Getting to Effectiveness – Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance

BANK POLICY INSTITUTE

October 29, 2018

Table of Contents

Introduction	1
AML/CFT Program Resources	3
SAR & CTR Resources and Effectiveness	5
a. SAR Resources and Effectiveness	5
b. Structuring SAR Resources and Effectiveness	7
c. CTR Resources and Effectiveness	7
KYC Program Resources and Effectiveness	9
Sanctions Program Resources and Effectiveness	10
Conclusion	12

Introduction

In 2018, the Bank Policy Institute[1] undertook an empirical study to better understand the resources U.S. financial institutions are devoting to Bank Secrecy Act, anti-money laundering and sanctions compliance, and whether these resources are efficiently and effectively supporting law enforcement and national security efforts. The purpose of the Bank Secrecy Act, which was enacted in 1970, is to require certain reports or records that have a "high degree of usefulness" to law enforcement or national security officials.[2] Yet, very little is known about what records and reports are highly useful to law enforcement. Furthermore, Congress granted authority to implement the BSA to the Secretary of the Treasury, thereby designating an agency with both financial and law enforcement expertise as its administrator.[3] Since its enactment, the BSA has been amended but not significantly revised, while attending regulatory requirements have remained similarly stagnant. However, financial crime has changed over the intervening years. As discussed in substantial detail in previous letters and reports,[4] the AML/CFT regime needs to be redesigned in order to be more efficient and effective and address present-day risks, with the ultimate goal of enhancing national security and law enforcement efforts to detect and address domestic and international money laundering and terrorist financing. Any revisions to the regime should be flexible enough to account for the changing ways in which illicit financial activity is conducted.

This study is intended to assist public sector efforts to address the outdated and misaligned nature of the current AML/CFT regime as well as any subsequent reviews of the sanctions regime that may be contemplated by the U.S. Department of the Treasury.[5] Nineteen member institutions participated in this study, with asset sizes ranging from approximately $50 billion to over $500 billion and the frequency of responses to specific questions within the survey varying due to the availability of data at participating institutions. To better understand institutional resources devoted to effectiveness, where appropriate, responses were categorized and analyzed based on the following categories: (i) small institutions were defined as having approximately $50 to 200 billion in U.S. assets; (ii) midsize institutions were defined as having $200 to 500 billion in U.S. assets; and (iii) large institutions were defined as having over $500 billion in U.S. assets. The survey questionnaire was developed with member feedback and conducted over a period of approximately four months. It targeted areas where, based on individual institutions' experiences, empirical data could be sought to better understand, on a case-by-case basis, the performance of the AML/CFT and sanctions regimes. Furthermore, it focused on the resources devoted to the maintenance of U.S.-based AML/CFT and sanctions program compliance and therefore does not account for the global investment financial institutions make in such programs. Notably, the inclusion of such global investments would significantly increase the data set forth in this report as many

---

1 The Bank Policy Institute (BPI) is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Its members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ millions of Americans, make a majority of the nation's small business loans, and are an engine for financial innovation and economic growth. This survey was conducted by The Clearing House Association ("TCH"), prior to its merger with the Financial Services Roundtable to form BPI. Because this merger was complete prior to the formal release of these survey results, they are being published on behalf of BPI.

2 *See* 31 U.S.C. § 5311, which states that "[i]t is the purpose of this subchapter [the BSA] to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."

3 See 31 U.S.C. 5318(a)(2) and (h)(2). As recently as 2014, the Secretary delegated that authority to FinCEN. See Treasury Order 180-01 (July 1, 2014).

4 *See* The Clearing House Association letter to Treasury re "Request for Comments Regarding Suspicious Activity Report and Currency Transaction Report Requirements," April 10, 2018, *available at* bpi.com/wp-content/uploads/2018/04/20180410_tch_comment_letter_to_fincen_on_sar_and_ctr_requirements.pdf; The Clearing House Association and the Financial Services Roundtable letter to Treasury on its "Review of Regulations," July 31, 2017, *available at* bpi.com/wp-content/uploads/2017/07/Joint-_Trades_Comment_Letter_to_Treasury_on_Review_of_Regulations.pdf; The Clearing House Association, A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement, ("TCH AML/CFT Report") (February 2017), *available at* bpi.com/wp-content/uploads/2018/07/20170216_tch_report_aml_cft_framework_redesign.pdf.

5 *See* U.S. Department of the Treasury, *Review of Regulations*, June 14, 2017, *available at* www.federalregister.gov/documents/2017/06/14/2017-12319/review-of-regulations. The Treasury Department's *Review of Regulations* was issued in furtherance of Executive Orders 13771 and 13777.

midsize and most large institutions maintain AML/CFT and sanctions programs that are global in nature. Therefore, figures for U.S.-based programs are only approximations and may underestimate the resources institutions are devoting to compliance efforts as different institutions have different ways of attributing figures to their U.S. programs given that many institutions allocate resources on a global programmatic basis.

All responses were provided to BPI's counsel, which consolidated the data, performed certain quality checks (and followed up with respondents as appropriate) and provided summary statistics, on an anonymized basis, to BPI and participating institutions. As there is no established metric for measuring whether financial institutions' BSA reports are "useful" to law enforcement, and little to no feedback from law enforcement on the matter, a proxy was used to evaluate this component, which was derived from tracking instances where law enforcement reached out to institutions – through subpoenas, national security letters or requests for backup documentation – on their filings; certain questions also considered whether law enforcement inquiries were made pursuant to Section 314(a) of the USA PATRIOT Act.

