# 21-1250

In the

# United States Court of Appeals
# for the Second Circuit

SOKHNA GUEYE,

*Plaintiff–Appellant*,

v.

PEOPLE'S UNITED BANK, NATIONAL ASSOCIATION,

*Defendant–Appellee*,

v.

PATRICIA HOFFMAN,

*Defendant*.

ON APPEAL FROM THE UNITED STATES
DISTRICT COURT FOR THE EASTERN DISTRICT OF NEW YORK

**BRIEF OF THE BANK POLICY INSTITUTE AND THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AS *AMICI CURIAE* SUPPORTING DEFENDANT–APPELLEE AND AFFIRMANCE OF THE DISTRICT COURT**


Tara S. Morrissey
U.S. CHAMBER LITIGATION CENTER
1615 H Street, N.W.
Washington, DC 20062
(202) 463-5337
*Counsel for the Chamber of Commerce of the United States of America*

Sharon Cohen Levin
SULLIVAN & CROMWELL LLP
125 Broad Street
New York, NY 10004
(212) 558-4000

Jennifer L. Sutton
Jordan M.H. Wish
Leslie B. Arffa
SULLIVAN & CROMWELL LLP
1700 New York Avenue, N.W.
Washington, DC 20006
(202) 956-7500

*Counsel for Amici Curiae*

## CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, the Bank Policy Institute ("BPI") and the Chamber of Commerce of the United States of America ("Chamber" and, together with BPI, "*Amici*") state as follows:

BPI is not a subsidiary of any other corporation. BPI is a nonprofit trade group that has no shares or securities that are publicly traded.

The Chamber is not a subsidiary of any other corporation. The Chamber is a nonprofit trade group and has no shares or securities that are publicly traded.[1]

---

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), *Amici* state as follows: (1) neither party's counsel authored the brief in whole or in part; (2) neither party nor its counsel contributed money that was intended to fund preparing or submitting the brief; and (3) no person other than *Amici*, their members, or their counsel contributed money that was intended to fund preparing or submitting the brief.

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Rules, and Regulations**

**Other Authorities**

## STATEMENT OF INTEREST

***BPI.*** BPI is a nonpartisan policy, research, and advocacy group that represents the nation's leading banks and their customers. BPI's member banks employ nearly two million Americans, make 68% of the nation's loans and nearly half of the nation's small business loans, and serve as an engine for financial innovation and economic growth.

***Chamber.*** The Chamber is the world's largest business federation. It represents approximately 300,000 direct members, and indirectly represents the interests of more than 3 million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files *amicus curiae* briefs in cases that raise issues of concern to the nation's business community.

*Amici* and their members are opposed to unlawful discrimination in all forms and are strong supporters of efforts to increase financial inclusion. To further these efforts, *Amici* and their members collaborate closely with community organizations and numerous other stakeholders.

*Amici* have an interest in this case because their financial institution members are subject to extensive regulation and supervision under the Bank Secrecy

Act ("BSA") and other anti-money laundering ("AML") requirements. *Amici* have significant knowledge of, and experience with, BSA/AML regulation, and can bring to the Court's attention context that may not otherwise be provided by the parties or the other *amicus*. Furthermore, a study published by BPI regarding Suspicious Activity Reports ("SARs") has been referenced in this litigation. *See Amicus Curiae* Brief in Support of Plaintiff-Appellant, *Gueye* v. *People's United Bank, N.A*., No. 21-1250, Dkt. No. 68, 16 (2d Cir. Aug. 30, 2021) ("Appellant *Amicus* Brief").

## SUMMARY OF ARGUMENT

*Amici* and their members are committed to promoting economic inclusion, including by refraining from all unlawful discrimination, and combatting money laundering. This case concerns the interplay between financial institutions' efforts to further these two goals. This brief focuses on the second, seeking to illuminate the evolving and incredibly complex legal regime that governs what institutions must do to detect and deter money laundering.

"With few exceptions, criminals are motivated by one thing—profit." FinCEN, *What is Money Laundering?* (Nov. 1, 2021), http://www.fincen.gov/what-money-laundering. And criminals generally seek to place their ill-gotten gains, however acquired, into legal financial systems and institutions. Money laundering—making illegitimate funds appear legitimate and using financial systems to fund illegal activity—is a global problem of enormous prevalence and consequence.

Concerned with the "heavy utilization of our domestic banking system by the minions of organized crime," Congress enacted the Bank Secrecy Act in 1970. *Cal. Bankers Ass'n* v. *Shultz*, 416 U.S. 21, 30 (1974) (citing Pub. L. No. 91-508, 84 Stat. 114). Today, under the BSA and other AML requirements, financial institutions must monitor, record, and report their customers' activities through extensive BSA/AML compliance programs that seek to identify and discourage money laundering.

An adequate compliance program must include appropriate measures to mitigate money laundering-related risk in a manner tailored to an institution's operations. Such activities include, among other things, gathering detailed information about customers and their transactions. At the outset of a relationship, an institution must verify a customer's identity and understand the nature and purpose of the relationship. Ongoing monitoring is then required to detect potential suspicious activity and, when detected, to report that activity to government authorities in the form of SARs. This monitoring also enables institutions to assess the money laundering-related risks a given customer poses to an institution and, if it deems those risks unsustainably high, to close the customer's account. Financial institutions that make the wrong decision about whether to file SARs or close accounts may face immense civil and criminal penalties and severe reputational damages.

