CATO
POLICY
ANALYSIS

July 26, 2022 Number 932

Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals

By Norbert J. Michel and Jennifer J. Schulp

EXECUTIVE SUMMARY

The Bank Secrecy Act of 1970 (BSA) requires financial institutions to assist federal agencies in detecting and preventing money laundering and other crimes. It now forms the basis of a costly and extensive regulatory framework that forces private financial companies to act as law enforcement agents. The evidence shows that this regulatory framework has not appreciably reduced criminal activity. It has, however, placed major burdens on law-abiding Americans, including weakening their constitutional rights.

Given that Congress enacted the BSA without careful study, it is hardly surprising that the resulting regulatory framework has proved so ineffective at stopping criminal activity. The BSA's broad sweep today, however, seems surprising because even in 1974, when evaluating a far narrower regime, five Supreme Court justices, including Justice Thurgood Marshall, raised major concerns with the BSA's requirements under the Fourth Amendment. While two of those justices ultimately found that the BSA, as it stood in 1974, did not violate the Constitution, today's BSA asks more of financial institutions and citizens and operates on a financial system that has changed dramatically from the early 1970s. In fact, two current Supreme Court justices (Justices Neil Gorsuch and Sonia Sotomayor), recognizing these (and other) changes, have signaled a willingness to revisit some of the constitutional questions that the Court raised in the early 1970s.

It should be easy for Congress to fix the BSA because the basic framework to balance the competing interests of individuals' financial privacy and the government's ability to gather evidence to enforce laws is already present in the Fourth Amendment. This constitutional right generally requires the government to obtain a warrant upon a showing of probable cause to obtain access to an individual's person, house, papers, and effects. It is this framework that should guide reform of the BSA to limit government intrusion into individuals' private financial affairs.


NORBERT J. MICHEL is vice president and director of the Cato Institute's Center for Monetary and Financial Alternatives.
JENNIFER J. SCHULP is director of financial regulation studies at the Center for Monetary and Financial Alternatives.

INTRODUCTION

The Bank Secrecy Act of 1970 (BSA) and its later amendments, including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act) in 2001, require financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering and other crimes. The BSA now forms the basis of an extensive—and costly—regulatory framework. Yet, if judged by the standard of reducing predicate crimes, there is virtually no empirical evidence to suggest that the approach has worked. Instead, the evidence suggests that the BSA framework has proven a minor inconvenience for criminals but a major burden on law-abiding citizens.

The BSA was enacted without careful study or forethought. Congressional hearings clearly show that the bill's supporters had not fully considered whether the legislation included appropriate solutions to the supposed abuse of secret foreign bank accounts. Congress and the Department of the Treasury then spent five-plus decades building on this shaky BSA framework to supposedly better deter criminals, but the evidence shows no net benefit to this approach. Rather, the expansion of the BSA has dramatically increased explicit compliance costs for financial institutions and diminished Americans' constitutionally protected rights.

> "The evidence suggests that the BSA framework has proven a minor inconvenience for criminals but a major burden on law-abiding citizens."

At minimum, Congress should amend the BSA to remove the reporting requirements that force financial institutions to act as law enforcement agents and allow the U.S. government to intrude into private citizens' financial business without the protections guaranteed by the Constitution. Limiting the BSA to recordkeeping requirements would preserve relevant information for criminal investigations and allow federal resources to be more efficiently focused on catching criminals while respecting constitutional safeguards. As the digital age takes hold, it is more important than ever that the United States lead the way in protecting individuals' rights against government overreach and setting the standard for personal financial privacy.

HISTORY OF THE ANTI–MONEY LAUNDERING FRAMEWORK

Congress passed a bill in 1970, several titles of which have become known as the BSA.[1] No member did more to promote that legislation than Rep. Wright Patman (D-TX), the chairman of the House Committee on Banking and Currency in 1968. Known as the "last populist," Patman ultimately served 24 consecutive terms in the House (from 1929 to 1976), and he believed that "the root of all evil was the concentration of economic power in the hands of a small number of bankers, business executives and government officials."[2] Patman held a "preliminary inquiry" hearing in December 1968 and then introduced his legislation at another hearing in December 1969.

The stated purpose of the 1968 hearing was to "inquire into some of the practices of foreign banking institutions, and their depositors."[3] At the end of the hearing, Patman announced his intent to introduce a bill. According to Patman, his legislation would

> make it a criminal offense for any U.S. citizen to have financial dealings with a foreign financial institution that does not allow bona fide inspection of its records by our various regulatory agencies concerning the transactions involving the Americans. This legislation would merely extend the financial safeguards that we have in this country to foreign financial institutions dealing with Americans. It would go a long way toward protecting the interests of the vast majority of Americans who do not engage in any financial manipulations and would prevent the outflow of so-called hot money to foreign banking institutions.[4]

Ultimately, the legislation that became the BSA went much further than merely extending existing "financial safeguards" and did not make it a crime to deal with foreign financial institutions. It remains the statutory foundation for the existing federal anti–money laundering (AML) regulatory framework.

Patman's bill made two major changes to existing federal laws: one that required financial institutions to maintain records "where such records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings" and one that required the reporting of certain financial transactions to the Treasury Department.[5] The bill specified that transactions of more than $5,000 in monetary instruments transferred either into the United States or out of the United States had to be reported.[6] This provision became the statutory basis for requiring the filing of a Report of International Transportation of Currency or Monetary Instruments, or CMIR. The bill also required reporting on domestic transactions, which became the statutory basis for filing currency transaction reports, or CTRs. The bill left the details on what would be required up to the Treasury.[7]

Given this statutory language, Patman clearly did not direct his bill solely toward making it more difficult for Americans to hide funds using foreign financial institutions. It is even more disturbing, though, how little justification the hearings revealed for the changes that the bill implemented. Both the 1968 and 1969 hearings relied on little more than government officials' anecdotes and assurances that access to more information was essential to effective law enforcement. None of the witnesses provided data to support the prevalence of the ostensible money laundering problems through either domestic or foreign financial institutions. Moreover, the witnesses barely discussed how the specific legislative proposals for domestic transactions might improve the ability to prosecute crimes. Given that the witnesses acknowledged the successful prosecutions that were already taking place, this shortcoming is notable.

1968 Hearing

Patman began the 1968 hearing by summarizing the problems his committee was considering. Against a backdrop of using secret foreign bank accounts, he mentioned "the illicit financial manipulation of huge sums of money," income tax evasion, fraudulent defense contracts, the theft of Treasury bills, corporate kickbacks by Vietnamese importers, various types of securities fraud, and the use of "fictitious" and "dummy" corporations. One witness, U.S. attorney for the Southern District of New York Robert Morgenthau, decried how secret Swiss bank accounts had become an "increasingly widespread and versatile tool" to evade U.S. laws and regulations. He explicitly accused many of the "millions of Americans" who vacation in Europe of finding that "secret foreign banks are available readily to them for lucrative criminal purposes." Yet he was unable to provide any data to support his claims. Morgenthau similarly claimed that "enormous numbers" of investors used foreign banks to "evade income taxes on their trading profits" and that the number of tax evaders had become "very large," representing "a loss of tax revenues in the many millions of dollars."[8]

"It is even more disturbing, though, how little justification the hearings revealed for the changes that the bill implemented."

Morgenthau also complained of other illegal activities, including fraudulent stock market transactions, insider trading, and the avoidance of margin requirements. Most of his anecdotes discussed cases that were successfully prosecuted even though the alleged activity took place long before the 1968 hearing. He testified that he often could not prosecute criminals because foreign banks would not "furnish witnesses competent to introduce their banking documents into evidence," and as a result, "it should be obvious" that the increasing number of "successfully prosecuted criminal cases" by his office represented only "a small fraction of the crimes committed by Americans through secret foreign accounts." He also opined that "even if 99 or 98 percent of citizens pay their income taxes and abide by the securities laws, a substantial percentage of our citizens are evading the payment of taxes and violating other laws through the use of Swiss and other foreign banks." In Morgenthau's view, this situation was "a serious problem in itself, and if it goes unchecked, more and more people are going to try to use this device."[9]

Other witnesses, such as Irving Pollack and Mahlon Frankhauser of the Securities and Exchange Commission (SEC), similarly described stories of tax evasion and violations of securities laws and regulations. However, just as Morgenthau had done, Pollack mentioned examples of fraud that had already been successfully prosecuted, such as the case where "American corporate officials, and others, used such foreign intermediaries to mask a massive distribution

to the American public of worthless securities of an insolvent corporation at a manipulated price." Separately, then assistant attorney general Fred Vinson outlined some of "the principal Federal laws and regulations" that criminals might violate using foreign bank accounts, singling out Section 7 of the 1934 Securities Exchange Act, whereby the Federal Reserve sets limits on how much credit can be used to purchase securities.[10]

"What was even stranger, though, was that Vinson later testified that many countries, even Switzerland, *did* share financial transaction and account holder information with U.S. authorities."

What was even stranger, though, was that Vinson later testified that many countries, even Switzerland, *did* share financial transaction and account holder information with U.S. authorities. Vinson pointed out that the problem with the Swiss banks—the most frequently used foreign institutions for these purposes—was not that the Swiss refused to help U.S. prosecutors. The problem instead was that Swiss laws required court orders for Swiss bankers to disclose information. Vinson objected that the court order process took too long and stated that the difficulty was "more a matter of attitude than of law; the attitude being, regardless of the merit of the request, that they should be very slow, and they are very slow to furnish judicial assistance." It is difficult to see how any of the changes in Patman's bill addressed this problem, and even Pollack affirmed his belief that the only solution would be for the United States to enter into treaties or other international agreements for sharing information.[11]

Regardless of whether it was possible for prosecutors to gather sufficient information in a timely manner, the witnesses again presented no empirical evidence describing the size and scope of the alleged problems. Pollack stated that it would "take some time" to find out what percentage of exchange trading was done on behalf of foreigners or foreign accounts. Frankhauser added that the SEC "unfortunately lack[s] very precise figures in this area" and that the SEC "do[es] not know the full extent or number of special omnibus accounts that are carried by U.S. brokers for Swiss banks." After Patman referred to an FBI estimate that "there might be as much as $12 million a year in skim, gambling skim winding up in the hands of members of organized crime," a "significant amount" of which may go abroad, Pollack stated that "just how great [these fraudulent transactions] are is a difficult thing for any of us, I guess, to estimate, since we can't get the information because of restrictive laws operating in foreign countries."[12]

1969 Hearing

Patman held another hearing in December 1969 and introduced his draft legislation. At the beginning of the hearing, Patman announced that his legislation had been "carefully drafted so that it is aimed at the prevention of the use of secret foreign financial facilities for illegal purposes by those subject to U.S. laws."[13] But as discussed at the 1968 hearing, the problem was primarily caused by foreign banking laws, meaning that cooperation from foreign governments is necessary to facilitate information sharing with federal authorities. The bill does nothing to directly address that issue, though, and Patman expressly stated that he wanted to avoid creating burdensome regulations that would infringe on the laws of any other nation.