The results found that:

- Survey participants are employing over **14,000 individuals**, investing approximately **$2.4 billion** and utilizing as many as **over 20 different I.T. systems** per institution **to assist them with BSA/AML compliance**;

- In 2017, survey participants reviewed approximately **16 million alerts**, filed over **640,000 SARs** and more than **5.2 million CTRs**, and institutions that record data regarding law enforcement inquiries reported that a median of **4% of SARs** and an average of **0.44% of CTRs warranted follow-up inquiries from law enforcement**;

- In 2017, survey participants that recorded alerts by activity type reported that **18% of their alerts related to structuring**, **40%** of their filed SARs involved potential structuring[6] and **3, 545** of those **structuring SARs warranted follow-up inquiries from law enforcement**;

- In 2017, survey participants reported that of approximately **2.36 million "high risk" customers**, a median of **roughly 6% were subject to SAR filings** while **0.3%** of these SAR filings **warranted follow-up inquiries from law enforcement**; and

- Survey participants are employing over **915 individuals**, investing roughly **$173 million**, and utilizing **3 to 6 I.T. systems** at each institution to assist them with U.S.-based sanctions compliance, yet when screening wires and customer and related party accounts for potential OFAC matches, institutions reported **true matches** with an overall median of **0.00004%**, with some institutions reporting **no true customer matches at all**.

[6] We note that, in this case, provided responses may not be completely comparable. A full explanation is provided in footnote 24. A median is used here to assist in providing an exemplary value.

AML/CFT Program Resources

The Bank Secrecy Act requires financial institutions to set basic requirements for AML/CFT programs, including: (i) the development of internal policies, procedures and controls; (ii) designation of a BSA or compliance officer; (iii) ongoing training requirements; and (iv) a robust audit or independent review function. Financial institutions invest significant resources in complying with these and other responsibilities promulgated under the statute, including conducting customer due diligence and filing SARs and CTRs, among others.

To that end, 17 institutions reported that they employ over 14,000 full-time individuals to assist them with these efforts, with smaller institutions employing an average of approximately 220 personnel and large institutions contributing about 60% of the total population of individuals.[7] These individuals generally serve in various aspects in an institutions' three lines of defense, as illustrated in Chart 1. As a general matter, the first line of defense refers to employees who assist with AML compliance as part of the business line, the second line of defense refers to AML compliance staff and the third line of defense encompasses an institution's independent AML audit function.

Chart 1: U.S. Financial Institutions' AML Personnel Split by Lines of Defense

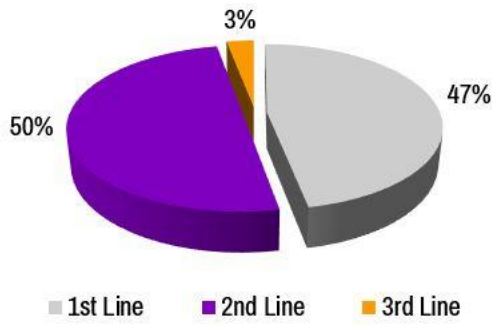


Diagram 1: Percentage of U.S. Financial Institutions' AML Staff Devoted to Key Compliance Activities

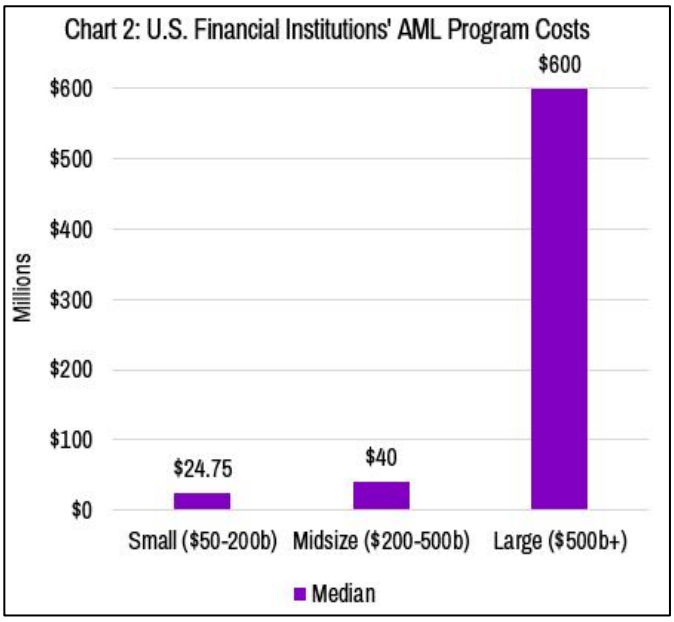
Analytic Models and Model Validation, 2.4%	Screening, 9%	Transaction Monitoring, 12%	SARs, 22%	Proactive Initiatives, 6%	Other, 48.6%
Includes staff that create, develop, tune and validate models used by automated monitoring systems.	Includes staff that perform name searches against various watch lists as well as sanctions employees.	Includes staff that work on alert management, triage, and disposition prior to the case investigation stage and excludes personnel working on proactive matters.	Includes investigative staff as well as employees who prepare SAR filings themselves and excludes personnel working on proactive matters.	Includes staff devoted to financial institution efforts to develop new and innovative methods for detecting suspicious activity. This category does not include investigative or other staff working on alerts or cases generated by the institution's transaction monitoring platform.	The remainder of financial institutions' AML staff are training customer-facing employees; issuing policies and procedures; conducting quality assurance over data and processes; documenting, monitoring and governing decisions relating to their AML programs; making customer relationship decisions and managing the testing, auditing and examinations of such programs and systems, among other things.
17 Respondents	17 Respondents	17 Respondents	18 Respondents	15 Respondents	

All % reflect the median response except "other."