The *Amicus* brief filed in support of Plaintiff-Appellant cites data BPI originally published in 2018 to argue that institutions can use BSA compliance programs to engage in discriminatory practices. Appellant *Amicus* Brief at 16. BPI's findings, however, in no way support the tying of financial institutions' extensive BSA compliance efforts to unlawful discrimination. These institutions operate extensive programs to facilitate compliance with anti-discrimination and other consumer protection requirements. Such programs operate alongside, and complement, BSA/AML programs. To the extent Plaintiff or its *Amicus* takes issue with the requirements of the BSA, its arguments are better aimed at Congress than at this Court. And indeed, *Amici* and their members support efforts to reform the BSA and the AML regulatory regime.

## ARGUMENT

### I. The BSA Furthers Efforts to Detect and Deter Illicit Use of the U.S. Financial System and U.S. Financial Institutions.

"Money laundering is the criminal's way of trying to ensure that, in the end, crime pays." John McDowell & Greg Novis, *The Consequences of Money Laundering and Financial Crime*, ECON. PERSPECTIVES (May 2001) at 6. Under federal law, money laundering includes conducting transactions to conceal the criminal source of the proceeds to make ill-gotten gains appear legitimate (*i.e.*, making "dirty" money "clean"), as well as conducting transactions to fund illegal activity. 18 U.S.C. §§ 1956-1957. Money laundering is extensive and global. The

United Nations estimates that between $800 billion and $2 trillion is laundered every year, U.N., Office on Drugs and Crime, *Money Laundering* (2021), http://www.unodc.org/unodc/en/money-laundering/overview.html, and Congress has described money laundering as "the financial fuel that permits transnational criminal enterprises to conduct and expand their operations." 31 U.S.C. § 5311 note.

Money launderers "subvert legitimate financial mechanisms and banking relationships by using them as protective covering for the movement of criminal proceeds and the financing of crime and terrorism." *Id.* The BSA and various other AML requirements promote detection and deterrence of this use of financial institutions by imposing a comprehensive regulatory regime on financial institutions that is vigorously enforced by the applicable regulators and the Department of Justice.

Congress passed the BSA in 1970 as the "Currency and Foreign Transactions Reporting Act," recognizing the "increasing use of banks and other institutions as financial intermediaries by persons engaged in criminal activity." *Ratzlaf* v. *United States*, 510 U.S. 135, 138 (1994) (citing Pub. L. No. 91-508, Tit. II, 84 Stat. 1118). As initially implemented, the BSA and related regulations required banks to maintain records of certain transactions and to report to the Treasury Department various cash transactions. *See Cal. Bankers Ass'n*, 416 U.S. at 30–41.

Over the past half-century, Congress has repeatedly amended and expanded the BSA. Regulators, including the Financial Crimes Enforcement Network ("FinCEN"), a Treasury bureau established in 1990 to focus on combating money laundering, have also expanded AML-related obligations. Examples of these amplified obligations include the following:

1. Banks and a wide swath of "financial institutions" must establish programs "reasonably designed to assure and monitor" their compliance with the BSA. *See* 12 U.S.C. § 1818(s); 31 U.S.C. § 5318(h). Banks became subject to BSA/AML program requirements beginning in 1987, *see* Procedures for Monitoring Bank Secrecy Act Compliance, 52 Fed. Reg. 2858 (Jan. 27, 1987); broker-dealers, casinos, and certain other institutions beginning in 2002, *see* Anti-Money Laundering Programs for Financial Institutions, 67 Fed. Reg. 21,110 (Apr. 29, 2002); and, earlier this year, FinCEN sought comment on whether, following related congressional amendments, antiquities dealers should have to maintain BSA/AML compliance programs as well, *see* Anti-Money Laundering Regulations for Dealers in Antiquities, 86 Fed. Reg. 53,021 (Sept. 24, 2021).

2. Certain financial institutions are required to file reports on transactions they identify as "suspicious." *See* 31 U.S.C. § 5318(g). Some banks were required by regulation to file "criminal referrals" as early as the 1970s and 1980s, *see, e.g.*, Interpretive Rulings, 36 Fed. Reg. 17,000 (Aug. 26, 1971); Reports

of Suspected Crimes, 50 Fed. Reg. 34,857 (Aug. 28, 1985), a process that was standardized by the creation of the "Suspicious Activity Report" in 1996, Amendment to the Bank Secrecy Act Regulations; Requirement to Report Suspicious Transactions, 61 Fed. Reg. 4326 (Feb. 5, 1996). SAR filing obligations have been extended to other institutions as well, for example, to broker-dealers in 2002. Amendment to the Bank Secrecy Act Regulations—Requirement that Brokers or Dealers in Securities Report Suspicious Transactions, 67 Fed. Reg. 44,048 (July 1, 2002).