Patman also claimed that his legislation and the 1969 hearings were "a direct result of a 1-day investigative hearing held by this committee on December 9, 1968," and that those hearings revealed that "the use of these secret foreign bank accounts and foreign financial institutions as part of illegal schemes by American citizens and others created a tremendous and grave problem of law enforcement in the United States." He then mentioned that Morgenthau (who participated in both hearings) had estimated that the loss in tax revenues to the U.S. government due to the use of these secret foreign accounts was in the "hundreds of millions."[14] The record from the 1968 hearing demonstrates, however, that Patman's statements (at best) mischaracterize what occurred during those proceedings.

One of the most revealing exchanges at the 1969 hearing occurred when Rep. William Widnall (R-NJ) briefly stopped Patman from getting to the first witness.

> *Widnall*: Before you start off . . . may I ask this question: You have read a list of those who will be heard

from or you hope to hear from during the course of these hearings. The bill encompasses more than just Swiss bank accounts. Is it contemplated that any banks will be invited to act as witnesses?

Patman: Yes. If they would like to appear, we will be glad to have them. Would you submit the names of any you want to testify?

Widnall: Nobody has asked me, but the question arose in my mind because there is in the bill some things that would involve banks.[15]

Patman then moved on, and the remainder of the testimony was remarkably like that given during 1968, when multiple government officials discussed the problem of secret foreign bank accounts with respect to tax evasion and fraud.

> "Several members also objected that the domestic transaction reporting requirements would violate the privacy of bank customers, that they would 'unduly burden legitimate commercial transactions,' and that they delegated 'too much power' to the Treasury secretary."

Morgenthau's 1969 testimony referenced some of the same prosecutions that he had discussed in 1968, as well as additional cases that resulted in convictions. He also reiterated his belief that there were many more instances of criminal activity that he was unable to prosecute (due to either lack of resources or because the existing evidence was inadmissible in court) and gave his estimate that "deposits in secret foreign bank accounts held for illegal purposes have a value in the hundreds of millions of dollars."[16] As during the first hearing, he provided no evidence to substantiate this opinion, nor did he discuss the legitimate reasons in the U.S. tax code for Americans to invest in foreign jurisdictions.[17]

Later, when answering Widnall and Rep. Ben Blackburn (R-GA), then assistant U.S. attorney general Will Wilson acknowledged that there was nothing illegal about transporting large amounts of cash *unless* the money was stolen property or somehow derived by illegal means and that prosecutors face the same search and seizure problems with any kind of property that Americans attempt to transport internationally. Similarly, Widnall told two witnesses (Randolph Thrower, the IRS commissioner, and Eugene Rossides, an assistant Treasury secretary) that while he understood they were both endorsing the *objectives* of the bill, he recognized that "you are trying your best to point up the difficulties in connection with not just the administration of it but in arriving at the right solution, and until you have had a chance to study it even more."[18]

Given how this process unfolded, it is hardly surprising that multiple members of Congress complained that the bill's domestic transaction reporting requirements did not address the legislation's stated purpose. As a 1983 report by the Department of Justice noted, "many Congressmen argued that the reports regarding domestic transactions [in the BSA] were not relevant to the purpose of the legislation, which was to address the problems caused by the foreign bank secrecy laws" and that those portions of the bill should be severed and considered later. Patman, however, was able to overcome such objections by "stressing the urgent need for the legislation and the need for uniform recordkeeping." Several members also objected that the domestic transaction reporting requirements would violate the privacy of bank customers, that they would "unduly burden legitimate commercial transactions," and that they delegated "too much power" to the Treasury secretary.[19]

Despite these misgivings, Patman's legislation passed in 1970 and still forms the core of the AML regulatory framework in the United States and, thanks mainly to the efforts of the U.S. government, many other countries.

THE BANK SECRECY ACT, THEN AND NOW

The biggest statutory changes implemented by the BSA in 1970 were the new recordkeeping and reporting requirements. As noted earlier, the legislation required financial institutions to maintain records "where such records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings" and gave the Treasury

secretary the regulatory authority to determine which records displayed such usefulness.[20]

Separately, the legislation required reporting of two types of transactions in currency. First, anyone, "whether as principal, agent, or bailee," who transfers funds in to or out of the United States "in an amount exceeding $5,000 on any one occasion" must report the transaction according to regulations promulgated by the Treasury secretary.[21]

Second, the legislation required the reporting of certain domestic financial transactions, but it left virtually all those details (including a threshold amount) up to the Treasury. The legislation stated:

> Transactions involving any domestic financial institution shall be reported to the Secretary at such time, in such manner, and in such detail as the Secretary may require if they involve the payment, receipt, or transfer of United States currency, or such other monetary instruments as the Secretary may specify, in such amounts, denominations, or both, or under such circumstances, as the Secretary shall by regulation prescribe.[22]

The Treasury promulgated the first BSA rules in 1972, requiring financial institutions to "file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution, which involves a transaction in currency of more than $10,000."[23] This $10,000 reporting threshold remains unchanged.

The next time that Congress made major changes to the BSA was in 1986, when it passed the Money Laundering Control Act, which established money laundering as a criminal offense.[24] In addition, Section 1354 of the act made it a criminal offense to structure transactions to evade the BSA reporting requirements.[25] This law also expanded compliance obligations for banks by amending Section 8 of the Federal Deposit Insurance Act and Section 206 of the Federal Credit Union Act to require essentially all banks subject to federal regulation to "establish and maintain procedures reasonably designed to assure and monitor the compliance" with the BSA provisions and to include a review of banks' BSA compliance procedures in all federal bank examinations.[26]

In 1992, the Annunzio-Wylie Anti–Money Laundering Act strengthened sanctions for BSA violations.[27] For instance, Sections 1501 and 1502 provided that federal banking regulators could appoint a conservator or revoke a federal banking charter for banks guilty of a money laundering offense.[28] Section 1504 provided that federal banking regulators could remove officers or directors of a depository institution for various BSA violations (including those committed by other employees of the institution),[29] and Section 1512 prohibited the operations of an illegal money transmitting business.[30]

"But the most consequential change made in 1992 was the addition of the statutory basis for requiring financial institutions to file what are now known as suspicious activity reports (SARs)."

But the most consequential change made in 1992 was the addition of the statutory basis for requiring financial institutions to file what are now known as suspicious activity reports (SARs). Specifically, Section 1517 authorized the Treasury secretary to "require any financial institution, and any director, officer, employee, or agent of any financial institution, to *report any suspicious transaction* relevant to a possible violation of law or regulation."[31] As a result of this statutory requirement, financial institutions were required to file "criminal referral forms," with supporting documentation, with multiple federal agencies.[32]

The Money Laundering Suppression Act of 1994 established the modern SAR reporting regime by authorizing the Treasury to designate a single officer or agency to "refer any report of a suspicious transaction to any appropriate law enforcement or supervisory agency."[33] This led to the creation of the Financial Crimes Enforcement Network (FinCEN).

In April 1996, FinCEN finalized the first regulation to create "a new method for the reporting by depository institutions, on a uniform 'Suspicious Activity Report,' of suspicious transactions and known or suspected criminal violations."[34] The final rule required banks to file for transactions—not limited merely to transactions in currency—of at least $5,000 that they know (or have reason to suspect) are derived from illegal activity, or those that they believe are designed to "hide or disguise funds or assets derived from

illegal activities . . . as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation."[35]

The next major change to the BSA came after the September 11, 2001, terrorist attacks, when Congress passed the Patriot Act. Title III of the Patriot Act added multiple provisions intended to improve the federal government's ability to stop terrorist financing internationally.[36] For example, Section 311 authorized the Treasury secretary to designate a foreign jurisdiction or foreign financial institution as a primary money laundering concern,[37] and Section 312 required U.S. financial institutions that maintain a banking relationship with "a non–United States person" to "establish appropriate, specific, and, where necessary, enhanced, due diligence policies, procedures, and controls" to detect and report money laundering.[38] Section 313 prohibited U.S. financial institutions from establishing correspondent accounts with foreign shell banks (those that have no physical presence in any country),[39] and Section 319 enhanced the federal government's ability to seize funds in an interbank account in the United States.[40] Section 356 also expanded the group of financial institutions required to file SARs to include broker-dealers (firms engaged in purchases and sales of securities).[41]

"Prior to the act, financial institutions were generally charged with obtaining information about the beneficial owners of a corporate customer as part of their customer identification programs and customer due diligence processes."

