, and AML technical assistance.

Some entities, such as the Financial Action Task Force and the Basel Committee on Banking Supervision, provide standard-setting guidance relevant to AML matters. Others, such as the Egmont Group of Financial Intelligence Units and the International Criminal Police Organization, contribute to the implementation of such standards through information sharing. The United Nations Office of Drugs and Crime, the World Bank, and the International Monetary Fund also maintain capabilities to monitor and assess national AML policies and provide technical assistance on AML capacity-building priorities. Other international and regional organizations—including the Organisation for Economic Co-operation and Development, the G-20, and the Organization of American States—have working groups and initiatives focused on various AML matters.

Recent Developments

This section highlights key changes to the BSA/AML regime enacted by the AML Act of 2020.

- **BSA mission and information sharing.** The act broadens the mission of the BSA to safeguard national-security-related dimensions of financial crime, including terrorist financing. It also enhances feedback opportunities among financial institutions, regulators, and law enforcement related to BSA/AML priorities and expands options for data sharing among financial institutions. To that end, the act directs the Treasury Department to establish a pilot program allowing financial institutions to share certain information with their foreign branches, subsidiaries, and affiliates.
- **Technology innovation.** The act encourages financial institutions to explore technology solutions, such as artificial intelligence, for BSA/AML compliance.
- **Cryptocurrency.** The act amends the BSA's definition of *monetary instrument* to include "value that substitutes for monetary instrument." Similarly, it amends the BSA's definitions of *financial institution* and *money transmitter* to include businesses exchanging or transmitting "currency, funds, or value that substitutes for currency or funds." These changes are seen as codifying FinCEN's BSA authorities over various cryptocurrencies and digital assets.
- **Reporting requirements.** The act requires the Secretary of the Treasury to review existing BSA requirements and consider options related to streamlining and automating certain reports, as well as modernizing other relevant regulations and guidance. It requires a review and strategy to address financial services de-risking concerns. The act also adds antiquities dealers to the list of financial institutions subject to BSA coverage.
- **Whistleblower protections and BSA penalties.** The act establishes additional protections for whistleblowers, additional penalties for BSA violators, and a new prohibition on the concealment of the sources of assets in monetary transactions. It bars those found to have committed serious BSA violations from serving on boards of U.S. financial institutions for 10 years.
- **Treasury support and staffing.** The act authorizes an additional $10 million for FinCEN operations and $60 million annually through FY2024 for Treasury's Office of Technical Assistance. The act further provides special hiring authority to Treasury's Office of Terrorism and Financial Intelligence; expands Treasury's attaché program; and establishes an interagency AML/CFT personnel rotation program, foreign financial intelligence unit liaisons, BSA information security officers, and a FinCEN "analytical hub."

Beneficial Ownership Transparency

Beneficial ownership refers to the natural person who invests in, controls, or otherwise benefits from an asset, such as a bank account, real estate, company, or trust. In the United States, corporations and limited liability companies are formed at the state level, and most states do not collect, verify, or update identifying information on their beneficial owners. This gap in the U.S. AML regime was a source of long-standing international criticism. The act requires those forming certain new legal entities, and certain existing entities, to provide FinCEN with identifying information about their beneficial owners. *Covered beneficial owners* is defined, in part, to mean persons who directly or indirectly own 25% or more of a legal entity or exercise "substantial control" over it. Covered entities must update information as it changes. FinCEN must store the information in a non-public database for at least five years and allow various U.S. government entities and financial institutions to access the information, subject to certain terms. Under the act, penalties for unauthorized disclosure of this information to the public are severe, though some countries store such information in public registries.

Rena S. Miller, Specialist in Financial Economics
Liana W. Rosen, Specialist in International Crime and Narcotics

IF11064

Disclaimer