3. Banks and certain other financial institutions are required to verify the identities of their customers, *see* 31 U.S.C. § 5318(*l*), and to conduct due diligence on them in order to both understand the nature and purpose of customer relationships and monitor transactions on an ongoing basis, *e.g.*, 31 C.F.R. § 1020.210(a)(2)(v). Congress enacted requirements regarding verification of customer identities in 2001, which became effective for relevant financial institutions in 2003. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 326, 115 Stat. 272, 317 (codified at 31 U.S.C. § 5318(*l*)); *see also*, *e.g.*, Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090 (May 9, 2003). FinCEN also historically recognized, both in guidance and enforcement actions, that comprehensive due diligence on financial institution customers is a necessary

component of a strong BSA/AML compliance program. Customer Due Diligence Requirements for Financial Institutions, 77 Fed. Reg. 13,046 (Mar. 5, 2012). FinCEN clarified and codified its expectations in a formal customer due diligence rule, which became effective in 2018. Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29,398 (May 11, 2016).

4. Earlier this year, Congress amended the BSA to describe the multiple purposes the statute now serves: *reporting and recordkeeping* of information "highly useful" for criminal, tax, or regulatory investigations or risk assessments, or intelligence or counterintelligence activities; *preventing money laundering* through the establishment of risk-based BSA/AML programs; facilitating the *tracking of illicit funds*; *assessing illicit finance risks to financial institutions* to protect the U.S. financial system from abuse; and establishing frameworks for *information sharing* among financial institutions, regulators, the Treasury Department, and law enforcement to identify, stop, and apprehend criminals. Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, § 6101, 134 Stat. 3449 (codified at 31 U.S.C. § 5311).

## II. Financial Institutions Must Implement and Maintain Tailored, "Risk Based" BSA/AML Compliance Programs.

Banks and other financial institutions must implement BSA/AML compliance programs that address a constellation of statutory and regulatory requirements and expectations. The various requirements addressed, the multiple purposes served, and the complexity of modern financial systems make BSA/AML programs intricate, multifaceted, and expensive. A BPI survey of 17 member institutions found that, as of 2017, they were collectively employing over 14,000 individuals and deploying up to 20 information technology systems to assist in BSA/AML compliance; 14 of these institutions together were investing approximately $2.4 billion on these efforts. BPI, *Getting to Effectiveness: Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance* 2 (Oct. 29, 2018), http://bpi.com/getting-to-effectiveness-report-on-us-financial-institution-resources-devoted-to-bsa-aml-sanctions-compliance. The following sections describe in greater detail how institutions implement BSA/AML programs, the customer monitoring they are required to undertake, and the substantial civil and criminal penalties they may face if their programs are deemed inadequate.

### A. A BSA/AML Compliance Program Must Be Tailored to an Institution's Unique Risks.

"[A]t a minimum," a BSA/AML compliance program rests on four pillars: (1) a system of internal policies, procedures, and controls; (2) a designated "BSA officer"; (3) ongoing employee training; and (4) independent testing. 31 U.S.C. § 5318(h); *see also* 12 C.F.R. §§ 21.21(d), 208.63(c), 211.5(m), 211.24(j), 326.8(c), 748.2(c). Additionally, in 2018, FinCEN codified longstanding expectations that certain institutions, including banks, implement a fifth pillar—

procedures to conduct ongoing due diligence on their customers. *E.g.*, 31 C.F.R. § 1020.210.

Crucially, each BSA/AML program must be "*reasonably* designed to assure and monitor compliance" with regulatory requirements and "*risk-based*," meaning that "attention and resources . . . should be directed toward higher-risk customers and activities, consistent with the risk profile of a financial institution." 31 U.S.C. § 5318(h)(2)(B)(iv) (emphasis added). In other words, when implementing a "risk-based" compliance program, an institution must identify and manage the money laundering-related risks applicable to *that specific institution*. *See, e.g.*, FinCEN, *Bank Secrecy Act Effectiveness and Efficiency Fact Sheet* (June 2007), http://www.fincen.gov/sites/default/files/shared/bsa_factsheet.pdf. Because each program is specific to an institution, institutions have substantial discretion to craft an appropriate program. *See* Federal Financial Institutions Examination Council, *BSA/AML Examination Manual* ("FFIEC Examination Manual"), *BSA/AML Compliance Program Structures* (2015), https://bsaaml.ffiec.gov/docs/manual/08_ProgramStructures/01.pdf.

To construct an appropriately tailored program, a financial institution generally undertakes a comprehensive risk assessment of its activities. Such an assessment considers the money laundering- and other illicit finance-related risks associated with the institution's products, services, customers, and geographies. *See*

FinCEN & Federal Banking Agencies, *Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision* 2 (July 22, 2019) ("Joint Statement"), http://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-81a.pdf.[2] This risk assessment allows the institution to determine the risks that it believes it can adequately mitigate—and therefore is willing to assume—and those it cannot.

Adequate management and mitigation of money laundering-related risks require extensive controls, policies, and procedures. For example, if a particular type of account poses a higher risk, an institution may determine further steps are necessary. Such action could include, among other things, requiring additional documentation to confirm the activities of certain customers or undertaking more detailed monitoring of those customers' transactions. *See* Financial Action Task Force, *The Banking Sector: Guidance For a Risk Based Approach* 19-22 (Oct. 2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf. Risk assessments generally must be updated as an institution's activities and customers, along with the related risks,

---

[2] We refer to the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency ("OCC") collectively as the "federal banking agencies."

change. FFIEC Examination Manual, *BSA/AML Risk Assessment* (2020), https://bsaaml.ffiec.gov/docs/manual/03_BSAAMLRiskAssessment/01.pdf.

FinCEN and other authorities provide extensive guidance to institutions to inform their assessments of relevant money laundering- and other illicit finance-related risks. Some of this guidance is highly relevant to this litigation.