Multiple sections of the Patriot Act (such as Sections 328 and 330) imposed responsibilities on the executive branch to negotiate with and encourage foreign governments to assist the U.S. government in detecting money laundering and terrorist financing. Section 361 formally made FinCEN a bureau of the Treasury Department, and Section 363 increased civil and criminal penalties for money laundering. Interestingly, Section 371 made "the act of smuggling bulk cash itself a criminal offense," after noting that Congress found that "effective enforcement of the currency reporting requirements" of the BSA have "forced drug dealers and other criminals engaged in cash-based businesses to avoid using traditional financial institutions."[42]

Another major Patriot Act provision is directly related to financial firms' operations. Section 326 required the Treasury secretary to prescribe regulations that establish "the minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution."[43] These regulations must, at minimum, "require financial institutions to implement, and customers (after being given adequate notice) to comply with reasonable procedures" to verify each potential account holder's identity, including maintaining records of the information used to verify identity and consulting government-provided lists of known terrorists.[44] To implement these requirements, FinCEN has promulgated regulations that generally compel financial institutions to have written customer identification programs that are appropriate for their "size and type of business," as well as appropriate "risk-based procedures for conducting ongoing" customer due diligence.[45]

The Anti–Money Laundering Act of 2020 implemented the most recent set of legislative changes to the BSA.[46] The act expands the federal government's role in combating financial crimes in multiple ways, such as by creating FinCEN domestic liaisons, BSA information security officers, BSA innovation officers, and a government-based financial crimes tech symposium.[47] Through these and other changes, the act is supposed to "improve coordination and information sharing" among federal agencies and law enforcement to help counter terrorism and money laundering. It also codifies that the AML regulatory framework is supposed to be based on risk and tries to modernize the regulatory framework by (among other changes) accounting for the use of cryptocurrency and digital assets. Specifically, the act expands BSA definitions in several places to include the term "value that substitutes for currency."[48]

One of the biggest changes that the 2020 act implements to the BSA is the establishment of "uniform beneficial ownership information reporting requirements." Prior to the act, financial institutions were generally charged with obtaining information about the beneficial owners of a corporate customer as part of their customer identification programs

and customer due diligence processes. Section 6403 of the act places the burden on the company and requires the company to report identifying information to a central database that FinCEN manages, in accordance with regulations to be promulgated by the Treasury.[49] These provisions are intended to prevent people from circumventing AML laws using shell corporations, one problem that the BSA was supposed to mitigate when originally enacted in 1970.[50]

"Financial institutions file millions of reports each year even though records show that there are only about 2,000 money laundering investigations per year."

As this brief history makes clear, Congress gave federal regulators a great deal of discretion to establish the AML regulatory framework, which has expanded well beyond the basic recordkeeping and reporting requirements established by the BSA in 1970. The AML framework has also led to the creation of multiple, expensive, and overlapping national and international bureaucracies. Mostly due to the efforts of the U.S. government, there is now a long list of national and international agencies, as well as national laws and international agreements, governing the exchange and reporting of financial information. For instance, there are more than 100 foreign financial intelligence units around the world, a role that FinCEN fills in the United States.[51] Virtually all countries now have laws and regulations that require private entities to collect and report financial information much like what the United States requires under the BSA.[52] Both American and foreign financial institutions must report on the financial activities of their U.S. customers under the Foreign Account Tax Compliance Act and the qualified intermediary rules.[53] The terrorism-related Information Sharing Environment, a center within the Office of the Director of National Intelligence, involves thousands of federal, state, local, and tribal government agencies,[54] and the FBI also operates (among other programs) a National Data Exchange. Finally, the International Criminal Police Organization, or INTERPOL, maintains various information-sharing databases that it makes available to its 190 members.[55]

Moreover, the wide discretion given to FinCEN, as well as the potential for being held criminally liable, predisposes financial institutions to err on the side of filing too many reports rather than too few. As a result, financial institutions—a list of companies that now includes banks, broker-dealers, pawnbrokers, travel agencies, and at least 10 other types of companies[56]—file millions of reports each year even though FBI and IRS records show that there are only approximately 2,000 money laundering investigations per year.[57] The current approach is heavily biased toward collecting as much information as possible with little regard for whether the information is useful for investigations and even less regard for the burdens imposed on financial institutions and those who seek their services.

COSTS AND BENEFITS OF THE BSA/AML REGIME

Multiple federal regulators enforce the BSA/AML rules, which impose heavy compliance costs on financial institutions and individual citizens alike.[58] Essentially, the AML rules ensure that financial institutions cannot legally transfer money without knowing who the customer is and having some idea of where the money came from.[59] The rules make it very difficult for anyone to transfer funds anonymously unless they use small amounts of paper currency.

Current federal regulations require financial institutions to report transactions of more than $10,000[60]—the same threshold used for currency transaction reports in the original 1972 rule—and the failure to report such transactions is a criminal offense.[61] Most financial institutions have a $5,000 threshold for filing SARs, but some, such as most money-service businesses, have their own $2,000 threshold.[62] Separately, all financial institutions categorized as money-service businesses must obtain and record specific information for all transfers of at least $3,000,[63] and all currency exchangers must track any exchange that exceeds $1,000 in either domestic or foreign currency.[64]

The AML rules also go well beyond the submission of reports. Federal regulators require, for instance, financial institutions to institute formal BSA/AML compliance programs.[65] Regulators heavily micromanage this process, requiring (at minimum) internal controls, independent testing for compliance, hiring a compliance officer, and providing employees

with formal training programs.[66] The overall BSA compliance program is distinct from a customer identification program,[67] and it is not uncommon for regulators to require financial institutions to devote additional personnel and physical resources to their compliance programs.[68]

In December 2021, for instance, FinCEN fined the CommunityBank of Texas $8 million for BSA violations that occurred between 2015 and 2019, on top of the $1 million fine assessed by a separate investigation for related violations by the Office of the Comptroller of the Currency (OCC).[69] According to FinCEN, the bank's compliance program during the relevant period was insufficient because it was "understaffed," even though the bank retained "six to eight BSA staff, including a BSA Officer and several BSA analysts, of which three reviewed case alerts on a regular basis and provided quality control review for one another."[70]

These types of regulations impose on financial institutions high explicit and implicit costs, some of which are passed on to consumers. The regulations leave financial institutions in constant legal jeopardy with a set of largely unreasonable expectations. For instance, the consent order between FinCEN and the CommunityBank of Texas faults the bank for failing to file SARs on persons that were known to be gamblers. The order then singles out one such customer (Customer A) and says that "in June 2019, Customer A, Customer A's spouse, and another family member pleaded guilty to criminal charges including structuring, tax evasion, and money laundering associated with operating an illegal sports gambling operation from at least 1985 until April 2017."[71] It makes little sense to fine a bank (or any private business) for failing to detect criminals who, allegedly, were able to evade law enforcement for more than 30 years.

More broadly, it makes little sense to force private businesses to serve as law enforcement officials. It is hardly surprising, therefore, that the BSA/AML regime has proved so ineffective at stopping criminal activity. If judged by the standard of reducing predicate crimes, there is virtually no empirical evidence to suggest that the BSA/AML framework has worked.

One comprehensive study, for instance, points out that the U.S. General Accounting Office (GAO) has made several unsuccessful attempts to study the effectiveness of SAR filings in terms of prosecutions and convictions. One problem is that prosecutions often involve simultaneously charging perpetrators with money laundering violations, thus obscuring whether law enforcement discovered, for example, a drug crime because of money laundering or vice versa. According to the GAO, as of 2002, FinCEN was unable to report whether any of its SAR-based referrals resulted in criminal prosecutions.[72] As late as 2014, academic research affirmed that possible benefits from the existing AML framework (internationally) had not yet been demonstrated.[73] More recently, Rep. Patrick McHenry (R-NC), ranking member of the House Financial Services Committee, repeatedly asked the Treasury and FinCEN for evidence—not merely anecdotes about enforcement actions—that the AML regime provides a net benefit. According to McHenry, the information provided thus far "does not justify the burden placed on small businesses."[74]

"If judged by the standard of reducing predicate crimes, there is virtually no empirical evidence to suggest that the BSA/AML framework has worked."

Not only have the BSA/AML regulations been sharply criticized as a costly, ineffective approach to reducing crime, but they have also been criticized for being overly intrusive and elaborate, as well as for distorting the classical constructions of criminal law and criminal procedure. For example, one criminal law journal article reports that the framework for fighting money laundering, including the BSA, displays (among other problems) a "disproportionate imposition of severe penalties on predicate offenders who are easily detected."[75] That is, money laundering charges tend to be simply added to the main offense rather than providing any independent benefit.[76]

Overall, the evidence suggests that the AML regulatory framework has done little more than produce an information overload through excessive reporting. In 2015, for instance, the FinCEN director announced that the agency receives "approximately 55,000 electronically filed BSA reports from more than 80,000 financial institutions and 500,000 individual foreign bank account holders *each day*."[77] In 2020, FinCEN Director Kenneth Blanco caused

a stir when he announced that since 2013, FinCEN had received nearly 70,000 SARs related to "cryptocurrency exploitation," but he neglected to mention that this is a small proportion of SARs for an agency that received almost 2.3 million SARs in 2019 alone.[78]

FinCEN has also struggled with the fact that financial institutions may be reluctant to make tough decisions about what is and is not reportable on a SAR, further adding to the voluminous data by including more reports that have lower value to law enforcement officials. FinCEN has long recognized the problem of filing a SAR "defensively," so to speak, and the filing can form the basis for liability for the financial institution itself,[79] but it is easy to understand the temptation to file more, rather than less, often.[80]

This problem is compounded by the multitude of federal regulators who lay claim to ensuring compliance with the AML regulatory framework. In addition to FinCEN, the federal banking regulators, the IRS, the SEC, and the Financial Regulatory Authority, among others, examine and investigate the effectiveness of financial institutions' AML compliance programs and whether those firms have met their obligations to file SARs, have a customer identification program, and perform customer due diligence.[81] It is not unusual for more than one regulator to bring an action on the same set of facts. Regulators levied more than $592 million in fines for AML violations in 2021 alone, and they have long cited AML enforcement as a top priority, often bringing with it some of the highest fines collected by the agencies.[82]

Unsurprisingly, research suggests that compliance costs are high for financial companies, with a disproportionate burden falling on smaller firms.[83] Though few total compliance cost estimates exist, one based on Office of Management and Budget burden-hour estimates suggests that total BSA/AML costs are between $5 billion and $8 billion per year.[84] This total cost can be used to estimate per-conviction figures, but because federal agencies' money laundering statistics vary, these averages display a wide range. For instance, using IRS-initiated money laundering sentences, and assuming (generously) that all such sentences would not have occurred but for the AML statutes, the per-conviction cost is at least $7 million.[85] Using, instead, the FBI's money laundering conviction totals, the per-conviction cost is between $107 million and $178 million.[86]

Given the stakes, financial firms may be reluctant to take on customers or activities that make their regulatory compliance more difficult. In fact, in 2018, the GAO "determined that Bank Secrecy Act/anti–money laundering (BSA/AML) regulatory concerns have played a role in banks' decisions to terminate and limit customer accounts and close bank branches."[87] Though not explicit, the AML regulatory framework imposes costs on would-be financial services customers, with firms simply refusing to provide some financial services to certain customers. These rules have also likely contributed to financial firms' hesitancy to work with emerging industries, such as cryptocurrency-related companies and blockchain-based technologies. This hesitancy can hinder innovation and competition in financial markets, one of several difficult-to-quantify costs associated with this regulatory regime.