Diagram 1 further reflects resources that institutions are devoting to key AML compliance activities. AML compliance staff serve many functions at an institution: they train customer-facing employees so they can escalate unusual activity; advise their business colleagues; conduct customer due diligence and develop customer risk profiles; tune detection systems to generate investigative cases; assess and analyze the financial crimes risks inherent in and the controls placed over financial institutions' products and services; resolve investigative cases; and, when appropriate, report suspicious activity to the government. Some also work on strategic initiatives aimed at understanding and reporting on significant financial crimes threats or other proactive efforts. Finally, institutions have AML staff devoted to issuing policies and procedures; conducting quality assurance over data and processes; documenting, monitoring and

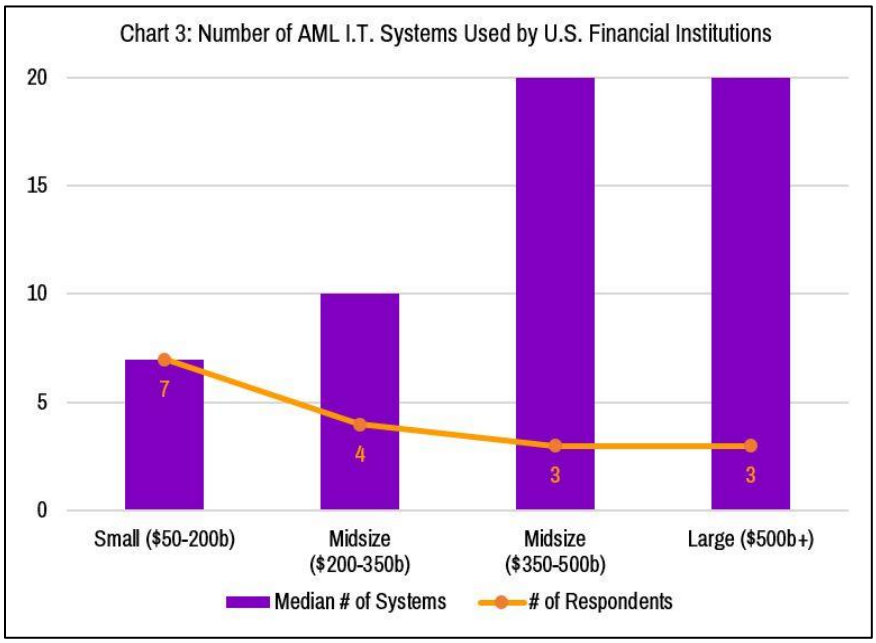
[7] Of note, these figures exclude contractors.

governing decisions relating to financial institutions' AML programs; making customer relationship decisions; and managing the testing, auditing and examinations of such programs and systems. To that end, 12 respondents indicated that their AML compliance staff make up a little more than one third of the overall population of these institutions' compliance and risk functions.



In addition to the personnel financial institutions devote to AML compliance, they also dedicate substantial financial resources to support such efforts. Accordingly, 14 institutions reported that in the aggregate they devote approximately $2.4 billion to AML/CFT compliance.[8] Chart 2 shows institutions' median AML/CFT costs broken out by asset size, with large institutions accounting for 80% of the aggregate total.

Finally, a key programmatic element that significantly impacts financial institutions' investment in AML compliance is technology, as it typically constitutes a substantial portion of a financial institution's AML budget. As shown in Chart 3, based on the median responses of 17 participants, banks utilize up to 20 different I.T. systems, such as transaction monitoring and Know-Your-Customer,[9] to assist them in conducting their AML programs.



As previously discussed, the purpose of the BSA is to provide law enforcement with leads that are of a "high degree of usefulness," and financial institutions are devoting substantial resources towards that goal, yet very little is known about the effectiveness of banks' filings. Thus, the following section will focus on the leads being provided through the submission of SARs and CTRs, and whether the resources deployed in support of these efforts appear to be fulfilling the regime's purpose.

[8] Cost includes technology (e.g. KYC and TM programs), outside consultants, human capital, and other AML-related business-as-usual costs and excludes lines of business, sanctions and fraud costs.

[9] Although the term "KYC" is not used in regulations, it is generally used in industry and regulator parlance to broadly refer to institutions' obligations to collect, analyze, and use information about their customers to comply with various AML requirements that require financial institutions to understand, to some extent, the nature and identities of the parties with whom or on whose behalf they are conducting financial transactions.