For example, although FinCEN and the federal banking agencies recognize that charities play important roles in supporting communities, these agencies have historically identified charities, particularly those operating abroad, as presenting heightened money laundering, fraud, and terrorist financing risks. *See* FFIEC Examination Manual, *Nongovernmental Organizations and Charities* (2014), https://bsaaml.ffiec.gov/docs/manual/09_RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/27.pdf; *see also* FinCEN & Federal Banking Agencies, *Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations* (Nov. 19, 2020), http://www.occ.gov/news-issuances/news-releases/2020/nr-ia-2020-155a.pdf. "Terrorist supporters," the U.S. government has warned, may "abuse charitable organizations abroad as a cover to raise and move funds, personnel, military supplies, and other resources." U.S. Dep't of Treasury, *National Terrorist Financing Risk Assessment* 24 (2018), https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf. For charity customers identified as higher risk, institutions are therefore advised to impose mitigating controls, which may include more stringent verification, documentation, and monitoring requirements (each of which is discussed in more detail below). FFIEC Examination Manual, *Nongovernmental Organizations and Charities*, *supra*, p. 12.

In addition, authorities have advised that specific geographic areas, including certain areas at issue in this case, present higher money laundering-related risks. In 2016, for example, the State Department described Senegal as "vulnerable to money laundering," due to, among other things, "criminal activity by foreigners," "limited law enforcement capacity," and "inadequate enforcement of relevant laws." U.S. Dep't of State, Bureau for Int'l Narcotics & Law Enforcement Affairs, *Money Laundering and Financial Crimes Country Database* 389 (June 2016), http://2009-2017.state.gov/documents/organization/253983.pdf. As early as 2013, the Financial Action Task Force ("FATF"), an international organization of which the United States is a member, noted risks related to terrorism financing in West African countries, including Senegal. FATF, *Terrorist Financing in West Africa* (Oct. 2013), http://www.fatf-gafi.org/media/fatf/documents/reports/TF-in-West-Africa.pdf. In 2018, a regional AML organization identified deficiencies in Senegal's AML regime and explained that Senegal is "vulnerable" to money laundering risk because of, among other factors, the prevalence of cash transactions and poor supervision of nonprofit organizations. Inter-Governmental Action Group against

Money Laundering, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Senegal, Mutual Evaluation Report* 1 (May 2018), https://www.giaba.org/media/f/1099_ENG%20-%20Final%20MER%20Senegal%20May%202019%20Rev82219.pdf. This year, FATF identified Senegal as having "strategic deficiencies" in its AML regime. *See* FinCEN, FIN-2021-A003, *Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies*, FIN-2021-A003 (Mar. 11, 2021).

When a country does not have a strong AML regime, transactions involving that country pose a higher risk. If the risks associated with those transactions are not adequately managed, an institution could unwittingly facilitate the processing of illicit funds.

This is not to suggest that institutions should, or even could, refuse to accept any charity or person with ties to Senegal as a customer. Instead, this discussion illustrates the sorts of factors an institution must take into account in assessing risks, including in determining where customers or transactions pose risks and in developing means to appropriately "manage customer relationships and mitigate risks." Joint Statement at 2.

### B. BSA/AML Compliance Requires Active Monitoring by Institutions of their Customers.

In addition to assessing the general risks of their activities, financial institutions must analyze the specific risks posed by each customer. They must do so both when accepting a new customer and on an ongoing basis.

#### 1. New Customers: Verification and Due Diligence

When a customer opens an account, a financial institution needs to ensure that it knows who the customer is. Or, as FinCEN has put it, an institution must have procedures that enable it "to form a reasonable belief that it knows the true identity of each customer." *E.g.*, 31 C.F.R. § 1020.220(a)(2). As with other elements of a BSA/AML compliance program, such verification procedures must be tailored to the institution's assessment of applicable risks; however, an institution must at a "minimum" verify a customer's personal information and determine whether the customer appears on any government-issued list of known or suspected terrorists. *Id.*

In addition to confirming a customer's identity, many institutions, including banks, must undertake sufficient due diligence to understand "the nature and purpose of [the] customer relationship." *E.g.*, *id.* § 1020.210(a)(2)(v)(A). Information gathered as part of due diligence is then used to develop a "customer risk profile." *Id.*

Consistent with the "risk-based" approach demanded by the BSA, the scope of due diligence when a customer relationship is formed, including the documentation that a customer will be required to provide, beyond specified minimums, depends on an assessment of the risk that will be posed by the relationship. And much like the illicit finance risks presented to an institution more generally, a particular customer's money laundering-related risk will depend on a number of factors. These include the products and services to be used, the nature of the customer's business or other activities, and the geographic locations where the customer does business. FFIEC Examination Manual, *Customer Due Diligence* (2018), http://bsaaml.ffiec.gov/docs/manual/06_AssessingComplianceWithBSA RegulatoryRequirements/02.pdf. For a customer determined to be lower risk, the nature and purpose of the relationship and the associated customer risk profile may be largely "self-evident." *Id.* For a customer determined to present a higher risk, more detailed information may be necessary to assess the nature and purpose of the relationship and to develop a risk profile. To take one example, if a charity is identified as higher risk, it may be necessary, as part of initial due diligence, to evaluate that charity's principals and donors and to obtain additional information about its finances, funding, and expenditures. *See* FFIEC Examination Manual, *Nongovernmental Organizations and Charities*, *supra*, p. 12.

