February 2025

The Bank Secrecy Act is Broken

Examining the burdens, costs, and failures of the Bank Secrecy Act (BSA), and the potentially disastrous implications of applying the BSA to decentralized finance (DeFi).

Gavin Zavatone
Henry Michaelson

DeFi Education Fund

defieducationfund.org

Introduction

On February 5, 2025, the Senate Banking Committee held a hearing focused on investigating the impacts of debanking in America. The hearing highlighted a strong bipartisan interest in protecting Americans' access to inclusive and affordable financial services. The hearing also dove into anti-money laundering (AML) policy and its relationship to debanking; there was substantial discussion on the efficacy and costs of the AML framework. As Aaron Klein, Senior Fellow at Brookings Institution, submitted in his written testimony: "Unfortunately, our AML system in practice operates with a great deal of inefficiency, which makes banking more expensive for everyone, and drives the debanking of some consumers and small businesses." Throughout the hearing, witnesses and Members of the Committee highlighted salient concerns about the AML framework's efficacy and implementation, effectively raising related questions about harmful approaches that have been advanced to rope decentralized finance (DeFi) into the existing AML framework.

Perhaps surprising: up to $2 trillion in illegal transactions annually—about 2-5 percent of the world's gross domestic product (GDP)—passes through the global financial system. (Comparatively, estimates indicate that 0.4 percent of all crypto transaction volume went through illicit addresses in 2024.) This trend persists despite the cornucopia of laws in many jurisdictions that are meant to prevent illicit finance. Unfortunately, AML efforts are not effectively achieving these critical policy objectives, but rather costing financial institutions billions of dollars to collect sensitive personal information on millions of individuals and their transactions. This is especially true in the United States under the Bank Secrecy Act (BSA) AML regime.

The Department of Justice (DOJ) has brought concerning federal prosecutions against software developers who are not subject to the BSA AML framework, which is designed for financial institutions. With the emergence of decentralized finance (DeFi), many industry participants are unsure of their obligations under the BSA when, on one hand, the Financial Crimes Enforcement Network (FinCEN) has concluded that partial control over a user's crypto is insufficient to classify certain persons, like wallet developers, as money transmitters. And, on the other hand, the DOJ has pursued two troubling federal prosecutions of noncustodial software providers for the alleged unlicensed ownership or operation of an unregistered money transmitting business.

Subjecting software providers and operators that neither accept nor transmit funds on behalf of their users would place a de facto ban on noncustodial software, as they cannot functionally comply with BSA obligations for money transmitters. Furthermore, should DeFi be subject to the BSA, American users of DeFi technologies would be forced to surrender their right to privacy. As this paper will explain, roping in DeFi would be a hefty cost for an AML regime that is currently falling short of effectively achieving its stated goals (detecting and preventing illicit finance).

In January 2025, TRM Labs released highlights from their 2024 Crypto Crime Report, which concluded that despite the massive rally in crypto markets last year (with crypto transaction volume soaring to over $10.6 trillion, up 56 percent from 2023), illicit volume dropped to $45 billion, down 24 percent from 2023. This represents 0.4 percent of overall crypto transactions and marks a 51 percent decrease from 2023—where TRM currently determines that illicit volume accounted for 0.86 percent of total crypto transactions.

The Bank Secrecy Act (BSA), originally designed to combat illicit finance, has become a largely ineffective and burdensome regulatory framework for financial institutions. Despite imposing immense compliance costs—amounting to nearly $59 billion annually in the U.S. alone—the BSA demonstrates minimal success in proactively detecting and prosecuting financial crimes. Although millions of transactions are reported, law enforcement rarely utilizes these reports to initiate investigations or proactively prevent and detect illicit finance. This system disproportionately harms smaller financial institutions, stifles financial innovation, and raises serious concerns about arbitrary enforcement, privacy violations, and restrictions on decentralization.

Nevertheless, concerning legislative proposals and federal prosecutions seek to subject decentralized finance (DeFi) to the BSA's AML regime, even as efforts to combat illicit finance in traditional finance (TradFi) show little promise. These efforts could impose billions in compliance costs, create barriers to entry for startups, contribute to debanking, and risk the weaponization of sensitive financial data against Americans.