SAR & CTR Resources and Effectiveness

Financial institutions provide leads to law enforcement through two main reports, SARs and CTRs. Current regulations dictate that banks are required to file a SAR with Treasury's Financial Crimes Enforcement Network (FinCEN) on federal criminal violations that: (i) involve insider abuse; (ii) total at least $5,000 where a suspect can be identified; or (iii) total at least $25,000, regardless of whether a suspect can be identified. A SAR is also required for transactions totaling at least $5,000 if the financial institution knows, suspects, or has reason to suspect that the transaction: (i) may involve money laundering or other illegal activity; (ii) is designed to evade the BSA or its implementing regulations (e.g. structuring); or (iii) has no business or apparent lawful purpose or is not of the type in which the customer would be expected to engage. In 2017, FinCEN received over 2 million SAR submissions from filers including depository institutions, money service businesses and casinos, among others.[10]

Financial institutions are also required to file CTRs with FinCEN on each transaction in currency (deposit, withdrawal, exchange, or other payment or transfer) of more than $10,000 by, through, or to the institution. While some exemptions apply, the CTR requirement notably includes an aggregation component requiring financial institutions to treat "[m]ultiple currency transactions totaling more than $10,000 during any one business day…as a single transaction if the bank has knowledge that they are by or on behalf of the same person."[11] CTRs have seen various iterations since their inception; however, in recent years, over 15 million CTRs have been filed in the United States per year.[12]

a. SAR Resources and Effectiveness

Financial institutions utilize alerts, generated from rules-based transaction monitoring systems or manual/human-initiated alerts, as their initial notification of potential suspicious activity. Some of these alerts, once reviewed, become full case investigations – which generally necessitates the production of additional investigatory materials, written summaries and other documentation. Finally, some of these full case investigations become SAR filings.

In order to execute this process, in 2017, 18 respondents reported employing roughly 3,650 individuals on their SAR teams, with the same number of respondents indicating that they filed over 640,000 SARs and the largest institutions accounting for roughly 75% of both totals. While the SARs submitted by 18 respondents accounted for approximately 31.6% of the over 2 million SARs filed with FinCEN in 2017, it should be noted that the vast majority of the SARs provided were filed by depository institutions (banks and credit unions), which submitted a total of 916,351 SARs, and money service businesses, which filed 874,131 SARs.[13] Previous BPI research found that, in 2016, of the roughly 1 million SARs filed annually by depository institutions, approximately 50% were filed by only four large banks. In addition, the median response from 13 financial institutions indicated that in 2017, 25% of their SAR submissions were on "transactions with no apparent economic, business, or lawful purpose" as required by regulation, with the largest

---

10 *See* "SAR Stats," *available at* www.fincen.gov/fcn/Reports/SARStats. The total number of SARs filed in 2017 was 2,034,406; *accessed* October 18, 2018. SARs are filed under numerous suspicious activity categories including money laundering, fraud, cyber, terrorist financing and structuring, among others.

11 *See* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, "Currency Transaction Reporting – Overview," p. 81.

12 *See* FATF Anti-money laundering and counter-terrorist financing measures, *Mutual Evaluation of the United States*, December 2016, pg. 54; *available at* www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

13 *See* SAR Stats, *supra* n. 10.

institutions reporting such SARs at the greatest frequency.[14] In addition, 14 respondents reported that a median of 4% of their 2017 SARs warranted law enforcement contact.[15]

Furthermore, 17 respondents reported that in 2017 their institutions collectively reviewed approximately 16 million AML alerts and filed over 633,000 SARs, with an implied aggregate conversion rate to SARs of 4%.[16] This conversion rate is not a true reflection of the resources devoted to SAR filings as the alerts provided related to AML transactions only, whereas the number of SARs filed includes both fraud and AML SARs. However, it is still instructive as including fraud alerts would have decreased the conversion rate further. It should be noted that while there may be instances where multiple alerts lead to one SAR filing, these numbers appear to reflect a low ratio of SAR filings to alerts, as shown in Table 1 below.

Table 1: 2017 U.S. Financial Institutions' AML Alert Generation, Case Investigation[17] and SAR Filing Statistics

	% of transactions that generated AML alerts (Approx.)	No. of AML Alerts Generated (Approx.)	Conversion Rate of Alerts to Cases*^ (Approx.)	Conversion Rate of Cases to SARs*^ (Approx.)
Large ($500b+)	0.6%	2.8 million	20%	42%
Midsize ($200-500b)	2%	117, 000	9.5%	54%
Small ($50-200b)	0.08%	107,000	8%	53%
No. of Respondents	12	13	13	13

* Responses provided fell within a very broad range.

^ Note: A direct correlation cannot be drawn as the alerts provided related to AML only, whereas the number of SARs filed includes both fraud and AML SARs.

The percentages above are based on median responses.

While this study focuses on the resources financial institutions devote to SAR filings, such filings can also impact customers as multiple filings may result in the termination of a customer's account or additional institutional or examiner scrutiny. Regulatory guidance indicates that banks should continue to review suspicious activity to determine whether "other actions," such as terminating a customer relationship, "may be appropriate," and that examiners should, as part of their review of institutions' SAR program, review banks' account termination policies, procedures and processes.[18] In 2017, 12 respondents reported that a median of roughly 28% of SAR filings resulted in account terminations due to multiple filings, a metric that is inherently subjective given the differences in AML policies and procedures at financial institutions. However, 8 of these institutions reported that a median of approximately 3.65% warranted law enforcement contact on the relevant SAR filings.[19] Given the sample size, it is difficult to determine the statistical significance of the various rates of law enforcement follow-up; however, it should be noted that when comparing the overall rate of law

14 The relevant SAR filing category is discussed in this report. However, 31 CFR 1020.320 (a)(2)(iii) states that a SAR is required when "[t]he transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction." FinCEN's SAR Stats tool indicates that 16.2% of SARs filed in 2017 were unknown purpose SARs, with the largest number of submissions coming from depository institutions. *See* SAR Stats*supra* n. 10. The total number of unknown purpose SARs filed in 2017 was 329,658. Of note, more than one type of suspicious activity may be indicated on a SAR.