### 2. Existing Customers: Ongoing Monitoring

Financial institutions must conduct ongoing monitoring of customers, to satisfy their SAR filing and BSA/AML program obligations. 31 C.F.R. §§ 1020.210(a)(2)(v)(B), 1020.320(a)(2)(iii). Much like an institution's risk profile, a customer's risk profile can evolve over time, and even a lower risk customer may engage in higher risk activity or use a financial institution for an illegitimate purpose. The ongoing monitoring and suspicious activity reporting obligations work hand-in-hand to help an institution identify those higher risk activities and potentially illicit uses. This monitoring represents a core BSA/AML compliance activity, and occupies a substantial part of the time, resources, and expenses associated with BSA/AML programs.

<u>Description of Ongoing Monitoring Processes</u>. Monitoring is undertaken using a variety of mechanisms. Smaller, less complex institutions may rely more on certain manual processes. These include reports of transactions that could raise money laundering-related concerns, such as those involving large amounts of cash or transfers to certain foreign jurisdictions. Larger, more complex institutions may rely to a greater extent on automated monitoring, potentially through the use of advanced technologies like artificial intelligence, to recognize transaction patterns that raise concerns. FFIEC Examination Manual, *Suspicious Activity Reporting* (2014), https://bsaaml.ffiec.gov/docs/manual/06_Assessing

ComplianceWithBSARegulatoryRequirements/04.pdf. Yet again, an institution's monitoring activities must be tailored to its assessment of relevant money laundering- or other illicit finance-related risks. For higher-risk customers, more frequent and more detailed reviews of transactional activity may be appropriate. *See, e.g.*, 81 Fed. Reg. at 29,399. Closer scrutiny is also generally undertaken with respect to products that present a higher risk of being used to facilitate money laundering.

Regulators expect that an individual transaction will be subject to more searching review if it raises a "red flag." Red flags are frequently identified by FinCEN and other governmental authorities to aid institutions in detecting transaction patterns that present heightened money laundering-related concerns. *See, e.g.*, FinCEN, FIN-2021-A004, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* (Nov. 8, 2021). A red flag is not conclusive evidence of money laundering, but red flag transactions are generally subject to additional, detailed investigation and evaluation, frequently by experienced personnel focused on financial crime matters.

Of relevance to this litigation, certain uses of ATMs may raise red flags. For example, FinCEN and the federal banking agencies have determined that anomalies in account behavior or a large amount of movement of funds into and out of an account (*i.e.*, "high velocity" transactions) should be considered red flags, as should a deposit of funds into an account in the United States, followed by a withdrawal of those funds shortly thereafter using an ATM in another country. *See* FFIEC Examination Manual, *Electronic Banking* (2015), https://bsaaml.ffiec.gov/docs/manual/09_RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/07.pdf. FinCEN, *SAR Bulletin: Automated Teller Machines* (June 1999), https://www.fincen.gov/sites/default/files/shared/sarbul1.pdf. As another example, due to heightened risks of terrorism financing in West Africa, FATF has identified red flags specific to transactions in that region including, among others, frequent international transfers to and from accounts of newly established entities, unexplained transfers, and frequent cash deposits into or withdrawals from charity accounts by individuals with no apparent relationship. FATF, *Terrorist Financing in West Africa*, *supra*, p. 13, at 34–35.

Suspicious Activity Reporting. A core purpose of transaction monitoring is to enable institutions to report suspicious transactions to government authorities through the filing of SARs with FinCEN. Regulators and law enforcement recognize that SARs and other BSA reports supply crucial information: they provide leads to law enforcement and other regulatory agencies; they help expand cases and put together pieces that authorities would not otherwise see; and they alert authorities to trends in illicit activity so activities can be deterred or their effects mitigated. Prepared Remarks of FinCEN Director Kenneth A. Blanco at the

11th Annual Las Vegas Anti-Money Laundering Conference and Expo (Aug. 14, 2018), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-11th-annual-las-vegas-1; *see also* U.S. Gov't Accountability Off. (GAO), GAO-20-574, *Anti-Money Laundering: Opportunities Exist to Increase Law Enforcement Use of Bank Secrecy Act Reports* 14–15 (2020).

SARs must be filed in a wide range of circumstances. Notably, the filing requirements apply not just when a financial institution knows of money laundering, but broadly to cover a situation where the institution "suspects" money laundering. Under regulations promulgated by FinCEN and the federal banking agencies, financial institutions generally must file SARs with respect to any transaction conducted or attempted by, at or through the institution that involves or aggregates to at least $5,000 in funds or other assets, where the institution knows, suspects, or has reason to suspect that the transaction (i) involves money laundering or other illegal activity; (ii) is designed to evade the BSA or its implementing regulations; or (iii) has no business or apparent lawful purpose or is not the type of transaction that the relevant customer would normally be expected to engage in, and the institution knows of no reasonable explanation for the transaction after examining the available facts. 31 C.F.R. § 1020.320(a); *see also* 12 C.F.R. §§ 21.11(c), 208.62(c), 211.5(k), 211.24(f), 353.3(a), 748.1(c). Some institutions are also required to file SARs in other circumstances, such as when a bank identifies certain criminal transactions involving its own officials. *E.g.*, 12 C.F.R. § 21.11(c)(1).