As some have attempted to extend the BSA framework to DeFi, it is crucial to assess its current inefficacies and recognize that applying its burdensome requirements to DeFi would not only be impractical but would also cripple an emerging industry without meaningfully curbing illicit finance. Overall, these problems show how the BSA is ill-suited for DeFi and noncustodial blockchain participants. Instead, the federal government should prioritize developing a more effective and well-suited AML framework for the existing financial system. As legislation is progressed on DeFi, AML policy should focus on trusted intermediaries and respect disintermediation.

I. Overview of the BSA

The BSA forms the backbone of American AML policy by mandating risk-based programs and information-sharing mechanisms for financial institutions. These include traditional banks, credit unions, investment companies, currency exchanges, and money services businesses (MSBs). Crypto denominated transactions are covered by the framework as "value that substitutes for currency," prompting custodial crypto exchanges, like Coinbase or Kraken, to register as financial institutions and report BSA data on customers and their transactions.

These financial institutions must implement comprehensive AML programs that include four key components: (1) internal policies and controls, (2) designated compliance officers, (3) ongoing employee training, and (4) independent audit functions. Additionally, under 31 U.S.C. §

5318(g)(1) and § 5313(a), institutions must file Suspicious Activity Reports (SARs) for potentially illegal transactions and Currency Transaction Reports (CTRs) for cash transactions exceeding $10,000 in one business day. These requirements are primarily achieved through "know-your-customer" (KYC) requirements to open or operate an account.

FinCEN is a bureau within the Department of U.S. Treasury that is tasked with implementing and enforcing the BSA; FinCEN also oversees the collection of BSA data, which contains sensitive personal identifying information from both SARs and CTRs, and maintains storage systems for this information. Through Memorandum of Understanding (MOUs), FinCEN facilitates access to this data for law enforcement agencies, creating an information-sharing network among financial institutions, regulators, the Treasury, and law enforcement.

The BSA Regime is Struggling to Achieve its Critical Objectives

Unfortunately, in spite of the BSA, illicit finance, money laundering, and criminal financial activity remain rampant in the United States and around the globe. There are numerous quantitative data points that support this statement:

- In a recent blog post, DEF highlighted significant examples of BSA noncompliance in the traditional financial system, with over $18 trillion of transaction volume going unmonitored at a major U.S. bank.
- In a 2018 Department of Treasury Money Laundering Risk Assessment, Treasury officials estimated that about $300 billion is generated annually in illicit proceeds.
- Academic studies indicate that existing AML policy currently demonstrates significant weaknesses.
- A former government prosecutor stated that as much as 99.9 percent of money laundering in the traditional financial sector goes unprosecuted.

As Brookings Institution Fellow, Aaron Klein, recently submitted in his written testimony to the Senate Banking Committee –

> "Unfortunately, our AML system in practice operates with a great deal of inefficiency, which makes banking more expensive for everyone, and drives the debanking of some consumers and small businesses."

The problem with BSA implementation is nuanced but significant: (1) it is overly burdensome and costly, (2) it has demonstrated minimal success in achieving its key objectives through transaction reporting, review, and investigation, and (3) it creates negative downstream effects, including arbitrary enforcement, prohibitive compliance costs, and centralization.

The inefficiency and burden of the AML systems draws into question important concerns about the burdens and inefficiencies if DeFi were subjected to the BSA's framework – at the most extreme example, the BSA has the potential to decimate the DeFi industry.

I. Immense BSA Compliance Costs

In the Senate debanking hearing, witnesses noted the immense burden AML compliance places on financial institutions and its downstream impacts on consumers. Mr. Klein argued that the "economics of [our AML system] are not in line with the objectives of it." He claimed that, under the BSA, financial institutions report too much irrelevant information, and banks are let off the hook by simply paying fines. He concluded in his written testimony by asserting that these costs are passed back onto consumers and businesses toward those who are the subject of SAR filings.