15 As discussed in the introduction, law enforcement contact includes subpoenas, national security letters or requests for SAR backup documentation.

16 It should be noted that in order to better understand the resources devoted to AML compliance, fraud alerts were not included in the aggregate total of alerts, but fraud SARs were included in the total number of SARs as the requirement to report on "suspicious transactions" is promulgated under the BSA.

17 Case investigations were defined as investigations that generally necessitate the production of additional investigatory materials, written summaries and other documentation.

18 *See* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, "Suspicious Activity Reporting – Overview" p.69 and "Suspicious Activity Reporting - Examination Procedures" p. 77.

19 As discussed in the introduction, law enforcement contact includes subpoenas, national security letters or requests for SAR backup documentation.

enforcement follow-up on all the SARs submitted by these 8 institutions with the rate of law enforcement follow-up on SAR filings that resulted in account terminations, the data appears to reflect some correlation, suggesting that law enforcement may follow up at a higher frequency on SARs filed on terminated accounts.

b. Structuring SAR Resources and Effectiveness

FinCEN's SAR Stats tool indicates that almost half of the over 2 million SARs filed in 2017 were submitted due to suspicions of structuring.[20] FinCEN regulations broadly define structuring by stating that "a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency, in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the [CTR reporting requirements]. 'In any manner' includes, but is not limited to, the breaking down of a single sum of currency exceeding $10,000 into smaller sums… [t]he transaction or transactions need not exceed the $10,000 reporting threshold at any single financial institution on any single day in order to constitute structuring within the meaning of this definition."[21]

Given the large number of structuring SARs filed, this study further investigated the resources financial institutions are devoting to these submissions. Eleven financial institutions reported that, on average, they spend 1.4 hours completing a structuring SAR narrative, with the smallest institutions reporting that they spend a median of 1.65 hours completing such narratives. In addition, of the 13 institutions that reported a percentage of alerts related to structuring, the median response was 18%.[22] Furthermore, 8 institutions reported a median of about 42% of these alerts as standalone structuring alerts.[23] In addition, while responses varied and the provided responses may not be comparable in certain cases,[24] a median of 15 institutions indicated that 40% of their SAR filings involved structuring. As discussed previously, given the resources devoted to investigating alerts, including those signaling potential structuring, 11 institutions reported that they received a total of 3,545 follow-up requests from law enforcement on their structuring SARs, with the four largest reporting institutions accounting for more than 90% of the aggregate total.

c. CTR Resources and Effectiveness

According to Federal Reserve Board data, the amount of currency in circulation has steadily increased over the last two decades with over 41.6 billion U.S. notes in circulation, amounting to over $1.5 trillion, as of December 31, 2017.[25] Additional research indicates that cash is still widely used by consumers for low-dollar, in-person purchases, with

---

20 *See* SAR Stats*supra* n. 10. The total number of SARs filed in 2017 that indicated structuring was 928,927; *accessed* October 23, 2018. Of note, more than one type of suspicious activity may be indicated on a SAR.

21 *See* 31 CFR 1010.100.

22 Based on the data provided by respondents, this percentage translates to a total of 1.57 million alerts.

23 Based on the data provided by respondents, this percentage translates to about 650,000 alerts.

24 Specifically, certain respondents appear to have provided the percentage as a total of both AML and fraud SAR filings (as previously indicated, fraud SARs were included in the total number of SARs as the requirement to report on "suspicious transactions" is promulgated under the BSA), but other respondents appear to have provided them as a percentage of AML SARs only. Furthermore, the survey question was also intended to capture all SAR filings that involve structuring (i.e., those SAR filings for which structuring was indicated as an activity category, even if other activity categories were also identified as part of the same filing), though a few respondents may have provided data for only standalone structuring SARs. Therefore, a median is used to assist in providing an exemplary value.

25 *See* Board of Governors of the Federal Reserve System, "Volume of currency in circulation, in billions of notes as of December 31 of each year," *available at* www.federalreserve.gov/paymentsystems/coin_currcircvolume.htm, *accessed* August 21, 2018. *See also* Board of Governors of the Federal Reserve System, "Volume of currency in circulation, in billions of dollars as of December 31 of each year," *available at* www.federalreserve.gov/paymentsystems/coin_currcircvalue.htm, *accessed* August 21, 2018.

"households with an annual income of less than $50,000 per year rely[ing] more heavily on cash than [] higher income groups."[26]

As described above, financial institutions are required to file CTRs on currency transactions of more than $10,000, aggregating multiple transactions as necessary. They also are required to file SARs when they suspect that customers are structuring their transactions in order to avoid the CTR filing threshold. To that end, 17 institutions reported filing more than 5.2 million CTRs in 2017, with 57% of this total submitted by three large institutions. Box 1 provides additional statistics on how dollar thresholds appear to impact the frequency of CTR filings.