Under these broad filing requirements, institutions therefore must file SARs in many cases that do not involve obvious money laundering or other illegality. To the contrary, as FinCEN described when publishing the initial SAR form in 1996, SARs are intended to report the much wider universe of transactions that "legitimately can and should raise *suspicions* of *possible* illegality." 61 Fed. Reg. at 4329 (emphases added). These suspicions are developed through monitoring and investigation of customer transactions, including by comparing transactional activity to expected activity (*i.e.*, the nature and purpose of the customer relationship and customer risk profile generated through due diligence). *See* 81 Fed. Reg. at 29,398. Institutions are unlikely to have perfect information about a customer when determining whether to file a SAR, but an institution's processes of investigation and review will enable it to make as informed a decision as possible.

A key component of this far-reaching reporting regime is SAR confidentiality. Neither financial institutions nor governmental authorities may disclose SARs or information that would reveal the existence of a SAR to third parties. 31 U.S.C. § 5318(g)(2)(A). Both criminal and civil penalties may be imposed for violations. 31 U.S.C. §§ 5321, 5322; 31 C.F.R. §§ 1010.820, .840.

SAR confidentiality serves to protect financial institutions and their customers, while promoting law enforcement objectives. As to institutions, confidentiality facilitates the "creation of an environment that encourages financial institutions to report suspicious activity without fear of reprisal" from their customers or others. Confidentiality of Suspicious Activity Reports, 75 Fed. Reg. 75,593, 75,595 (Dec. 3, 2010). As to customers, confidentiality protects SARs from public disclosure that could "harm the privacy interests of innocent people whose names may be contained therein." *Cotton* v. *PrivateBank & Tr. Co.*, 235 F. Supp. 2d 809, 815 (N.D. Ill. 2002). Additionally, the "[r]elease of an[y] SAR could compromise an ongoing law enforcement investigation, tip off a criminal wishing to evade detection, or reveal the methods by which banks are able to detect suspicious activity." *Id.*

<u>Assessment of Money Laundering-Related Risks</u>. Beyond the filing of SARs and other reports, customer monitoring also enables institutions to update customer information and thereby determine the risk a customer's activity poses on an ongoing basis. 31 C.F.R. § 1020.210(b)(2)(v)(B). As described above, one purpose of BSA/AML risk assessments is to identify risks that an institution can effectively mitigate and will assume. If an institution determines that a customer poses a risk that the institution is unwilling or unable to manage, it may terminate its relationship with that customer. FinCEN & Federal Banking Agencies, *Answers to*

*Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations* 3 (Jan. 19, 2021) ("SAR FAQs"), http://www.fincen.gov/sites/default/files/202101/Joint%20SAR%20FAQs%20Final%20508.pdf.

The decision to maintain or close an account is generally a risk-based decision for an individual financial institution, one that is often made with less than complete information. As discussed below, however, failing to close an account where illicit finance risk was unduly high or not properly managed, even only with the benefit of hindsight, has been the basis for criminal and regulatory actions against financial institutions for BSA/AML violations.

### C. Institutions Are Routinely Subject to Scrutiny of their BSA/AML Compliance and Face Substantial Civil and Criminal Liability for Programs Found Inadequate.

Financial institution regulators conduct frequent examinations of BSA/AML compliance programs. *See* Joint Statement, at 2 ("The federal banking agencies conduct risk-focused BSA/AML examinations, and tailor examination plans and procedures based on the risk profile of each bank[,] . . . [including by] generally allocat[ing] more resources to higher-risk areas, and fewer resources to lower-risk areas."). Institutions face severe sanctions for findings of noncompliance, including for failing to file SARs when required, failing to close accounts engaged in problematic transactions, and otherwise maintaining inadequate BSA/AML programs.

BSA/AML-related enforcement actions brought against financial institutions by a variety of government agencies have led to massive penalties. From 2009 through 2015, the federal government assessed about $5.2 billion in sanctions against financial institutions related to BSA/AML violations. *See* GAO, GAO-16-297, *Financial Institutions: Fines, Penalties, and Forfeitures for Violations of Financial Crimes and Sanctions Requirements* 11 (2016). Sample criminal and civil enforcement in this area include: (1) 2018 actions by the Justice Department, FinCEN, Federal Reserve, and OCC that resulted in U.S. Bancorp paying more than $600 million related to findings that it had, among other things, failed to maintain an adequate compliance program and failed to timely file SARs or close accounts of a customer involved in illegal activity;[3] (2) 2015 actions by, among others, the Justice Department, the Federal Reserve, and New York state authorities that resulted in Commerzbank paying close to $1.5 billion in penalties related to, among other things, findings that it had failed to maintain an adequate compliance program and to file SARs related to a multibillion-dollar securities fraud operated through the

[3] *See, e.g.*, DOJ, *U.S. Attorney Announces Deferred Criminal Charges Against U.S. Bancorp* (Feb. 15, 2018), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-us-bancorp-violations-bank.

bank;[4] and (3) 2014 actions by the Justice Department, FinCEN, and the OCC that resulted in JPMorgan paying over $2 billion in forfeiture and penalties related to findings that the bank had failed to maintain an adequate compliance program.[5]

## III. BPI's Study Reinforces the BSA's Broad Mandate and Does Not Present Any Evidence of Discrimination

The brief of an *Amicus Curiae* in support of Plaintiff-Appellant cites data published by BPI to argue that this Court should view account closings attributed to BSA/AML compliance as suspect. That study, however, provides no evidence that BSA/AML compliance is being used to engage in unlawful discrimination. Instead, it merely underscores the broad scope of BSA regulatory requirements.