In his written testimony, Mr. Kline wrote: "Our AML framework generates significant expenses for a subset of consumers and businesses. Banks respond economically and will tolerate and pass along AML costs for customers who are profitable enough. Those who are not profitable have a hard time getting a bank account. A New York Times study identified who many of these people are: small businesses that deal with a lot of cash—such as bars, restaurants, and cannabis firms—and people who send money to their families overseas."

AML policy is immensely expensive for financial institutions to comply with. Estimates indicate that American financial institutions are spending upwards of $50 billion to comply with the BSA, while global estimates indicate that the total cost of financial crime compliance across all financial institutions reached $213.9 billion in 2021, surpassing the $180.9 billion figure recorded in 2020, with the majority of this year-over-year increase being represented by Western Europe and the United States. In 2018, the Federal Reserve Bank of St. Louis conducted a survey and found that the Bank Secrecy Act is the costliest of all financial regulations for banks to comply with (accounting for 22.3 percent of their total compliance costs).

Recent numbers suggest that financial institutions around the country are spending upwards of $59 billion a year complying with the BSA regime. In a 2020 Study, the U.S. Government Accountability Office (GAO) concluded that compliance costs generally tended to be proportionally greater for smaller banks than for larger banks, comprising about 2 percent of the operating expenses for each of the three smallest banks in 2018 but less than 1 percent for each of the three largest banks in GAO's review. GAO found that requirements to verify a customer's identity and report suspicious and other activity generally were the most costly area, accounting for between 29 and 28 percent of total compliance costs on average at 11 selected banks. Therefore, compliance costs disproportionately harm smaller financial institutions. And, more importantly, compliance costs can hurt the consumer downstream by increasing the costs of financial services.

Compliance costs are much more onerous and challenging for small or new participants in the financial services markets. Therefore, start-ups, disruptors, and competitive financial services markets are at a disadvantage. In a 2015 Congressional Research Service (CRS) study on the regulatory burden on small banks, the CRS concluded that smaller banks face challenges in compliance because investments in software, manpower, and expertise disproportionately impact their operations relative to larger banks. These burdensome costs make it more difficult than necessary for financial institutions to invest in robust and effective AML systems. Further, the report concludes that the costs of regulatory compliance, including hiring compliance officers and purchasing systems, are significant operational burdens that are especially pronounced for small institutions.

II. BSA Data Usage is Minimally Useful in Generating Outcomes

In the recent Senate Banking Committee hearing, Mr. Kline stated in his written testimony:

> "Using the information and data from the banking system can allow law enforcement to catch and convict criminals. An analogy: if criminals are like scuba divers swimming in darkness at the bottom of the ocean, they can be hard to find. Money, like air bubbles, floats to the surface. If you can trace the bubbles to the bottom, you can catch the crook."

He continued the analogy in his oral testimony by asserting that "all we are doing in the current process is blowing air into the system."

The BSA AML system is opaque, and many struggle to understand the efficacy of the framework. In a February 2024 report, GAO found a lack of government-wide statistics regarding BSA data usage and investigation outcomes. Therefore, GAO recommended that FinCEN and DOJ "improve the reliability of its law enforcement surveys" and "coordinate with other agencies to develop a methodology to produce government-wide data on investigation outcomes." GAO's recommendations represent a continuation of the concerning trend of flawed data collection, review, and transparency on the collection of individual's private personally identifying information.

Additionally, an estimated 47 percent of agencies searched CTRs as a standard practice for each investigation or prosecution. Notably, the GAO report found that for IRS criminal investigations, on average, about 35 cases originated from CTRs each fiscal year from 2020 to 2022. However, the GAO study noted that other than the IRS, few law enforcement agencies track whether using CTRs leads to tangible outcomes, such as case originations, indictments, convictions, or recoveries. In a 2022 report, GAO found that law enforcement agencies had difficulty linking BSA reports to outcomes, and some reported difficulty determining what it means to "use" a BSA report, another critical technicality which was highlighted by Senator Andy Kim (D-NJ) during the Senate Banking Committee hearing on debanking.