"Federal Deposit Insurance Corporation surveys also suggest that approximately one-third of the unbanked have chosen to stay out of the banking system because they do not want to provide the personal information that AML regulations require."

Many law-abiding customers have had their accounts frozen, at least temporarily, and have been kept out of the banking system. For instance, long before 2022, many Russian Americans had their accounts closed by banks who feared being liable for AML violations simply due to these customers' connections to Russia. Similarly, a recent World Bank survey demonstrated that firms providing foreign remittance services have been increasingly scrutinized under the AML regime since the early 2000s; of more than 80 money transfer operators across 13 countries, almost half had their bank accounts closed.[88] In the United States, Federal Deposit Insurance Corporation surveys also suggest that approximately one-third of the unbanked have chosen to stay out of the banking system because they do not want to provide the personal information that AML regulations require.[89]

The BSA framework is an ineffective way to fight crime. Indeed, multiple members of Congress noted during the 1968 and 1969 hearings that it was difficult to see how any of the legislative changes they were contemplating would solve the foreign-bank money laundering and tax evasion problems that they were hoping to stop. The expansion of the BSA over the years has not changed this basic dynamic.

> "Even without BSA/AML reporting requirements, financial institutions already have incentives to implement programs that avoid criminal activity, including cybercrimes."

It is also not clear why a heavy AML burden should be placed on (either narrowly or broadly defined) financial institutions because *all* business transactions can potentially be used to launder money. Regardless, most types of businesses—financial or otherwise—are generally ill-equipped to catch criminals, especially when those criminals go to great lengths to conceal their crimes.[90] It makes little sense to penalize legitimate businesses for failing to know that their customers might have engaged in criminal activity, and prosecutors should prosecute criminals for their crimes irrespective of what payment methods they use.

While BSA supporters typically point to enforcement actions or prosecutions as evidence that the regime is working, such examples, by themselves, provide no such proof. First, many actions arise from other criminal activity, thus alerting federal regulators who otherwise would not have discovered BSA/AML violations. These cases demonstrate that the BSA/AML regulations did not stop criminal activity.

Other incidents show how difficult it can be to detect criminal activity and that federal regulators are themselves vulnerable to criminals. For example, in 2016, North Korean hackers broke into the SWIFT messaging network, stealing almost $100 million from the Bank of Bangladesh by routing it into private accounts through the Federal Reserve Bank of New York.[91] Had it not been for a fluke occurrence, the thieves would have tricked the New York Fed into routing them nearly $1 billion from the Bank of Bangladesh.[92] Similarly, the U.S. federal government has proven itself to be far from immune to cybercrime in recent years, and the SARs database itself contains a wealth of information that could be attractive to hackers or other criminals. On these grounds alone, it makes sense to avoid creating these data-rich targets inside federal agencies.

Even without BSA/AML reporting requirements, financial institutions already have incentives to implement programs that avoid criminal activity, including cybercrimes. It is doubtful—based on experience—that holding these firms legally responsible for AML programs that fail to stop criminals can improve those incentives. Even if Congress fully repealed the BSA, it would remain illegal for financial institutions to knowingly facilitate criminal activity such as tax evasion or the sale of illegal drugs,[93] and reputational risks for financial institutions found to be assisting criminals are high.

Regardless, there is little to support the idea that federal agencies have the knowledge and ability to design AML programs that more effectively deter criminal activity. It is not unusual for federal regulators to cite financial institutions for AML violations after federal regulators, during their annual bank examinations, certified that the offending bank had a sound AML program in place. The frequency of these occurrences suggest that enforcement often operates with the benefit of hindsight and that certifications in the examination process say little about whether a financial institution has an AML program that can identify criminal activity.

In January 2021, for instance, FinCEN announced that it would assess $290 million in penalties against Capital One, a fine that came two years after the OCC had assessed $100 million in penalties for the same violations. FinCEN said that Capital One failed to "adequately monitor the cashing of millions of dollars" of checks by more than 100 customers dating between 2008 and 2014.[94] The OCC has examined Capital One every year, for decades, and the OCC has been statutorily required to review banks' BSA/AML programs during those exams beginning in 1986. At the very least, it is difficult to argue that the OCC knew how to design an effective BSA/AML program for Capital One. Overall, the evidence demonstrates that the BSA/AML regulatory framework does little more than impose heavy explicit and implicit costs on millions of Americans.

PRIVACY, CONSTITUTIONAL RIGHTS, AND THE BSA

Personal and financial privacy are key components of life in free societies, where individuals enjoy a private sphere free of government involvement, surveillance, and control.[95] Unless there is a reasonable suspicion that they have committed a crime or conspired to commit a crime, people should generally be free to live their lives unmolested and unsurveilled by the government.[96] Financial privacy is of deep and abiding importance to freedom, but many governments have shown themselves willing to routinely abuse private financial information. Financial privacy can let people protect their life savings when a government tries to confiscate its citizens' wealth, whether for political, ethnic, religious, or "merely" economic reasons. As events in Canada in early 2022 demonstrate, even relatively free governments are sometimes willing to use private financial information to quell nonviolent protests.[97]

In 2021, the Biden administration proposed to "create a comprehensive financial account information reporting regime" for all financial accounts with a "gross flow threshold" of $600 or more.[98] In response, many Americans expressed their disbelief that such a proposal did not run afoul of the protections guaranteed by the Fourth Amendment to the U.S. Constitution.[99] As it turns out, many Americans wondered the same thing about the BSA when it was enacted in 1970, sparking lawsuits that ended up before the Supreme Court.[100]

The two major Supreme Court cases regarding the BSA were *California Bankers Association v. Shultz* (decided 6–3) in 1974 and *United States v. Miller* (decided 7–2) in 1976.[101] These cases resulted in Americans losing what one commentor has called any "protectible interest in records held by a third party."[102] Both cases are ripe for revisiting, though, in light of the concerns that some justices raised at the time, the changes in information sharing brought by the digital age, and the increasingly broad reach of the BSA.

California Bankers Association v. Shultz

In *California Bankers Association v. Shultz*, the Court addressed the constitutionality of both the recordkeeping and reporting provisions of the BSA, upholding those provisions.[103] The Court held that the BSA recordkeeping provisions did not violate the Fourth Amendment, finding that nothing in the recordkeeping provisions require that any information be disclosed to the government.[104] The Court rejected plaintiffs' argument that the banks were themselves effecting a seizure of customer records acting as "agent[s] of the Government," noting that banks, who are themselves a party to the transaction, "voluntarily kept records of this sort before they were required to do so by regulation."[105]

"Financial privacy is of deep and abiding importance to freedom, but many governments have shown themselves willing to routinely abuse private financial information."

The Court also upheld the reporting provisions of the BSA, finding no violation of the Fourth Amendment. For the foreign reporting requirements, the Court relied on the fact that the requirements dealt with matters "in foreign commerce," over which the government has stronger authorities.[106] For the domestic reporting requirements, the Court's analysis was different: it held that the reporting requirements did not violate any Fourth Amendment rights of the banks because they are parties to the transactions themselves but found that the depositors lacked standing to assert a Fourth Amendment claim because they had not shown that their transactions were required to be reported.[107]

Thus, while the Supreme Court upheld the BSA's reporting provisions, it did not address the fundamental question of whether the reporting requirements violated the Fourth Amendment rights of bank customers to be free from the government's search and seizure of their records. The lower court had found that the provision violated the Fourth Amendment, "insofar as it authorizes the Secretary to require virtually unlimited reporting from banks and their customers of domestic financial transactions as a surveillance device for the alleged purpose of discovering possible, but unspecified, wrongdoing among the citizenry."[108]

Although the Court upheld the BSA, the justices were divided over the BSA's implications for

constitutional protections. Even Justices Lewis Powell and Harry Blackmun, who joined the majority in upholding the law, wrote a concurring opinion explicitly cautioning against "a significant extension of the regulation's [domestic] reporting requirements":

> Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy. Moreover, the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process.[109]

Justices William O. Douglas, William J. Brennan Jr., and Thurgood Marshall filed separate dissents voicing similar concerns with the BSA but found that the law, as then conceived, violated the Constitution.

Justice Douglas recognized that "customers have a constitutionally justifiable expectation of privacy in the documentary details of the financial transactions reflected in their bank accounts." He acknowledged that the "wall is not impregnable" but found that both the recordkeeping and reporting provisions ran afoul of the Fourth Amendment.[110] On the recordkeeping provision, Douglas wrote:

> Since the banking transactions of an individual give a fairly accurate account of his religion, ideology, opinions, and interests, a regulation impounding them and making them automatically available to all federal investigative agencies is a sledge-hammer approach to a problem that only a delicate scalpel can manage. Where fundamental personal rights are involved—as is true when as here the Government gets large access to one's beliefs, ideas, politics, religion, cultural concerns, and the like—the Act should be "narrowly drawn" to meet the precise evil. Bank accounts at times harbor criminal plans. But we only rush with the crowd when we vent on our banks and their customers the devastating and leveling requirements of the present Act. I am not yet ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals.[111]

Douglas contrasted the BSA with other compulsory recordkeeping that did not raise the same constitutional concerns, noting that prior to the BSA, the United States had "confined compulsory recordkeeping to that required to monitor either (1) the recordkeeper, or (2) his business" and that even then "they must be records that would 'customarily' be kept, have a 'public' rather than a private purpose, and arise out of an 'essentially noncriminal and regulatory area of inquiry.'"[112]

Douglas returned to the characterization that a "checking account . . . may well record a citizen's activities, opinion, and beliefs" to find that the reporting provisions violate the Constitution.[113]

> The Fourth Amendment warrant requirements may be removed by constitutional amendment but they certainly cannot be replaced by the Secretary of the Treasury's finding that certain information will be highly useful in "criminal, tax, or regulatory investigations or proceedings."[114]

Justice Brennan joined Douglas's concurrence as to the recordkeeping provisions but wrote separately on the reporting provisions, finding that those provisions violated the Constitution by delegating to the Treasury secretary "in broad and indefinite terms under a statute that lays down criminal sanctions and potentially affects fundamental rights."[115]

"Justice Marshall wrote a separate dissent to emphasize that he saw the BSA's recordkeeping provisions themselves as an unlawful search and seizure."