Box 1: Analysis of the Impact of the CTR Threshold on 2017 Filings (Median %)
17 institutions reported filing 5.2 million CTRs.
9 institutions reported that 44% of their CTRs were for transactions totaling $15K or less.
8 institutions reported that 65% of their CTRs were for transactions totaling $20K or less.
8 institutions reported that 80% of their CTRs were for transactions totaling $30K or less.

In addition, 16 institutions reported employing approximately 550 full-time individuals to assist with CTR compliance. These employees, in part, facilitate institutions' efforts to comply with the CTR aggregation requirement, which for 7 institutions accounted for roughly 64% of their CTR filings.[27] Finally, 10 institutions reported law enforcement inquiries on CTRs in an average of roughly 0.44% of cases.

[26] *See* Shaun O'Brien, "Understanding Consumer Cash Use: Preliminary Findings from the 2016 Diary of Consumer Payment Choice," Federal Reserve Bank of San Francisco, November 28, 2017, *available at* www.frbsf.org/cash/publications/fed-notes/2017/november/understanding-consumer-cash-use-preliminary-findings-2016-diary-of-consumer-payment-choice/; *accessed August 21, 2018.*

[27] These 7 institutions indicated that of the roughly 2.49 million CTRs they filed, approximately 64%, or nearly 1.6 million, were the result of aggregating multiple transactions.

KYC Program Resources and Effectiveness

Financial institutions are required to conduct due diligence on their customers, or "know their customers," in order to "predict with relative certainty the types of transactions in which a customer is likely to engage."[28] Furthermore, for "high-risk" customers financial institutions are required to conduct enhanced due diligence (EDD). As a general matter, financial institutions spend significant time collecting defined enhanced due diligence on broad categories of customers that have been deemed high-risk, without differentiation, in regulatory guidance manuals.[29] This is evidenced by the 7 institutions, 5 of which were small institutions, that reported employing a total of 355 individuals to assist them in their EDD compliance efforts.

Given the additional oversight these customers receive, and the heightened potential for SAR filings on them, institutions provided statistics on the various resources they devote to this effort. 16 institutions reported a total of approximately 2.36 million "high-risk" customers, with 13 institutions reporting that a median of roughly 6% of these customers were the subject of a SAR filing in 2017 and 9 institutions reporting that a median of approximately 0.3% warranted follow-up inquiries from law enforcement.[30] Finally, 10 institutions reported that they exited "high-risk" customers, in part, due to AML/CFT concerns in about 1% of cases when a SAR was filed.

Table 2: Resources Devoted to PEP and Negative Media Screening

	No. of SARs Filed	% Resulting in Law Enforcement Contact
PEP	1,037* for 13 institutions	Less than 10% for 9 institutions. 7 institutions that collectively filed over 40% of the PEP SARs indicated receiving law enforcement contact on 3% or less of these SARs, with 6 institutions experiencing 0-1%.
Negative Media	2,687^ for 11 institutions	Median of 5% for 8 institutions

* 4 large institutions accounted for nearly 90% of the aggregate total
^ 3 large institutions accounted for nearly 70% of the aggregate total.

One example of an individual who could be considered "high-risk," and therefore subject to EDD, is a politically exposed person (PEP). The guidance on managing PEP-related risks was released in 2001,[31] and financial institutions use it and other regulatory guidance,[32] in addition to their own policies and procedures, to determine the risk rating to apply to a PEP and when to file a SAR. Negative media screening is another tool that financial institutions use to carry out their KYC obligations and determine SAR filings. To that end, 6 financial institutions responded that they invest $30 million in the aggregate on PEP and negative media screening, which is a requirement for all financial institutions. But, as Table 2 shows, PEP and negative media SARs warranted law enforcement follow-up in 5% or less of cases, with some outliers.

28 *See* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, "Customer Due Diligence–Overview," p. 56.

29 *Id* p. 57.

30 In this case, law enforcement inquiries include 314a requests, subpoena, national security letter, or request for SAR back-up documentation. 314a requests were included in this statistic as the focus of these survey questions was on the effectiveness of regulatory guidance that deems broad categories of customers as "high-risk" and not the narrower metric of the effectiveness of SAR filings.

31 *See* "Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds of Foreign Official Corruption," issued by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the U.S. Department of State, (January 1, 2001), available at www.treasury.gov/press-center/press-releases/Pages/guidance.aspx.

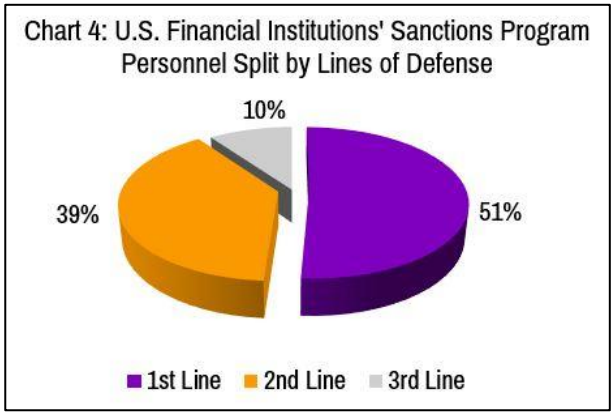
32 For example, *see* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, "Politically Exposed Persons–Overview," p. 290.

