Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Potential Paths To Modernizing The Bank Secrecy Act

By **Matthew Biben** (September 3, 2025, 5:58 PM EDT)


Matthew Biben

The Bank Secrecy Act, enacted in 1970, remains the cornerstone of the U.S. anti-money laundering and counterterrorist financing framework.

When it was adopted, the BSA marked a significant advancement in financial regulation. Yet, the statute was enacted at a time when most transactions occurred through physical banks, checks or cash, and international capital flows were relatively limited compared to today's globally interconnected financial system.

Prior reforms, while important, retained the BSA's essential framework: a system built on volume-based reporting, in which financial institutions must capture and transmit enormous amounts of data to regulators. The model presumes that greater data collection translates into greater visibility, but in practice this approach often generates diminishing returns.

Today, more than 50 years after the BSA's enactment, the financial landscape has been transformed by digitization, globalization and new business models.

In this environment, the BSA — designed for an analog economy — has become increasingly misaligned with both financial realities and the needs of modern businesses. Speaking at the U.S. Department of the Treasury's Financial Crimes Enforcement Network's BSA Advisory Group plenary meeting in June, Deputy Treasury Secretary Michael Faulkender outlined a modern BSA regime that includes "responsible financial innovation, including related to the use of digital assets."[1]

The BSA's modernization is essential to maintain effective oversight while promoting innovation, reducing costs and ensuring that U.S. financial institutions remain competitive globally.

Compliance Costs and Industry Impact

A 2024 industry study by LexisNexis Risk Solutions reported that the total cost of financial crime compliance in the U.S. and Canada has reached $61 billion.[2] As the number of BSA reports submitted continues to grow, FinCEN receives so much data that it is often unable to extract timely intelligence. Law enforcement officials acknowledge that much of the information they receive is duplicative or of limited investigative value.

The result is a compliance regime that imposes substantial costs on the private sector without delivering

commensurate benefits for public safety or financial integrity.

Emerging Technological Solutions

One promising avenue for reconciling the twin goals of effective law enforcement and efficiency lies in businesses' adoption of advanced technological tools. Today's technology allows for smarter, faster and more targeted oversight, if regulators are willing to modernize the framework to accommodate it.

Blockchain Analytics

The cryptocurrency sector exposes significant tensions between the BSA and modern finance. Blockchain technology eliminates intermediaries, decentralizing financial transactions and enabling users to transfer assets without banks or brokers.

Regulators have attempted to apply the BSA to crypto exchanges and custodial services, but the fit is imperfect.

Yet, blockchain ledgers record all cryptocurrency transactions in real time, making them uniquely traceable with the right tools. Private companies already provide blockchain analytics services that track illicit transactions linked to ransomware, terrorist financing or sanctioned entities.

Business Use Case

A fintech offering cross-border payment services could integrate blockchain analytics to automatically flag transfers linked to high-risk jurisdictions. This would allow the fintech company to demonstrate robust compliance during regulatory audits while reducing the need for blanket reporting of all transactions.

Zero-Knowledge Proofs

Zero-knowledge proofs are a form of advanced cryptography that allows one party to prove a fact to another without revealing the underlying data that establishes the fact. In simple terms, zero-knowledge proofs let a person demonstrate compliance without disclosing unnecessary personal details.

A cryptocurrency user could prove that their funds do not originate from a sanctioned wallet without exposing their entire transaction history. This allows compliance with AML rules while preserving privacy.

Business Use Case

A crypto exchange could integrate zero-knowledge proof compliance tools to show regulators that it screens for illicit activity while reassuring privacy-conscious customers that their personal data will not be over-collected.

Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning systems can analyze vast datasets, detect unusual patterns and learn from past cases, thereby reducing false alarms and focusing attention where it matters most.

Financial services firms and financial regulators outside the U.S. are actively deploying AI and machine learning systems for AML and compliance functions, dramatically improving their transaction monitoring

and market surveillance.

Business Use Case

A community bank might adopt an AI-powered monitoring system that reduces false positives by as much as 40%. Instead of maintaining a large manual review staff, the bank could redeploy resources toward customer service and local lending, improving efficiency while meeting compliance obligations.

Digital Identity Systems

A national digital identity framework would allow individuals to use secure, government-recognized credentials across financial services. Customers would no longer need to submit identity documents repeatedly for each account opening, and institutions would gain confidence in standardized, reliable verification.

Business Use Case

A large retail bank could streamline customer onboarding by adopting a government-backed digital ID system. This would cut know-your-customer costs, accelerate account opening and reduce fraud.

Pathways for Reform

To address the unique challenges of modern technology as well as the privacy concerns associated with the BSA, Congress and the relevant regulators have proposed various initiatives.

For instance, the Bank Privacy Reform Act — H.R. 533, introduced in 119th Congress — proposes a shift from volume-based to risk-based reporting, requiring warrants for government access to certain financial records, and focusing resources on national security priorities.

While the BPRA addresses privacy concerns and alleviates significant burdens on financial institutions, it fails to address the dynamics of modern markets.

Other reforms should include the following.

1. Indexing Reporting Thresholds to Inflation

The $10,000 currency transaction report threshold has remained unchanged since 1970. Adjusted for inflation, it would exceed $80,000 today.

Updating thresholds, whether retroactively or prospectively, would immediately reduce low-value reports, reduce the burden on financial institutions, improve consumer privacy and focus compliance on higher-risk activities.

2. Tiered Reporting Structures

A digital short-form suspicious activity report system, followed by detailed reports upon law enforcement request, would improve efficiency while ensuring that meaningful intelligence is captured.

3. Formal Feedback Mechanisms

FinCEN should provide systematic feedback on suspicious activity report utility, helping institutions refine compliance programs and allocate resources more effectively.

4. Innovation Sandboxes and Safe Harbors

Congress and regulators should establish statutory safe harbors for good faith adoption of innovative compliance tools, easing the transition for financial institutions experimenting with new models.

The U.K. has already deployed sandbox programs and tailored AML requirements for fintech companies, making London a leading hub for financial innovation.

5. Integration of Privacy-Preserving Technologies

Explicit statutory authorization for cryptographic compliance methods such as zero-knowledge proofs would bring U.S. regulation in line with international privacy standards.

Conclusion

While the BSA was a landmark achievement of its time, its analog design has become increasingly incompatible with today's digital financial ecosystem.

Legislative reforms such as the BPRA, coupled with regulatory adjustments including updated thresholds, feedback mechanisms and innovation sandboxes, would reduce unnecessary costs while enhancing the quality of financial intelligence.

Modernization is not merely a compliance concern but a competitiveness imperative. A more intelligent and adaptable BSA framework would empower the financial services industry to innovate responsibly, strengthen U.S. leadership in global finance and ensure that resources are strategically directed toward combating serious financial crime.

Matthew Biben is a partner at King & Spalding LLP. He previously served as an assistant U.S. attorney in the Criminal Division at the U.S. Attorney's Office for the Southern District of New York.

[1] Press Release, U.S. Dep't of the Treasury, Deputy Secretary Faulkender Lays Out Guiding Principles for Bank Secrecy Act Modernization(June 18, 2025), https://home.treasury.gov/news/press-releases/sb0173.

[2] Study Reveals Annual Cost of Financial Crime Compliance Totals $61 Billion in the United States and Canada, LexisNexis Risk Sols. (Feb. 21, 2024), https://risk.lexisnexis.com/about-us/press-room/press-release/20240221-true-cost-of-compliance-us-ca.