Justice Marshall also agreed with Douglas and Brennan but wrote a separate dissent to emphasize that he saw the BSA's recordkeeping provisions themselves as an unlawful search and seizure:

> By compelling an otherwise unwilling bank to photocopy the checks of its customers the Government has as much of a hand in seizing those checks as if it had

> forced a private person to break into the customer's home or office and photocopy the checks there.[116]

Marshall also worried that the existence of these records "will chill the exercise of First Amendment rights of association on the part of [contributors to political organizations] who wish to have their contributions remain anonymous."[117]

United States v. Miller

Just two years later, in 1976, the Supreme Court again considered a case related to the BSA. In *United States v. Miller*, the Court addressed whether a person under criminal investigation had standing to challenge IRS subpoenas seeking information from the person's bank collected pursuant to the BSA's recordkeeping provisions.[118] While the *California Bankers Association* case did not decide whether the reporting requirements were an unconstitutional seizure of a customer's information because the majority found that the plaintiffs lacked standing to bring the claim, the Court's decision in *Miller* essentially answered the question by holding that the Fourth Amendment does not protect information revealed to the bank. Justice Powell, writing for seven members of the Court, stated:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[119]

The Court rejected all arguments that the fact that the documents were compelled to be created by the BSA altered the analysis.

Justices Brennan and Marshall again dissented.[120] Brennan largely quoted from the lower court opinion, with which he agreed: "A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes."[121] That opinion recognized the important fact that

> for all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. . . . To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.[122]

"The holding in *Miller* established what is known as the 'third-party doctrine,' which has served as a serious limitation on the Fourth Amendment's protections."

Justice Marshall expressed his exasperation with the majority's ruling:

> I wash my hands of today's extended redundancy by the Court. Because the recordkeeping requirements of the Act order the seizure of customers' bank records without a warrant and probable cause, I believe the Act is unconstitutional and that respondent has standing to raise the claim. Since the Act is unconstitutional, the Government cannot rely on records kept pursuant to it in prosecuting bank customers.[123]

The holding in *Miller* (along with another Supreme Court case in the 1970s regarding the privacy of telephone records[124]) established what is known as the "third-party doctrine," which has served as a serious limitation on the Fourth Amendment's protections by stripping a person of an expectation of privacy over information that a person voluntarily provides to a third party.

Looking Ahead

After the Supreme Court decided these cases in the 1970s, Congress passed a law to try to strengthen citizens' diminished privacy rights and constitutional protections.[125] That attempt, however, failed to allay privacy concerns amid the ever-widening regulatory framework that Congress authorized the Treasury to implement. As a result, many of the same privacy rights concerns exist today—to an even larger degree in some ways. The type of information contained in a SAR, for example, is essentially an accusation—by a financial institution, reported to the federal government—that someone has acted illegally. Even the collection of this information under strict confidentiality requirements is problematic for citizens' constitutionally protected rights, likely more so in the digital age than in the 1970s.

Yet the BSA/AML framework has consistently expanded in scope, size, and cost. In total, five justices in the *California Bankers Association* case—Powell, Blackmun, Douglas, Brennan, and Marshall—raised issues with the BSA's sweep under the Fourth Amendment. Although two of them (Powell and Blackmun) found that the BSA, as it stood in the 1970s, did not violate the Constitution, today's BSA—particularly the reporting requirements—is of much broader scope than the law that the *California Bankers Association* court faced. And the technology that gave Justice Marshall reason to find that the recordkeeping provisions constituted an unconstitutional seizure has only proliferated in later years, including by expanding the number of situations in which a customer interacts with an intermediary to conduct financial transactions. While the constitutionality of the BSA may have been upheld in 1974, these are questions that can—and should—be revisited as both the law and society have changed.

> "Especially given the technological advances in payments during the past few decades, it is now more important than ever to reform the BSA to protect privacy rights."

In fact, two current Supreme Court justices have signaled a willingness to revisit and revise the third-party doctrine. In the 2012 case *United States v. Jones*, Justice Sonia Sotomayor suggested that the idea that an individual waives privacy by sharing information with a third party might be "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[126] More explicitly, she wrote that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[127]

Justice Neil Gorsuch also wrote an extensive critique of the third-party doctrine in his dissent in *Carpenter v. United States* in 2018, in which the majority found that the third-party doctrine is not applicable to cellphone location data. Gorsuch, however, took on the third-party doctrine directly, arguing that under the traditional understanding of the Fourth Amendment's "protections for your papers and effects do not automatically disappear just because you share them with third parties."[128] Noting that "at least some of [the Supreme Court's] decisions have already suggested that the use of technology is functionally compelled by the demands of modern life," Gorsuch asserts that "just because you *have* to entrust a third party with your data doesn't necessarily mean that you should lose all Fourth Amendment protections in it."[129]

While it is virtually impossible to argue that the BSA/AML framework has markedly deterred criminal activity and provided a net benefit, federal officials have remained intent on further expanding the same approach. Especially given the technological advances in payments during the past few decades—changes that produce more voluminous transaction data with personal information that can more easily be shared—it is now more important than ever to reform the BSA to protect privacy rights.[130]

REFORM PROPOSAL

The basic framework to balance the competing interests of individuals' financial privacy and the government's ability to gather evidence to enforce laws is already present in the Fourth Amendment. This constitutional right generally requires the government to obtain a warrant upon a showing of probable cause to obtain access to an individual's person, house, papers, and effects. It is this framework that should guide reform of the BSA to limit government intrusion into individuals' private financial affairs.

One reasonable way for Congress to reform the BSA would be to require financial institutions to maintain records but to ensure that the government can only access customers' personal information with a valid search warrant. In this way, Congress could affirm that the Bill of Rights is not, to paraphrase Justice Douglas, intended to aid the prosecution of criminal cases. Given the high costs and the poor performance of the BSA in deterring criminal activity, it should be easy for Congress to implement this type of reform.

Moreover, aside from specific constitutional protections, financial privacy is vital because it can be the difference between survival and systematic suppression of an opposition group. Many businesses, dissidents, and human rights groups maintain accounts outside the countries where they are active for precisely this reason, and there are many legitimate reasons to operate anonymously owned "shell" companies.[131] The current financial regulatory framework is inconsistent with these principles.

"One reasonable way for Congress to reform the BSA would be to require financial institutions to maintain records but to ensure that the government can only access customers' personal information with a valid search warrant."

To reform the BSA so that it is consistent with these principles, Congress could keep intact the sections of the BSA that require financial institutions to maintain records but repeal those that require financial institutions to report customers' financial information to government agencies.

The main changes to the U.S. Code would be as follows:[132]

- Amend 12 U.S.C. § 3402 to strike as follows:

> Except as provided by section 3403(c) or (d), 3413, or 3414 of this title, no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and—
> ~~(1) such customer has authorized such disclosure in accordance with section 3404 of this title;~~
> ~~(2) such financial records are disclosed in response to an administrative subpoena or summons which meets the requirements of section 3405 of this title;~~
> (3) such financial records are disclosed in response to a search warrant which meets the requirements of section 3406 of this title;
> ~~(4) such financial records are disclosed in response to a judicial subpoena which meets the requirements of section 3407 of this title; or~~
> ~~(5) such financial records are disclosed in response to a formal written request which meets the requirements of section 3408 of this title.~~

- Amend 12 U.S.C. § 3413 to delete *all but* the first two subsections, with the resulting statutory language as follows:

> (a) Disclosure of financial records not identified with particular customers
>
> Nothing in this chapter prohibits the disclosure of any financial records or information which is not identified with or identifiable as being derived from the financial records of a particular customer.
> (b) Disclosure to, or examination by, supervisory agency pursuant to exercise of supervisory, regulatory, or monetary functions with respect to financial institutions, holding companies, subsidiaries, institution-affiliated parties, or other persons
>
> This chapter shall not apply to the examination by or disclosure to any supervisory agency of financial records or information in the exercise of its supervisory, regulatory, or monetary functions, including conservatorship or receivership functions, with respect to any financial institution, holding company, subsidiary of a financial institution or holding company, institution-affiliated party (within the meaning of section 1813(u) of this title) with respect to a financial institution, holding company, or subsidiary, or other person participating in the conduct of the affairs thereof.

- Repeal 12 U.S.C. § 3414
- Amend 31 U.S.C. § 5311 by deleting all but the first section, with the resulting statutory language as follows:

  (1) require financial institutions to retain transaction records that include information identified with or identifiable as being derived from the financial records of particular customers

- Repeal 31 U.S.C. §§ 5313–16
- Repeal 31 U.S.C. § 5318(a)(2)
- Repeal 31 U.S.C. § 5318A
- Repeal 31 U.S.C. § 5324
- Amend section (a) of 31 U.S.C. § 5325 so that it reads:

  (a) In General.—No financial institution may issue or sell a bank check, cashier's check, traveler's check, or money order to any individual in connection with a transaction or group of such contemporaneous transactions which involves United States coins or currency (or such other monetary instruments as the Secretary may prescribe) in amounts or denominations of $3,000 (adjusted for inflation with the consumer price index each fiscal year hereafter X, 20XX.") or more unless—

- Repeal 31 U.S.C. § 5326
- Repeal 31 U.S.C. §§ 5331–32[133]
- Repeal 31 U.S.C. § 5336
- Repeal 31 U.S.C. §§ 5341–42
- Repeal 31 U.S.C. §§ 5351–55

CONCLUSION

The United States should never have led the way in designating private companies as an extension of law enforcement agencies to criminalize the use of money. It should have done all that was necessary to strengthen the protections guaranteed by the Fourth Amendment to the Constitution to guard against government intrusion that diminishes financial privacy. It is, of course, not too late for the federal government to reverse course, thus reaffirming its commitment to protecting individuals' rights against government overreach.