By way of background, in a study published in 2018, BPI surveyed eight financial institutions and found that, as of 2017, law enforcement had contacted those institutions regarding less than four percent of SAR filings. BPI, Getting to Effectiveness, *supra*, p. 9. The Appellant *Amicus* Brief cites a BPI blog post

---

4 *See, e.g.*, DOJ, *Commerzbank AG Admits to Sanctions and Bank Secrecy Violations* (Mar. 12, 2015), https://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million-and.

5 *See, e.g.*, DOJ, *Manhattan U.S. Attorney and FBI Assistant Director-In-Charge Announce Filing Of Criminal Charges Against and Deferred Prosecution Agreement with JPMorgan Chase Bank, N.A.* (Jan. 7, 2014), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-filing-criminal.

publicizing this data that also notes that only a "tiny subset [of SARs] result[ed] in an arrest and ultimately a conviction." BPI, *The Truth About Suspicious Activity Reports* (Sept. 22, 2020), http://bpi.com/the-truth-about-suspicious-activity-reports/. As the *Amicus* supporting Plaintiff-Appellant sees it, this data shows that BSA/AML compliance programs are not "narrowly tailored and effective" at "ferreting out financial wrongdoing," "but rather a broad compliance-oriented paradigm ripe for misuse." Appellant *Amicus* Brief at 16.

The BPI study, however, does not suggest that financial institutions are engaging in bad conduct or otherwise shielding unlawful discriminatory behavior from view. Three specific points bear mentioning in response.

1. The statistic pointed to—the percentage of SARs that lead to law enforcement inquiry or are followed by an arrest or conviction—reflects the breadth of SAR filing requirements and has no relationship to discrimination. As described above, complying with the BSA involves a major undertaking. SAR regulations sweep in an expansive set of transactions—capturing many situations in which an institution does not, and frequently cannot, know whether there is underlying criminal activity. Institutions are responsible for reporting these transactions, which are then added to a large database searchable by law enforcement and national security authorities. *See* GAO, *Anti-Money Laundering*, at 4, 19. And again, a SAR can provide important information even if it does not lead to law enforcement

follow-up, an arrest, or a conviction. Given the potential for regulatory criticism and civil and criminal liability if an institution is determined not to have filed a SAR when required, it should come as no surprise that institutions scrupulously file SARs in connection with a wide range of transactions for which they could be deemed required. *See, e.g.*, GAO, GAO-09-226, *Bank Secrecy Act, Suspicious Activity Report Use is Increasing* 18–19 (2009). Indeed, regulators have not intimated that financial institutions are "over-filing" SARs.

Congress, FinCEN, and others, including *Amici*, have recognized that BSA/AML compliance efforts, and SAR filing requirements in particular, can be better tailored to further the purposes of the BSA. Earlier this year, Congress directed the Treasury Department, in consultation with law enforcement, national security authorities, financial regulators, and other stakeholders, to review BSA reporting requirements, including for SARs, "to reduce any unnecessarily burdensome regulatory requirements and ensure" that reported information "fulfills the purposes" of the BSA. Anti-Money Laundering Act of 2020, § 6204; *see id*. § 6205 (requiring a similar review of the dollar thresholds applicable to SARs and other reports). Relatedly, last year, FinCEN recounted the status of its efforts working with law enforcement, financial institution regulators, and the financial industry, to "re-examine the BSA regulatory framework and the broader national AML regime" to "upgrade and modernize" that regime, including by "discard[ing] inefficient and unnecessary practices." Anti-Money Laundering Program Effectiveness, 85 Fed. Reg. 58,023, 58,024 (Sept. 17, 2020). But, even if there is room to improve the BSA/AML regulatory regime, there is no reason whatsoever to infer nefarious activity from the percentage of SARs that lead to law enforcement inquiry followed by an arrest or conviction.

2. Additionally, there is a fundamental distinction between the activity at issue in BPI's study (the filing of a SAR) and the activity at issue in this case (the closing of an account). A SAR does not need to, and frequently does not, result in the closing of a customer's account. *See* SAR FAQs at 3. For example, a SAR filed as a result of a single, one-off transaction may not lead to a determination that the customer poses an excessive money laundering risk to the institution, and that an account closing is appropriate. In other cases, however, the nature of the underlying conduct involved in the SAR filing, and other facts and circumstances that relate to the account, transaction, or customer, may lead to an account closing in connection with a SAR filing. Therefore, even if SAR filing requirements are too expansive, it does not follow that, in an individual case, a financial institution has impermissibly closed an account.

3. BSA/AML requirements and compliance programs do not exist in a vacuum. Financial institutions must also comply with myriad other legal demands, including various federal and state anti-discrimination and consumer protection

statutes. Like the BSA, these laws impose obligations on financial institutions at all stages of the customer relationship. Financial institutions cannot, for example, discriminate based on protected characteristics in determining how they extend mortgages and other loans. *See, e.g.*, 42 U.S.C. § 3605(a) (Fair Housing Act); 15 U.S.C. § 1691(a) (Equal Credit Opportunity Act); N.Y. Banking Law § 9-F.