FinCEN's 2023 "Year in Review" report states that banks and other financial institutions filed over 27.57 million reports under the BSA, most of which came in the form of CTRs. While FinCEN does not provide precise government-wide statistics on BSA-related criminal investigations, they do highlight specific statistics from certain agencies. According to FinCEN, 13.9 percent of Internal Revenue Service investigations in fiscal year 2023 originated from these reports. During that same time period, the IRS had 2,676 criminal investigations, meaning that approximately 372 investigations *originated* from a BSA report, despite billions of dollars being spent in compliance and the filing of millions of sensitive BSA reports. Thus, these IRS investigations originating from BSA data constitute approximately 0.00135 percent of the total BSA reports collected by FinCEN. Although the IRS only represents one agency with access to BSA data, the miniscule usage of BSA data to initiate IRS investigations represents a microcosm of a broader trend.

While BSA data can be *useful* in certain criminal investigations, red flags arise in *how* BSA data can be useful to investigators. FinCEN's report noted 85.7 percent of the IRS's criminal investigations recommended for prosecution "have a primary subject with a *related* [Bank Secrecy Act] filing." In other words, these investigations are not *originated* by a BSA filing. According to the FinCEN Year in Review Report, law enforcement agencies like the Federal Bureau of Investigation (FBI) *made use* of BSA data in only 15 percent of investigations. This highlights a concerning technicality: there is a vital difference between BSA data used to *initiate* investigations, as opposed to *supplement* investigations. In essence, the implications of these statistics lead to the inference that a majority of IRS criminal investigations don't come from BSA reports at all. Rather, BSA data is used to supplement existing investigations—the very definition of capricious oversight.

According to a December 2024 GAO Study, CTR BSA requirements have "expanded and do not fully align with the statutory objective of providing highly useful information." GAO concludes that while the CTR threshold ($10,000 per day) has remained unchanged for over 50 years, FinCEN's regulations have significantly expanded the scope of CTR requirements by increasing the types of institutions required to file and the amount of information collected. The GAO report found that an estimated 91 percent of surveyed agencies at least "occasionally" used CTRs to "develop leads for existing investigations."

The December 2024 GAO Study also revealed shocking statistics on how often CTRs are accessed, concluding that while law enforcement agencies find most CTRs "useful," they do not access most CTRs in the first place. "Of the more than 167 million CTRs filed from fiscal year 2014 through fiscal year 2023, about 5.4 percent (9 million) were accessed through the portal." Meaning, CTRs are often accessed after something else has prompted investigators to access a CTR. Moreover, fewer than 7 percent of CTRs were accessed within five years of filing, and 7.6 percent of fiscal year 2014 CTRs had been accessed by the end of fiscal year 2023. It becomes difficult to fathom the necessity of such stringent reporting when such a small percentage of law enforcement agencies ever utilize CTRs, leaving the vast majority of the reports untouched and unnecessarily retained.

As Nick Anthony of Cato Institute wrote in a recent article: “Given it’s the case that the majority of ‘useful’ reports are only used after an investigation has begun, there is little reason to justify mandating that these reports be filed instead of requiring law enforcement to obtain them via the warrant process.” The limited number of investigations originating from BSA data draws into question the efficacy of the BSA framework, and raises concerning questions about arbitrary financial data collection.

III. Downstream Impacts: Arbitrary Enforcement, Innovation Prohibitions, and Centralization

The fact that millions of Americans' intimately personal financial data is being filed away at FinCEN, which is not frequently used to *initiate* law enforcement actions but rather *supplement* them, is concerning and eschews requirements that any search or seizure be supported by a warrant based on probable cause. In effect, this framework creates downstream concerns about arbitrary enforcement, privacy violations, and prohibitive compliance costs.

FinCEN collects an abundance of sensitive financial data annually, which the House Select Subcommittee on Weaponization of Government has found has been arbitrarily enforced and weaponized by other government agencies. According to a December 2024 report, the FBI eschewed existing laws and regulations that disallow law enforcement agencies from seeking customer information from financial institutions without legal process. The report includes allegations that the FBI asked financial institutions to use “sweeping search terms,” ranging from political terminology to the purchase of religious texts, across financial transactions to identify political “extremism.”