Congress enacted the BSA without careful study and did not enact the appropriate solutions to the alleged problems associated with abusing secret foreign bank accounts. It is hardly surprising, therefore, that the BSA framework, though enormously costly, has provided no net benefit to deterring criminal activity. Congress should amend the BSA so that financial institutions are no longer forced to act as law enforcement agents. Requiring financial institutions only to maintain records would have the twin benefit of protecting individuals' financial privacy and improving federal agencies' abilities to prosecute criminal activity instead of devoting effort to examining program compliance and ensuring that financial institutions file millions of low-value reports.

NOTES

1. The 1970 bill does not have a specific title; it merely reads "An Act to Amend the Federal Deposit Insurance Act to Require Insured Banks to Maintain Certain Records, to Require That Certain Transactions in U.S. Currency Be Reported to the Department of the Treasury, and for Other Purposes," Pub. L. 91-508 § 231, 84 Stat. 1122 (1970). However, Title I of the bill is formally named Financial Record Keeping, and the short title of Title II of the bill is "The Currency and Foreign Transactions Reporting Act." Various government agencies have referred to the bill as "The Bank Records and Foreign Transactions Act," the "Currency and Foreign Transactions Reporting Act of 1970," or similar titles. See, for example, U.S. Department of Justice Archives, "2029. Overview of the Bank Records and Foreign Transactions Act," updated January 17, 2020; and Financial Crimes Enforcement Network (FinCEN), "FinCEN's Legal Authorities," Department of the Treasury.

2. Philip L. Zweig, *Wriston: Walter Wriston, Citibank, and the Rise and Fall of American Financial Supremacy* (New York: Crown Publishers, 1995), p. 194; and Eileen Shanahan, "Wright Patman, 82, Dean of House, Dies," *New York Times*, March 8, 1976.

3. *Legal and Economic Impact of Foreign Banking Procedures on the United States: Hearing before the Committee on Banking and Currency*, 90th Cong. 1 (1968).

4. *Legal and Economic Impact of Foreign Banking Procedures on the United States*, pp. 44–45.

5. An Act to Amend the Federal Deposit Insurance Act § 101, 84 Stat. 1114–15.

6. An Act to Amend the Federal Deposit Insurance Act § 231, 84 Stat. 1122–23.

7. An Act to Amend the Federal Deposit Insurance Act § 221, 84 Stat. 1122. The statutory language addressing domestic transaction reporting makes no reference to foreign financial institutions or transfers of U.S. currency to (or from) foreign financial institutions and is explicitly directed at domestic financial institutions.

8. *Legal and Economic Impact of Foreign Banking Procedures on the United States*, pp. 1–2, 11

9. *Legal and Economic Impact of Foreign Banking Procedures on the United States*, pp. 11–12, 44.

10. According to Pollack, the "persons causing this distribution were prosecuted under the registration and antifraud provisions of the Federal securities laws." Interestingly, Pollack later argued that it had become more difficult to prosecute cases because the Fed withdrew (in May 1968) one of the implementing regulations (section 7(f) of regulation T) for this provision in the U.S. Code. *Legal and Economic Impact of Foreign Banking Procedures on the United States*, pp. 5, 18, 24.

11. *Legal and Economic Impact of Foreign Banking Procedures on the United States*, pp. 19, 21, 30–32.

12. *Legal and Economic Impact of Foreign Banking Procedures on the United States*, pp. 21–22, 45–46.

13. *Foreign Bank Secrecy and Bank Records: Hearings before the Committee on Banking and Currency*, 91st Cong. 7 (1970).

14. *Foreign Bank Secrecy and Bank Records*, pp. 8–9.

15. *Foreign Bank Secrecy and Bank Records*, pp. 9–10.

16. *Foreign Bank Secrecy and Bank Records*, p. 18.

17. See, for example, Douglas J. Workman, "The Use of Offshore Tax Havens for the Purpose of Criminally Evading Income Taxes," *Journal of Criminal Law and Criminology* 73, no. 2 (Summer 1982): 675–706.

18. *Foreign Bank Secrecy and Bank Records*, pp. 46, 71.

19. The report specifically mentions Rep. William Widnall (R-NJ) and Rep. Richard Hanna (D-CA) as members opposing the domestic transaction reporting requirements (Hanna because they would violate customers' privacy). Criminal Division, "Investigation and Prosecution of Illegal Money Laundering: Narcotic and Dangerous Drug Section Monograph, A Guide to the Bank Secrecy Act," Department of Justice, October 1983, pp. 11–15.

20. An Act to Amend the Federal Deposit Insurance Act § 101, 84 Stat. 1114–15.

21. An Act to Amend the Federal Deposit Insurance Act § 231, 84 Stat 1122. The threshold for foreign transaction reporting was raised to $10,000 in 1984. Pub. L. 98-473 § 901, 98 Stat. 2135 (1984).

22. An Act to Amend the Federal Deposit Insurance Act § 221, 84 Stat. 1122.

23. See Department of the Treasury, Financial Recordkeeping and Reporting of Currency and Foreign Transactions § 103.22, 37 Fed. Reg. 66, 6913 (April 5, 1972).

24. Anti-Drug Abuse Act of 1986, 18 U.S.C. § 1956 (1986). The Money Laundering Control Act was subtitle H of the Anti-Drug Abuse Act of 1986, and it was an explicit component of the federal war on drugs and organized crime. See Michael Levi and Peter Reuter, "Money Laundering," in *Crime and Justice: A Review of Research*, ed. by M. Tony, vol. 34 (Chicago: University of Chicago Press, 2006), p. 296.

25. 31 U.S.C. § 5324.

26. 12 U.S.C. § 1818(s). Section 1366 of the Money Laundering Control Act also included civil and criminal asset forfeiture provisions.

27. The act was Title XV of the Housing and Community Development Act of 1992, Pub. L. 102-389, 106 Stat. 1571 (1992).

28. 12 U.S.C. § 1821(c)(5)(M); and 12 U.S.C. § 93(d).

29. 12 U.S.C. § 1821(e)(2).

30. 18 U.S.C. § 1960.

31. 31 U.S.C. § 5318(g)(1) (emphasis added).

32. FinCEN, "Suspicious Transactions Reporting Requirements," Department of the Treasury, 61 Fed. Reg. 4329 (February 5, 1996).

33. 31 U.S.C. § 5318(g)(4). The act was Title IV of the Riegle

Community Development and Regulatory Improvement Act of 1994, Pub. L. 103-325, 108 Stat. 2160 (1994).

34. FinCEN, "Suspicious Transactions Reporting Requirements," p. 4326.

35. FinCEN, "Suspicious Transactions Reporting Requirements," pp. 4331–2. The statutory requirement for SARs is encoded at 31 U.S.C. § 5318(g).

36. Title III was named the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.

37. 31 U.S.C. § 5318A.

38. 31 U.S.C. § 5318(i).

39. 31 U.S.C. § 5318(j).

40. 18 U.S.C. § 981(k).

41. 31 U.S.C. § 5318 note.

42. 31 U.S.C. § 5332 note.

43. 31 U.S.C.§ 5318(l)(1).

44. 31 U.S.C. § 5318(l)(2).

45. "Bank Secrecy Act/Anti–Money Laundering Examination Manual," Federal Financial Institutions Examination Council, July 28, 2006, pp. 42, 51.

46. The act was Division F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat 3388 (2021).

47. Section 6107 of the Anti–Money Laundering Act of 2020 establishes a chief domestic liaison that is required to appoint at least six domestic liaisons to perform outreach to Bank Secrecy Act (BSA) officers at financial institutions. Section 6303 establishes BSA information security officers (within each functional federal regulator, FinCEN, and the IRS) to be "consulted with" on several regulatory matters. Section 6208 establishes BSA innovation officers to provide outreach to law enforcement and government agencies and to provide technical assistance to financial institutions. Section 6211(b) requires the Treasury Department secretary to "periodically convene a global anti–money laundering and financial crime symposium."

48. See, for example, 31 U.S.C. § 5312(a).

49. 31 U.S.C. § 5336(a); and 31 U.S.C. § 5336(b).

50. The provisions are also controversial because much of the information is already being reported to the IRS. For more on the controversy surrounding beneficial ownership requirements, see David R. Burton, "Re: Beneficial Ownership Information Reporting Requirements," Comment Letter, Docket Number FinCEN 2021-0005 [RIN 1506-AB49], February 7, 2022; Norbert J. Michel, "Senators Trying to Add Beneficial Ownership Requirements to Latest National Defense Authorization Act," *Forbes*, July 1, 2020; David R. Burton, "The Corporate Transparency Act and the ILLICIT CASH Act," Heritage Foundation Backgrounder no. 3449, November 7, 2019; and David R. Burton, "Beneficial Ownership Reporting Regime Targets Small Businesses and Religious Congregations," Heritage Foundation Backgrounder no. 3289, March 5, 2018. See also "The Anti–Money Laundering Act of 2020: Congress Enacts the Most Sweeping AML Legislation Since Passage of the USA PATRIOT Act," *National Law Review* XII, no. 158 (January 19, 2021).

51. In general, financial intelligence units (FIUs) are national agencies responsible for requesting, receiving, analyzing, and disseminating disclosures of financial information to the requisite government authorities. More than 100 FIUs make up the Egmont Group, an international entity focused on cooperation and sharing information among FIUs. According to FinCEN, "The Egmont Group is designed to improve communication, information sharing, and training coordination amongst its FIU members. Its goal is to provide a forum for member FIUs to improve support to their respective governments in the fight against money laundering, terrorist financing, and other financial crimes." See FinCEN, "The Egmont Group of Financial Intelligence Units," Department of the Treasury.

52. Separately, more than 90 countries participate in the multilateral Convention on Mutual Administrative Assistance in Tax Matters, and the United States has bilateral income tax treaties, protocols, and tax-information-exchange agreements with approximately 70 countries. Moreover, private entities are required to provide a wide variety of information to the IRS with respect to both domestic and foreign operations. See Norbert J. Michel and David Burton, "Financial Privacy in a Free Society," Heritage Foundation, September 23, 2016.