Sanctions Program Resources and Effectiveness

While the focus on this study was on the resources financial institutions devote to BSA/AML compliance, there are many places in which sanctions compliance efforts coincide with these investments, therefore BPI also collected data on institutions' sanctions compliance programs.

As a general matter, sanctions programs are a vital tool to U.S. foreign policy, so it is essential that compliance expectations are risk-based and communicated consistently. Administered under the International Emergency Economic Powers Act[33] and other statutes, the President is granted broad authority to impose economic sanctions against countries and parties that threaten the national security, foreign policy and/or the economy of the United States. However, as U.S. sanctions programs have evolved, they have become more targeted.

The Treasury Department's Office of Foreign Assets Control (OFAC) maintains a list of Specially Designated Nationals and Blocked Persons (the SDN List) to whom all U.S. persons may not provide services. As a general matter, a substantial portion of the SDN List includes individuals that do not have a strong nexus to the United States, which impacts the likelihood that a financial institution will identify tangible property interests for blocking purposes. Furthermore, OFAC also maintains territory-based sanctions programs prohibiting U.S. persons and their foreign branches from directly or indirectly providing services for the benefit of certain territories or entities or individuals in those territories. In addition, OFAC has recently issued sectoral sanctions that prohibit U.S. financial institutions from dealing in certain debt and equity transactions with identified sanctions targets. These sectoral sanctions have impacted the resources U.S. financial institutions devote to sanctions compliance as banks generally comply with them by stopping transactions involving sanctions targets and working to identify their underlying purpose in order to draw conclusions as to whether they are covered transactions. U.S. financial institutions screen accounts and transactions against the SDN List, territory-based sanctions program lists, sectoral sanctions lists, internal lists and other governmental lists in order to avoid providing services for the benefit of prohibited individuals, in prohibited countries or regions, or otherwise deal in prohibited debt or equity transactions in the case of sectoral sanctions.

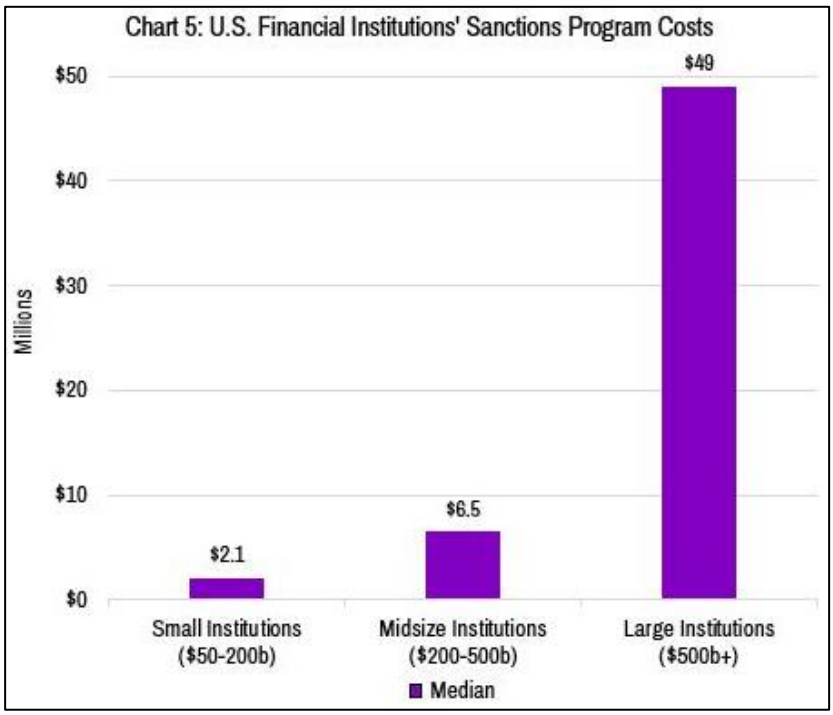


Accordingly, 16 institutions reported employing over 915 full-time employees to assist with their U.S.-based sanctions compliance efforts. Small institutions reported a median of 16 employees, smaller midsize ($200-350b) institutions reported a median of 18 employees, larger midsize ($350-500b) institutions reported a median of 77 employees, and large institutions reported a median of 175 employees. These employees are distributed across institutions' lines of defense as shown in Chart 4. In addition, 13 respondents reported spending an aggregate total of roughly $173 million on their U.S.-based sanctions programs. Furthermore, of 17 respondents, all but 3 indicated that U.S. sectoral sanctions have increased the cost of their programs – with 7 of the 14 institutions, 5 of which are small institutions, indicating that they experienced a median increase in program costs of 20%.[34]

[33] 50 U.S.C. 1701 et seq.

[34] As discussed above, sanctions programs that target certain regions or sectors of a non-U.S. economy are very difficult to implement and therefore impose significant burdens on financial institutions, particularly due to the lack of clarity in their application to intermediary financial institutions as well as the fact that the targets are not blocked or restricted from engaging in other activities throughout the U.S. financial systems.

Chart 5 provides additional information on the breakdown of institutions' sanctions program costs by asset size. It should be noted that respondent data on U.S.-based sanctions programs are estimates as institutions have different ways of attributing numbers to their U.S. programs. Furthermore, the impact of U.S. sanctions policy on the resources devoted to sanctions compliance by financial institutions is skewed to underestimations as financial institutions implement sanctions programs that are global in nature given the unique role of the U.S. in the global financial system.