The report also concludes that the FBI overlooked the BSA’s explicit requirements, which specifically assert that financial institutions, not law enforcement, should have discretion over filing SARs. The report only confirmed that *one* financial institution requested the proper legal process from the FBI, which the FBI responded to by claiming that, because financial institutions usually provide more information in similar situations without a subpoena, this financial institution should do the same. With limited pushback, there is concern from the Select Committee on capricious financial surveillance using BSA data.

The report also found that the “government’s access to Americans’ private financial data is widespread and virtually unchecked,” with approximately 25,000 government employees in various federal, state, and local positions having "warrantless access” to FinCEN’s database. Employees and their agencies can, without a warrant, copy FinCEN datasets in their entirety and keep them privately in their own data systems. With government encouragement to “more aggressively track Americans,” and a general lack of oversight of government employees that have access to data, the BSA and its corresponding data are at risk for weaponization.

This raises concerns particularly in a civil rights context (e.g., individual privacy, profiling, de-risking, and a lack of oversight or accountability). As Senator Elizabeth Warren (D-MA),

Ranking Member on the Senate Banking Committee, recently stated in the context of debanking, “It doesn’t matter who you voted for, what you believe, or the origin of your last name—people shouldn’t be arbitrarily denied access to their banks, locked out of their accounts, or stripped of their banking privileges.” Therefore, we should all be concerned about selective application of financial services denial or weaponization, especially when it comes to civil rights concerns and the collection of sensitive financial data.

In terms of compliance costs, legacy financial services providers are better equipped to bear the immense burden of BSA compliance, whereas smaller financial services companies seeking to disrupt or disintermediate the market face considerably higher barriers to entry and operation. This serves as an opposing force to decentralization and inclusive access to financial services.

Why is the BSA Ineffective?

This article has now explained that illicit finance is rampant in the traditional financial system despite the multitude of BSA filings and billions of dollars in compliance costs, and that BSA data is rarely used to initiate agency efforts to combat illicit finance. So, why isn’t the regime working?

First, the overwhelming data volume reported by financial institutions causes the BSA database to be inundated with SARs and CTRs, making it difficult to analyze and prioritize cases effectively. According to one survey, many financial institutions spend between 25 percent and 50 percent of all BSA compliance costs on CTR filings alone. In a December 2024 GAO Study, GAO concluded that the BSA framework places greater emphasis on compliance with reporting requirements and structure of the overall AML program in a financial institution versus prioritizing more comprehensive intelligence.

Additionally, criminals and bad actors have developed sophisticated techniques in the traditional financial system to avoid detection. By exploiting global jurisdictional gaps, structuring, trade-based money laundering, and offshore accounts, bad actors are able to sidestep SAR and CTR filings using financial intermediaries.

Finally, the AML framework is archaic and arbitrary. The framework mandates customer identification and reporting, but erroneously captures millions of reported transactions which meet the threshold for reporting, but are not illicit transactions at all. Not only are requirements for reporting capacious, but according to GAO, the $10,000 reporting threshold has not been increased since it was set in 1972, which means that the number of CTR filings has increased by about 62 percent since FY 2002 due to inflation of the U.S. dollar.

In the February 5th Senate hearing on debanking, Senator Andy Kim (D-NJ) spoke in alignment with Mr. Klein’s perspective on “excessive” filings, reiterating that millions of reports are being used but not getting proper feedback on how useful the reports are. Mr. Klein responded stating that “banks are not judged on the quality of their performance, they’re judged

on the quantity," and noted that the banks have every incentive to "file more without getting information as to the quality of it. This is how filings have increased 10 fold in 20 years." Senator Kim cited Mr. Klein's research, noting AML's ability to prosecute only "a few hundred out of millions of reports that come before them."

Without modernization and a shift toward targeted, adaptive intelligence, criminals will continue to exploit BSA's jurisdictional gaps and outdated thresholds, leaving U.S. financial institutions and law enforcement ill-equipped to combat emerging threats.