53. Internal Revenue Code §§ 1471–1474; "FATCA–Regulations and Other Guidance," IRS, updated July 6, 2021; 26 C.F.R. § 1.1441-1; and Internal Revenue Service Rev. Proc. 2014-39.

54. "Information Sharing Environment 2017 Annual Report to Congress," Office of the Director of National Intelligence, 2017; and Michel and Burton, "Financial Privacy in a Free Society."

55. Federal Bureau of Investigation, "FBI Information Sharing & Safeguarding Report 2012," Department of Justice, 2012; and International Criminal Police Organization, "INTERPOL Reviews Its Rules for the International Exchange of Criminal Data," March 22, 2019.

56. 31 U.S.C. § 5312(a)(2). The code also defines a financial institution as "any other business designated by the [Treasury] Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters." See 31 U.S.C. § 5312(a)(2)(z).

57. Michel and Burton, "Financial Privacy in a Free Society," tables 3, 4.

58. Aside from 31 U.S.C. § 5311 and what follows, Title X of the Dodd-Frank Act created the Consumer Financial Protection Bureau (CFPB) and gave the CFPB certain regulatory responsibilities for remittance transfers. The CFPB is imbued with unparalleled powers over virtually every consumer financial product and service, and it could easily create rules that extend the anti–money laundering (AML) regime under the pretense of protecting consumers. In fact, Section 1073 of the Dodd-Frank Act amended the Electronic Fund Transfer Act "to create a new comprehensive 'consumer protection regime' for remittance transfers sent by consumers in the United States to individuals and businesses in foreign countries." Electronic Fund Transfers (Regulation E), 12 C.F.R. pt. 1005 (October 28, 2013), pp. 3–4.

59. Broker-dealers must also comply with the Financial Industry Regulatory Authority Rule 3310, which sets forth minimum standards for a firm's written anti–money laundering compliance program.

60. 31 C.F.R. pt. 1010, subpart C; and Treasury Department, "Financial Recordkeeping and Reporting of Currency and Foreign Transactions," p. 6913.

61. 31 U.S.C. § 5313; 31 C.F.R. pt. 1010, subpart C; and Internal Revenue Code § 6050I.

62. The SAR thresholds for banks, casinos, and money-service businesses are found at 31 C.F.R. § 1020.320, 31 C.F.R. § 1021.320, and 31 C.F.R. § 1022.320, respectively.

63. Money-service businesses, including check cashers and providers of prepaid access cards, are defined at 31 C.F.R. 1010.100(ff).

64. The $3,000 money-service business requirement applies to all forms of payment. See FinCEN, "Bank Secrecy Act Requirements: A Quick Reference Guide for Money Services Businesses," Department of the Treasury. In early 2022, officials at the Homeland Security Investigations unit (a law enforcement division at the Department of Homeland Security) revealed to Senator Ron Wyden (R-OR) that its investigators (along with investigators at U.S. Immigration and Customs Enforcement) had collected records of any money transfer greater than $500 to or from Mexico, as well as "information on domestic or international transfers exceeding $500 to or from the states of Arizona, California, New Mexico and Texas." Michelle Hackman and Dustin Volz, "Secret Surveillance Program Collects Americans' Money-Transfer Data, Senator Says," *Wall Street Journal*, March 8, 2022.

65. 31 U.S.C. § 5318 authorizes the secretary of the Treasury Department to prescribe regulations that (among other things) require "a class of domestic financial institutions or nonfinancial trades or businesses to maintain appropriate procedures, including the collection and reporting of certain information" to comply with the Bank Secrecy Act. These regulations are at 12 C.F.R. § 208.63 (Procedures for Monitoring Bank Secrecy Act Compliance).

66. 12 C.F.R. § 208.63(c). For guidance, the Federal Financial Institutions Examination Council publishes a 344-page examination manual that outlines procedures and requirements for a Bank Secrecy Act/anti–money laundering compliance program. See "BSA/AML Examination Manual," Federal Financial Institutions Examination Council, February 27, 2015.

67. 12 C.F.R. § 208.63(b)(2). There is also a separate statutory requirement for the Anti–Money Laundering Program at 31 U.S.C. § 5318(h).

68. Federal regulators can also issue—and they have issued—geographic targeting orders within the United States, imposing *additional* reporting and recordkeeping requirements on "domestic financial institutions or nonfinancial trades or businesses in a geographic area." 31 U.S.C. § 5326(a); and 31 C.F.R. § 1010.370. Also see FinCEN, "FinCEN Targets Money Laundering Infrastructure with Geographic Targeting Order in Miami," news release, Department of the Treasury, April 21, 2015.

69. FinCEN, "FinCEN Announces $8 Million Civil Money Penalty against CommunityBank of Texas, National Association for Violations of the Bank Secrecy Act," news release, Department of the Treasury, December 16, 2021.

70. FinCEN, "Consent Order Imposing Civil Money Penalty," Department of the Treasury No. 2021-03, p. 4. This type of finding, where FinCEN holds a financial institution liable for failure to provide adequate resources to its compliance program, is comment. For example, FinCEN made a similar

finding against a broker-dealer for "fail[ing] to provide its [anti–money laundering] compliance office with the resources needed to ensure day-to-day compliance with the [Bank Secrecy Act]." FinCEN, "Assessment of Civil Monetary Penalty," Department of the Treasury No. 2018-03, p. 8.

71. FinCEN, "Consent Order Imposing Civil Money," p. 11.

72. See Levi and Reuter, "Money Laundering," p. 342.

73. Terence C. Halliday, Michael Levi, and Peter Reuter, "Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism," Center on Law and Globalization and the American Bar Foundation, January 30, 2014, p. 47. Also see J. C. Sharman, "Power and Discourse in Policy Diffusion: Anti–Money Laundering in Developing States," *International Studies Quarterly* 52, no. 3 (September 2008): 635–56. Sharman provides additional studies and discusses (among other issues) why so many countries now have virtually the same anti–money laundering regulatory framework despite so little evidence of policy effectiveness.

74. Norbert Michel, "Treasury and Congress Set to Pass Off New Regulatory Burden on Small Businesses," *Forbes*, January 27, 2020.

75. Mariano-Florentino Cuellar, "The Tenuous Relationship between the Fight against Money Laundering and the Disruption of Criminal Finance," *Journal of Criminal Law and Criminology* 93, no. 2 (2003): 312–466.

76. Tom Naylor, *Wages of Crime* (Ithaca, NY: Cornell University Press, 2002); and Peter Alldridge, *Money Laundering Law: Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime* (Portland, OR: Hart Publishing Co., 2003). As Alldridge discusses on page 25, it is unclear that criminal law theory justifies the criminalization of money laundering itself. For instance, criminal liability is morally justified based on harm (and fault) and the extent to which the act of money laundering itself is harmful is separate from the predicate criminal offense that might produce illegally obtained profits.

77. Jennifer Shasky Calvery, director of FinCEN, speech at the FSSCC–FBIIC Joint Meeting, New York, December 9, 2015, p. 2, (emphasis added).

78. Diego Zuluaga, "FinCEN's Suspicious Statistics," *Alt-M.org*, May 22, 2020. Zuluaga also points out that, according to FinCEN's database, virtual currency suspicious activity reports made up approximately 0.5 percent of all suspicious activity reports filed between 2014 and 2019.

79. FinCEN, "The SAR Activity Review: Trends, Tips & Issues—Issue 8," Department of the Treasury, April 2005, p. 9.

80. Charlie Steele, a former deputy director of FinCEN, observed, "I think its [sic] fair to say they err on the side of caution, when in doubt they file a [suspicious activity report] rather than deal with an aggressive enforcement action a few years down the line. . . . There's no question in my opinion that there's lots of defensive filing going on. So you end up with lots and lots of [suspicious activity reports] that in many ways the banks fear may never be looked at and they spending all this money on compliance." Carl Brown, "Not Enough Needles and Too Much Hay: The Problem with Suspicious Activity Reports," GRC World Forums, February 2, 2021.

81. The Securities and Exchange Commission's authority to bring enforcement actions for violations relating to a broker-dealer's anti–money laundering compliance program is on shaky ground. See Robert Loeb et al., "SEC v. Alpine Securities Corp.: The SEC's Authority to Enforce the Bank Secrecy Act Is Challenged," *Securities Litigation, Investigations and Enforcement* (blog), Orrick, July 10, 2018; and Russell Ryan et al., "*Alpine Securities v. SEC*," Legal Briefs, Cato Institute, August 20, 2021.

82. "Global Enforcement of Anti–Money Laundering Regulation: Shift in Focus," Kroll, 2022; Division of Examinations, *2021 Examination Priorities: Division of Examination* (Washington: Securities and Exchange Commission, 2021); and "2022 Report on FINRA's Examination and Risk Monitoring Program," Financial Industry Regulatory Authority Inc., February 2022.

83. Elizabeth A. Duke, "The Future of Community Banking," speech, Southeastern Bank Management and Directors Conference, Terry College of Business, University of Georgia, Duluth, Georgia, February 5, 2013; and Marshall Lux and Robert Greene, "The State and Fate of Community Banking," Harvard Kennedy School Mossavar-Rahmani Center for Business and Government Working Paper no. 37, 2015.

84. The sources for these estimates include FBI, IRS, and U.S. Sentencing Commission data, as well as FinCEN, Office of Management and Budget, and Bureau of Labor Statistics data. See Michel and Burton, "Financial Privacy in a Free Society," Appendix, pp. 18–22. (For additional details on how the estimates are derived, see pp. 10-13.) Separately, a 2018 St. Louis Federal Reserve survey reported 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), and FinCEN's own impact assessment of the 2016 customer due diligence rule included an upper bound compliance costs of $1.5 billion over 10 years. See Diego Zuluaga, "A War on Crime or on Business?," *Alt-M.org*, March 21, 2019.

85. Using IRS data, the $7 million per conviction cost is calculated as $4,813 million divided by 691 convictions and serves as a lower bound on the estimate. See Michel and Burton, "Financial Privacy in a Free Society," p. 13.