Consumer protection and anti-discrimination obligations also apply beyond the lending context. Financial institutions are subject not only to the statutes and regulations cited above, but also to several generally applicable anti-discrimination requirements, including, among numerous others, the federal and New York provisions at issue in this case, which may apply to discrimination related to deposit accounts. *See* 42 U.S.C. § 1981; N.Y.C. Admin. Code § 8-107(4) (New York City Human Rights Law), N.Y. Exec. Law § 296(2)(a) (New York State Human Rights Law); *see also* Cal. Civil Code § 52(a) (California Unruh Civil Rights Act).

Just as with BSA/AML compliance, institutions must maintain comprehensive and extensive programs to comply with anti-discrimination laws, and they are subject to regular examinations of these programs. *See, e.g.*, CFPB, *Supervision and Examination Manual: Overview*, 3–4 (Oct. 2012), https://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf?source=post_page; Federal Reserve, *Consumer Compliance*

*Handbook*, at iii (Nov. 2013), https://www.federalreserve.gov/boarddocs/supmanual/cch/cch.pdf (describing CFPB and Federal Reserve consumer compliance oversight and examinations).

And just as with BSA/AML compliance, institutions that violate anti-discrimination and consumer protection statutes can be subject to substantial liability. Indeed, last month, the Justice Department announced a new "aggressive and coordinated enforcement effort to address redlining," a form of lending discrimination in which lenders avoid providing services to certain communities because of the race or national origin of the people who live there. DOJ, *Justice Department Announces New Initiative to Combat Redlining* (Oct. 22, 2021), https://www.justice.gov/opa/pr/justice-department-announces-new-initiative-combat-redlining.

Past settlements have levied large fines on financial institutions related to discrimination in connection with lending practices. *See, e.g., United States and CFPB* v. *Trustmark National Bank*, No. 21-2664 (W.D. Tenn. Oct. 27, 2021) (settlements with the Justice Department, CFPB and OCC providing for a $5 million aggregate penalty); *United States* v. *Cadence Bank, N.A.*, No. 21-3586 (N.D. Ga. Aug. 31, 2021) (settlements with Justice Department and OCC providing for among other things, $3 million penalty and over $5.5 million in loan subsidies and other initiatives); *United States and CFPB* v. *Hudson City Savings Bank, F.S.B.*, No. 15-

7056 (D.N.J. Nov. 4, 2015) (settlements with the Justice Department and CFPB providing for a $5.5 million penalty and the creation of a $25 million loan subsidy fund); *United States* v. *Wells Fargo Bank, N.A.*, 891 F. Supp. 2d 143, 144 (D.D.C. 2012) (settlement with the Justice Department providing for at least $125 million in compensation to aggrieved borrowers, $50 million in down payment assistance).

Financial institutions may also face regulatory scrutiny, reputational harm, and financial liability if they violate anti-discrimination or consumer protection laws outside the lending context. BSA/AML compliance certainly does not provide an all-purpose defense to any such scrutiny or other allegations relating to unlawful discrimination.

Given financial institutions' commitments to adhering to anti-discrimination and other consumer protection laws, and the regulatory attention paid to these requirements, it should come as no surprise that financial institutions focus a great deal of time, energy, and resources on compliance. *Amici* are not aware of any evidence that BSA/AML compliance programs override these efforts and provide a surreptitious means of engaging in prohibited discrimination. When implementing and maintaining BSA/AML compliance programs financial institutions seek to fulfill their extensive legal obligations under the BSA; nothing more suspect is at work.

## CONCLUSION

For these reasons, this Court should affirm the judgment below.

Dated: New York, New York
November 29, 2021

Respectfully submitted,

/s/ *Sharon Cohen Levin*

Sharon Cohen Levin
Sullivan & Cromwell LLP
125 Broad Street
New York, NY 10004
(212) 558-4000

Jennifer L. Sutton
Jordan M.H. Wish
Leslie B. Arffa
Sullivan & Cromwell LLP
1700 New York Avenue, N.W.
Washington, DC 20006
(202) 956-7500

*Counsel for Amici Curiae*

Tara S. Morrissey
U.S. Chamber Litigation Center
1615 H Street, N.W.
Washington, DC 20062
(202) 463-5337
*Counsel for the Chamber of Commerce of the United States of America*

## CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g)(1), I certify that:

This brief complies with the length limitation of Circuit Rule 29.1(c) because this brief contains 6,340 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Microsoft Word 2016 Times New Roman 14-point font.

Dated: New York, New York
November 29, 2021

/s/ *Sharon Cohen Levin*

Sharon Cohen Levin
Sullivan & Cromwell LLP
125 Broad Street
New York, NY 10004
(212) 558-4000

*Counsel for Amici Curiae*

## CERTIFICATE OF SERVICE

I hereby certify that on November 29, 2021 I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Second Circuit by using the appellate CM/ECF system.

I certify that all participants in this case are registered CM/ECF users and that service will be accomplished through the CM/ECF system.

Date: November 29, 2021

/s/ *Sharon Cohen Levin*
Sharon Cohen Levin
Sullivan & Cromwell LLP
125 Broad Street
New York, NY 10004
(212) 558-4000

*Counsel for Amici Curiae*