Conclusion

Law enforcement's efforts to prevent illicit finance are central to ensuring American public safety, the rule of law, and national security. It is imperative that illicit finance is detected and prevented in a cost-effective and efficient manner that aligns with constitutional rights and respects decentralization.

Unfortunately, the BSA framework, as it stands, struggles to achieve its objectives of preventing illicit finance in American financial institutions. The ineffectiveness of the BSA warrants further attention and a thoughtful discussion on future improvements.

The problem with the BSA is nuanced but significant: (1) it is overly burdensome and costly, (2) it has demonstrated minimal success in achieving its key objectives through transaction reporting, review, and investigation, and (3) it creates harmful downstream effects, including arbitrary enforcement, prohibitive compliance costs, and centralization. The inefficiencies and burdens of the AML system highlight the challenges that would arise if DeFi were subjected to the framework. Simply, DeFi technologies should not be subject to the BSA.

Roping DeFi into the BSA framework through legislative proposals and federal prosecutions ignores the limits of the law and disregards the technological realities of DeFi. DeFi software providers and operators neither accept nor transmit funds on behalf of their users; thus, subjecting them to the BSA framework would effectively impose a de facto ban on noncustodial software, as compliance with BSA obligations for money transmitters (e.g., CTR and SAR filings) is functionally impossible.

Moreover, BSA filings are immensely burdensome and costly for financial institutions, while providing minimal value to regulators. Given that the current BSA framework is ineffective at detecting and prosecuting illicit finance, subjecting DeFi to the BSA AML framework would be both impractical and harmful. Doing so would decimate the industry without achieving AML policy goals. If DeFi protocols, which are often start-ups, were subjected to the BSA framework, they would face onerous and prohibitive compliance costs and other downside risks. Illicit finance policy should work to strengthen and protect American financial markets—not hinder innovation or shield legacy financial institutions from competition by imposing prohibitive compliance costs. Rather than imposing an ill-suited regulatory framework to DeFi, regulators should craft a framework that acknowledges the nature of the technology and decentralized

software. As DEF's Miller Whitehouse-Levine and Amanda Tuminelli recently published in an A16z crypto editorial:

> "the automobile likely would not have succeeded if carmakers were held liable for every collision outside of their control. Such policy could have killed automobile innovation and frozen car manufacturing in the United States. If policy and lawmakers can align on the realities of control and custody in the context of software development, we'll establish a clear and fair foundation for crypto entrepreneurs and developers to build in the United States."

Attempting to subject noncustodial software protocols that do not exercise "total independent control" over user assets to ineffective and burdensome AML statutes would cripple the industry, undermine the technology, and fail to achieve AML policy goals effectively.

While the BSA is ill-suited for DeFi, the industry is actively exploring and implementing ways to effectively detect and prevent illicit finance and bad actors, while maintaining the technology's decentralization and protecting users' privacy. For example, major DeFi Apps have successfully integrated wallet risk screening and cybersecurity checks into their front-end websites, successfully barring bad actors from interacting with the underlying protocol through the front-end. Further, DeFi Apps are employing advanced software to conduct wallet sanctions screening, transaction monitoring, and blockchain analysis. But, as a general principle, AML policy should focus on trusted intermediaries and be conscientious of disintermediation.

As Congress and regulators continue to debate key issues regarding AML policy and DeFi, they should consider how to address the existing barriers and ineffectiveness of the current framework. Instead of decimating DeFi by requiring compliance with costly and ineffective BSA data collection procedures, regulators have the opportunity to modernize the AML framework to more effectively detect and deter illicit finance in the financial system, more broadly.

About the DeFi Education Fund

The DeFi Education Fund is a nonpartisan research and advocacy group working to explain the benefits of DeFi, achieve regulatory clarity for the future of the global digital economy, and help realize the transformative potential of DeFi for everyone.

We exist because DeFi has immense potential for human prosperity, but that can only be realized with buy-in from governments and appropriate policy. We work to help realize DeFi's promise by educating regulators and policymakers and advocating for smart approaches.

For more information on our work or to find time to chat with a team member, please visit our website at www.defieducationfund.org