86. This range is calculated based on a total cost of $4,813–$8,013 million divided by 45 convictions. See Michel and Burton, "Financial Privacy in a Free Society," pp. 12–13.

87. The same Government Accountability Office report notes that "regulators have not fully assessed the [Bank Secrecy Act/anti–money laundering] factors influencing banks to derisk." See Gene L. Dodaro, "Priority Open Recommendations: Federal Deposit Insurance Corporation," letter from comptroller general of the United States to the Honorable Jelena McWilliams (chairman of the Federal Deposit Insurance Corp.), April 20, 2020; and Government Accountability Office, "Bank Secrecy Act: Derisking along the Southwest Border Highlights Need for Regulators to Enhance Retrospective Reviews," GAO-18-263, February 26, 2018.

88. See, for example, Masha Gessen, "Banking while Russian," *New York Times*, February 11, 2014; and Manuel Orozco, Laura Porras, and Julia Yansura, "Bank Account Closures: Current Trends and Implications for Family Remittances," Inter-American Dialogue, December 2015, p. 2.

89. For instance, when asked why they do not have a bank account, 36 percent of respondents cited "avoiding a bank gives more privacy," and 21 percent cited "personal identification, credit, or former bank account problems." See Federal Deposit Insurance Corp. (FDIC), *How America Banks: Household Use of Banking and Financial Services: 2019 FDIC Survey* (Arlington, VA: FDIC, October 2020), p. 17.

90. Congress has certainly been aware of this critique. In 1990, for example, law enforcement officials testified "how easy it was to launder money using large scale businesses including carpet stores and real estate firms." Associated Press, "It's Simple to Launder Money, Agents Report," *New York Times*, September 21, 1990.

91. Jim O'Grady and Kenny Malone, "A SWIFT Getaway," NPR, February 9, 2022.

92. Krishna N. Das and Jonathan Spicer, "How the New York Fed Fumbled over the Bangladesh Bank Cyber-Heist," Reuters, July 21, 2016.

93. Similarly, willful ignorance would still be penalized in criminal cases. Aside from overt criminal and civil violations, financial institutions would not be permitted, under current law, to rely on willful ignorance as an excuse. In 2011, the U.S. Supreme Court affirmed the validity of the willful blindness doctrine in both civil and criminal settings in *Global-Tech Appliances Inc. v. SEB S.A*. See "Willful Blindness," National Association of Criminal Defense Lawyers, March 18, 2020.

94. Valentina Pasquali, "Enforcement Actions against Capital One Raise Timing, Oversight Questions," *ACAMS Moneylaundering.com*, January 20, 2021.

95. In *Griswold v. Connecticut*, 381 U.S. 479 (1965), the U.S. Supreme Court affirmed that a right to privacy can be inferred from several amendments in the Constitution's Bill of Rights, including the Ninth and Fourteenth Amendments.

96. See, for example, *Terry v. Ohio*, 392 U.S. 1, 21 (1968). "And, in justifying the particular intrusion, the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."

97. Nicholas Anthony, "Canada's Plow through Financial Freedom Stopped Convoy," *Orange County Register*, February 24, 2022; Nicholas Anthony, "How Canada Made the Case for Cryptocurrency, Not CBDCs," *Cato at Liberty* (blog), Cato Institute, March 2, 2022; and Walter Olson, "Canada: In a Blow to Liberty, Government Invokes Emergencies Act against Domestic Protests," *Cato at Liberty* (blog), Cato Institute, February 16, 2022.

98. Department of the Treasury, "General Explanations of the Administration's Fiscal Year 2022 Revenue Proposals," May 2021, p. 88.

99. Nicholas Anthony, "Why Don't Americans Have Stronger Financial Privacy Rights?," *Cato at Liberty* (blog), Cato Institute, October 28, 2021.

100. Both the House and Senate realized soon after the 1970 Bank Secrecy Act was enacted that the law was not being enforced the way Congress had intended, and political support for Congress to change the law built up over several years in the early 1970s. See Nancy M. Kirschner, "The Right to Financial Privacy Act of 1978-The Congressional Response to *United States v. Miller*: A Procedural Right to Challenge Government Access to Financial Records," *University of Michigan Journal of Law Reform* 13, no. 1 (1979); and Catherine C. Wakelyn, "Bank Recordkeeping and the Customer's Expectation of Confidentiality," *Catholic University Law Review* 26, no. 1 (Fall 1976).

101. *California Bankers Association v. Shultz*, 416 U.S. 21 (1974); and *United States v. Miller*, 425 U.S. 435 (1976).

102. This language refers to the Supreme Court's decision in

Miller, 425 U.S. 435. See Kirschner, "The Right to Financial Privacy Act of 1978," p. 17.

103. This discussion focuses on Fourth Amendment protections, but those constitutional protections are not the only ones at issue in considering questions of financial privacy. The Bank Secrecy Act also raises questions, among others, about the Fifth Amendment's right against self-incrimination and due process protections and the First Amendment's speech and association rights.

104. *California Bankers Association*, 416 U.S. at 52.

105. *California Bankers Association*, 416 U.S. at 52–53.

106. *California Bankers Association*, 416 U.S. at 60–63.

107. *California Bankers Association*, 416 U.S. at 66–68.

108. *Stark v. Connally*, 374 F. Supp. 1242, 1251 (N.D. Cal. 1972); and David F. Dybvig, "Searches and Seizures—Banks and Banking—Witnesses—Right to Privacy; California Bankers Association v. Schultz," *Akron Law Review* 8, no. 1 (1975): 182.

109. *California Bankers Association*, 416 U.S. at 78–79; and Dybvig, "Searches and Seizures."

110. *California Bankers Association*, 416 U.S. at 82.

111. *California Bankers Association*, 416 U.S. at 85–86 (citation omitted).

112. *California Bankers Association*, 416 U.S. at 86. For additional information on Fifth Amendment rights as they relate to business records, see Georganne R. Higgins, "Business Records and the Fifth Amendment Right against Self-Incrimination," *Ohio State Law Journal* 38, no. 2 (1977): 351–77.

113. *California Bankers Association*, 416 U.S. at 90. Douglas drew an analogy to recording telephone calls: "Suppose Congress passed a law requiring telephone companies to record and retain all telephone calls and make them available to any federal agency on request. Would we hesitate even a moment before striking it down? I think not."

114. *California Bankers Association*, 416 U.S. at 90 (citation omitted).

115. *California Bankers Association*, 416 U.S. at 93.

116. *California Bankers Association*, 416 U.S. at 93–95. Justice Thurgood Marshall continues: "Our Fourth Amendment jurisprudence should not be so wooden as to ignore the fact that through microfilming and other techniques of this electronic age, illegal searches and seizures can take place without the brute force of the general warrants which raised the ire of the Founding Fathers."

117. *California Bankers Association*, 416 U.S. at 98; and Dybvig, "Searches and Seizures." The majority had argued, on the other hand, that there was no violation of Fourth Amendment rights because the Bank Secrecy Act recordkeeping requirements, as well as the implementing regulations, did not demand that any information be disclosed to the government. See M. Elizabeth Smith, "The Public's Need for Disclosure v. the Individual's Right to Financial Privacy: An Introduction to the Financial Right to Privacy Act of 1978," *Administrative Law Review* 32, no. 3 (Summer 1980): 517.

118. *United States v. Miller*, 425 U.S. 435 (1976).

119. *Miller*, 425 U.S. at 443.

120. Justice Douglas had retired from the Supreme Court in 1975.

121. *Miller*, 425 U.S. at 449 (internal quotation marks and citation omitted).

122. *Miller*, 425 U.S. at 451 (internal quotation marks and citation omitted).

123. *Miller*, 425 U.S. at 456.

124. *Smith v. Maryland*, 442 U.S. 735 (1979).

125. The Right to Financial Privacy Act (RFPA) of 1978, Pub. L. 95–630, 92 Stat. 3697 (1978), 12 U.S.C. §§ 3401–3422. The act was Title XI of the Financial Institutions Regulatory and Interest Rate Institutions Control Act of 1978. The RFPA established specific procedures that federal authorities must follow to obtain information from these records, such as obtaining a subpoena, notifying the customer, and providing the customer with the opportunity to object. The RFPA does, however, include multiple exceptions (12 U.S.C. § 3413), including any disclosures related to the Internal Revenue Code.

126. *United States v. Jones*, 565 U.S. 400, 417 (2012). See Anthony, "Why Don't Americans Have Stronger Financial Privacy Rights?"

127. *United States v. Jones*, 565 U.S. 400, 417 (2012).

128. *Carpenter v. United States*, 138 S. Ct. 2206, 2268 (2018).

129. *Carpenter*, 138 S. Ct. at 2270.

130. For an in-depth analysis of the Fourth Amendment

issues that the Bank Secrecy Act raises, especially those that are more relevant since the advent of cryptocurrency, see Jeremy Ciarabellini, "Cryptocurrencies' Revolt against the BSA: Why the Supreme Court Should Hold That the Bank Secrecy Act Violates the Fourth Amendment," *Seattle Journal of Technology, Environmental & Innovation Law* 10, no. 1 (May 6, 2020); and Paul Belonick, "Transparency Is the New Privacy: Blockchain's Challenge for the Fourth Amendment," *Stanford Technology Law Review* 23, no. 1 (Winter 2020): 114–81.

131. For instance, individual business owners may want to remain anonymous to avoid political backlash because their industry is frequently protested, to avoid negative financial consequences due to racism, or to become financially self-sufficient without fear of being harassed by someone who previously perpetuated violent behavior. See William J. Moon, "Anonymous Companies," *Duke Law Journal*, forthcoming, last revised June 1, 2022.

132. Other sections that refer to these provisions may also require revision in light of these suggested changes.

133. Congress should also either repeal or amend 26 U.S.C. § 6050I (Section 6050I of the Internal Revenue Code), subsections (a)(2), (d)(2), and (g)(1)), by striking "$10,000" each place the term appears and inserting "$50,000 (adjusted for inflation with the consumer price index each fiscal year hereafter X, 20XX.")

CITATION

Michel, Norbert J., and Jennifer J. Schulp. "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis no. 932, Cato Institute, Washington, DC, July 26, 2022.