Additionally, based on responses from 15 financial institutions, small financial institutions generally employ 3 sanctions I.T. systems, while midsize and large institutions employ 6 or more upstream, downstream and middleware systems that feed into sanctions screening filters. To better understand whether these resource investments are effective in ensuring sanctions compliance, institutions provided data on both wires screened for OFAC sanctions matches and customer accounts and related parties screened for OFAC matches. 12 institutions reported screening an aggregate total of over 1.5 billion wires for potential OFAC matches, generating alerts in approximately 13% of cases and resulting in true matches with an overall median of 0.00004%. Table 3 further breaks down financial institutions' wire sanctions screening efforts by asset size. In addition, 13 institutions reported that a very low percentage of customer accounts and related parties resulted in a true OFAC sanctions match in 2017, with an overall median of 0.00004%. Four of these 13 institutions reported identifying no true customer matches in 2017.

Very few true sanctions matches are derived from the resources institutions are investing in screening. Furthermore, it can be inferred that the likelihood of finding a customer match, with tangible property interests to block, is even more limited.

Table 3: 2017 U.S. Financial Institutions' Wire Sanctions Screening Efforts

	Median No. of wires screened (Approx.)	Median % of Sanctions Alerts Generated from Screened Wires (Approx.)	Median % of Sanctions Matches
Large ($500b+)	744 million	1.4%	0.0031%
Midsize ($200-500b)	3.6 million	20%	0.01%
Small ($50-$200b)	2.2 million	12%	0.000045%, with a few institutions reporting no true matches
No. of Respondents	12	12	13

Conclusion

Financial institutions devote thousands of employees and billions of dollars to BSA/AML and sanctions compliance. They are committed to this work and assisting law enforcement and national security officials in their efforts to protect the financial system from illicit activity. Yet, as the data shows, they are presently aware of only a modest number of concrete instances, a median of 4% for SARs and an average of 0.44% for CTRs, where law enforcement finds their reports useful.[35] Furthermore, not all SAR filing categories can be viewed in the same way. For example, structuring SARs could be considered "low-risk" or of little law enforcement value, yet they represent 18% of banks' AML alerts but warranted few law enforcement inquiries for most institutions. This suggests that Treasury, given its role as the administrator of the BSA, should lead a multi-agency review of the regime to prioritize the investigation and reporting of activity that fulfills the BSA's purpose of providing highly useful information, thereby increasing its effectiveness.[36] Such a review, along with the exploration of the provision of real-time data and law enforcement feedback, could assist in allowing financial institutions to provide higher-value information to law enforcement by re-deploying resources to more proactive AML/CFT efforts like identifying and developing techniques to combat emerging trends in illicit activity, investing more heavily in innovation generally (e.g. machine learning), and engaging in more proactive intelligence-led investigations.

However, the lack of prioritization and feedback on SARs and CTRs are not the only areas where the data suggests improvements can be made. As discussed previously, financial institutions spend significant time collecting defined enhanced due diligence on broad categories of customers that have been deemed high-risk in regulatory guidance manuals, yet only 0.3% of these SAR filings warranted followed up inquiries from law enforcement. This suggests that Treasury should take a more prominent role in coordinating AML/CFT policy and examinations, which is presently dispersed amongst multiple federal and state regulatory agencies. Relatedly, sanctions compliance programs appear to be producing similar results, with sanctions screening yielding few to no matches. Public-private sector dialogues on reform are needed to make both regimes more efficient and effective as anecdotal information from survey participants indicate that they're able to be most effective when they partner with law enforcement and national security officials. Therefore, as with the AML/CFT regime, Treasury should take a more prominent role in coordinating sanctions policy across the government to increase the effectiveness of sanctions compliance and further recognize a risk-based approach to compliance.

Finally, while not a primary focus of this study, the data shows that financial institutions are individually using anywhere from 9 to over 25 I.T. systems to support BSA/AML and sanctions compliance. While it is difficult to predict the impact that technological advances, such as machine learning or artificial intelligence, will have on financial institutions' compliance efforts they should be encouraged to test and innovate their policies, procedures, processes and technologies, including those related to identifying suspicious activity, in order to improve the efficacy of their programs.

The United States, through the Treasury Department, has led the world in shaping international standards and dialogue in these policy areas, and we encourage Treasury to continue to take a domestic and global leadership role in proposing changes to enhance the systemic effectiveness and sustainability of the AML/CFT and sanctions regimes.

---

35 *See supra* n. 2, which states that the purpose of the BSA is to provide law enforcement with leads that are of a "high degree of usefulness." As there is no established metric for measuring this a proxy was used, which was derived from tracking instances where law enforcement reached out to institutions – through subpoenas, national security letters or requests for backup documentation – on their filings.

36 Other regions have begun to investigate how financial intelligence supplied by financial institutions and other actors is being used by law enforcement. A 2017 Europol report found that, in a figure unchanged from 2006, only 10% of EU suspicious transaction reports were further investigated after collection. *See* European Union Agency for Law Enforcement Cooperation (Europol), From Suspicion to Action: Converting financial intelligence into greater operational impact, September 5, 2017, *available at* www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact.