July 31, 2017

Via the Federal eRulemaking Portal

U.S. Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

Re: Review of Regulations

Ladies and Gentlemen:

The Clearing House Association L.L.C. and the Financial Services Roundtable (collectively, the "Associations")[1] appreciate the opportunity to comment on the United States Department of the Treasury's *Review of Regulations*, which was issued in furtherance of Executive Orders 13771 and 13777 in order to facilitate review and make recommendations regarding regulations and guidance promulgated by the Treasury Department's Financial Crimes Enforcement Network ("FinCEN"), under the Bank Secrecy Act ("BSA") and related anti-money laundering and countering the financing of terrorism ("AML/CFT") laws, as well as the Office of Foreign Assets Control's ("OFAC") sanctions programs.

The United States has led the world in shaping international AML/CFT standards, and we encourage the Treasury Department to continue to take a global leadership role in proposing changes to enhance the systemic effectiveness and sustainability of the current regime. Accordingly, we commend the Treasury Department for undertaking this exercise to carefully assess the current AML/CFT and OFAC regulatory framework, which we believe is both timely and warranted. Treasury's review comes amidst a broad and emerging consensus that the AML/CFT regulatory regime is in urgent need of improvement.

As discussed in substantial detail in TCH's recently released report, *A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement*, the current AML/CFT regulatory regime needs to be redesigned in order to be more efficient and effective, with the goal of ultimately enhancing national security and law enforcement efforts to detect and address domestic and international money laundering and

[1] *See* Annex A to this letter for descriptions of the Associations.

terrorist financing.[2] That report, which reflects the input (and in many cases, explicit endorsement) of a wide range of stakeholders,[3] identifies a number of problems with the current BSA/AML framework and makes several recommendations for reform that would significantly improve the current regime's efficacy in apprehending criminals. Among the matters discussed in the report, we highlight six key principles that we suggest should guide the Treasury Department's review:

1. *Treasury, the Office of Terrorism and Financial Intelligence ("TFI"), and FinCEN should take a more prominent role in coordinating AML/CFT policy and examinations across the government and conduct a robust and inclusive annual process to establish AML/CFT priorities and provide an overarching purpose for the regime.*

2. *Treasury, TFI, and OFAC should take a more prominent role in coordinating sanctions policy across the government.*

3. *The public sector should continue to recognize, including in the examination context, that the AML/CFT and OFAC sanctions regimes are risk-based in nature and defer to institutions' judgments in this regard.*

4. *Treasury/TFI/FinCEN/OFAC, in coordination with the banking agencies, should communicate expectations clearly to the industry.*

5. *Treasury/TFI/FinCEN should significantly expand the ability of the private and public sectors to exchange information within and between each sector.*

6. *Treasury/TFI/FinCEN should encourage innovation and incorporate technological advances, including those related to data collection and analysis, into the regime to improve its efficacy and efficiency.*

To advance these key principles in the context of the Treasury Department's review, we make the following four specific recommendations for improving and redesigning the AML/CFT and OFAC regulatory frameworks:

- Treasury/TFI/FinCEN, as the agency entrusted with authority under the BSA, should communicate clear expectations to industry and other stakeholders, through regulations and guidance with respect to customer due diligence and related obligations;

---

[2] The TCH report is attached as Annex B to this letter. Similarly, FSR recently submitted to Treasury *Recommendations for Aligning Financial Regulation with Core Principles*, which also proposed changes to the AML/CFT regime and is available at http://www.fsroundtable.org/wp-content/uploads/2017/06/FSR-Letter-to-Treasury-on-Core-Principles-May-3.pdf.

[3] *See* TCH press release "The Clearing House Publishes New Anti-Money Laundering Report," (February 16, 2017), *available at* https://www.theclearinghouse.org/press-room/in-the-news/29170216%20tch%20aml%20cft%20report.

- Treasury/TFI/FinCEN should reform the BSA/AML reporting regime and expand information sharing authorities to enhance law enforcement's ability to apprehend criminals and counter terrorism in the 21st century;

- Treasury/TFI/FinCEN, in consultation with the federal banking agencies, should address the drivers of de-risking to prevent further damage to critical U.S. policy interests; and

- Treasury/TFI/OFAC should increase the efficiency and effectiveness of sanctions compliance, and further recognize a risk-based approach to compliance.

Each of these recommendations is described in further detail below. Collectively, these proposals would substantially enhance the efficiency and effectiveness of the current regime. Presently, financial institutions employ tens of thousands of people and invest billions of dollars annually in AML/CFT compliance.[4] However, many of the resources devoted to compliance have limited law enforcement or national security benefit, a direct result of the outdated and misaligned nature of the current regime. Redirecting those resources could substantially increase the national security of the country and the efficacy of its law enforcement and intelligence communities. The BSA was enacted at a time when banks were more alike than different. Restrictions on interstate banking meant that there were no truly national banks, and U.S. banks generally were not internationally active. However, today's customers and future customers increasingly use varying tools to conduct transactions with bank and non-bank financial institutions. Any revisions to the BSA/AML regime should be flexible enough to account for the changing ways in which customers interact with financial institutions. In addition, in light of the fact that the release "is issued for information and policy development purposes only," any changes to FinCEN regulations, forms or guidance documents made in response to this request should be subject to notice and comment under the Administrative Procedure Act. Furthermore, OFAC should, to the extent possible, engage in further dialogue with industry on current sanctions programs and their implementation.

I. Treasury/TFI/FinCEN, as the agency entrusted with authority under the BSA, should communicate clear expectations to industry and other stakeholders, through regulations and guidance with respect to customer due diligence and related obligations.

A. Background

Customer due diligence ("CDD") programs are considered a cornerstone of the U.S. BSA/AML regime. FinCEN and the federal banking agencies have incorporated CDD expectations into the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual* ("FFIEC Exam Manual") and provided guidance with regards to an institution's customer due

[4] *See* PwC Global Anti-Money Laundering, *available at* http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/anti-money-laundering.html ("According to new figures from WealthInsight, global spending on AML compliance is set to grow to more than $8 billion by 2017").

diligence policies, procedures, and processes. As the FFIEC Exam Manual states "[t]he objective of CDD should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage."[5] In addition to the pre-existing framework around CDD programs, in May 2016, FinCEN published its *Customer Due Diligence Requirements for Financial Institutions* final rule after a multiple yearlong rulemaking process. In the preamble, FinCEN notes its expectation that a covered institution's CDD program encompasses the following elements: "(i) customer identification and verification; (ii) beneficial ownership identification and verification; (iii) understanding the nature and purpose of customer relationships to develop a customer risk profile; and (iv) ongoing monitoring for reporting suspicious transactions and, on a risk-basis, maintaining and updating customer information."[6] It further acknowledges that the first element is already an established AML expectation under the final Customer Identification Program ("CIP") rule,[7] the second is a new regulatory requirement and the third and fourth, while an expected part of financial institution's suspicious activity reporting program, are formally codified by this regulation.

Since the release of the CDD rule, financial institutions have been working to implement the new components of the rule, which require them to make substantial changes to their AML compliance policies and procedures, including to the onboarding of new accounts and employee training practices as well as significant technological investments to incorporate the final rule into their current systems ahead of the May 2018 applicability deadline. The Associations recognize the importance of robust CDD processes and support Treasury's efforts to collect beneficial ownership information through other governmental mechanisms thereby "[i]ncreasing the transparency of U.S. legal entities through the collection of beneficial ownership information at the time of the legal entity's formation."[8] Furthermore, we agree with FinCEN's statement in the final rule that "[e]xpressly stating the [CDD] requirements facilitates the goal that financial institutions, regulators, and law enforcement all operate under the same set of clearly articulated principles."[9] Finally, there are many items in the final rule that we support, including FinCEN's

---

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

6 *See* 81 Fed. Reg. at 29,398.

7 *See* Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks ("CIP rule"), 12 CFR Part 21 (Office of the Comptroller of the Currency)("OCC"); 12 CFR Parts 208 and 211 (Board of Governors of the Federal Reserve System)("Federal Reserve"); 12 CFR Part 326 (Federal Deposit Insurance Corporation)("FDIC"); 12 CFR Part 748 (National Credit Union Administration)("NCUA"); and 31 CFR Part 1020.220 (FinCEN).

8 *See* 81 Fed. Reg. at 29, 401. *See also* The Clearing House Letter to Senators Grassley and Whitehouse and Representatives King and Maloney supporting beneficial ownership legislation, (August 8, 2016), *available at* https://www.theclearinghouse.org/-/media/tch/documents/research/articles/2016/08/20160808_tch_letter_incorporation_transparency_and_law_enforcement_assistance_act_support.pdf.

9 *See* 81 Fed. Reg. at 29, 449.

decision to not impose the beneficial ownership collection requirement retroactively and to link information updating requirements to triggering events.[10]

Below we set forth our concerns with FinCEN's recently finalized CDD rule, as well as with the broader regulatory framework around CDD obligations. With regards to FinCEN's final CDD rule, given that firms require time to incorporate any amendments into their programs, any changes to or further guidance on the rule should be made prior to the effective date, which in turn should be extended (and enforcement delayed) to allow ample time for the appropriate revisions to applicable processes and programs.

B. Burdens Imposed

Any CDD expectation should recognize that institutions' practices in conducting due diligence will differ based on the customers they serve, their lines of business, and the kinds of products and services they offer. Institutions should, therefore, be given considerable latitude in determining the appropriate level of CDD and designing monitoring systems to discover suspicious activity. Financial institutions should be expected to gather information that is needed to identify those customers that present the highest risk of money laundering, terrorist activity, or other criminal activity, so that monitoring resources can be focused on them rather than on lower risk customers.

As a general matter, there should be a three-tiered risk-based approach to CDD including: (i) basic identification of the customer, which would apply to all customers and would consist of collecting enough information to allow a financial institution to form a reasonable belief as to the identity of the customer; (ii) basic due diligence, which would apply to all customers and consist of collecting sufficient information to enable the institution to conduct a risk analysis of the customer to categorize the level of risk the customer presents to the institution; and (iii) enhanced due diligence ("EDD"), which would be required for certain customers considered to be high risk for money laundering and terrorist financing.[11] However, current CDD expectations are inconsistent across the federal banking agencies and generally lack a risk-based component. Notably, enforcement actions have been issued that require banks to include in their CDD processes information regarding a customer relationship across all lines of business, which is extremely difficult to implement for large organizations that operate in multiple jurisdictions and encounter legal barriers to the development of such an understanding. FinCEN, in consultation with the federal banking regulators, should further tailor CDD and related expectations to be more risk-based and applicable in a domestic context only, given the legal barriers to extraterritorial application.

---

[10] *See* 81 Fed. Reg. at 29, 410, which states that "FinCEN does expect financial institutions to update this [beneficial ownership equity prong] information based on risk, generally triggered by a financial institution learning through its normal monitoring of facts relevant to assessing the risk posed by the customer."

[11] *See* TCH Letter to the Basel Committee on Banking Supervision "Re: Comment Letter on Consultative Paper, Sound Management of Risks Related to Money Laundering and Financing of Terrorism," (September 27, 2013), *available at* https://www.theclearinghouse.org/-/media/files/association%20documents/20130927%20comments%20to%20basel%20on%20money%20laundering.pdf.

We recommend changes to the CIP rule, which is also the first prong of a CDD program as described by FinCEN in the final rule, in order to account for technological developments since the CIP rule's inception. Currently, under the CIP rule, financial institutions may use third parties to collect CIP information for credit card accounts and to verify information via non-documentary means for all account types.[12] Therefore, for accounts other than credit card accounts, financial institutions must obtain identifying information under the CIP collection prong directly from account holders. However, consumer demand for faster account opening periods via FinTech companies or mobile applications are placing greater demands on financial institutions to collect such information quickly without sacrificing data quality. Expanding an institution's ability to engage third parties for the collection of customer information could assist with this technologically-driven development. Therefore, we recommend that the Treasury Department, in concert with the relevant federal functional regulators, amend the CIP regulations, with appropriate controls in place, to allow financial institutions to engage third parties to collect CIP information for all account types.

Furthermore, FinCEN's final CDD rule should be amended to (i) allow financial institutions to identify beneficial owners on a per-customer, rather than per-account, basis; (ii) exclude from the definition of "legal entity customer" entities that are counterparts of U.S. publicly traded companies or registered and licensed under foreign laws comparable to those enumerated in the CDD rule; and (iii) affirm FinCEN's, rather than the federal functional regulators', ultimate authority to determine CDD standards.

The Treasury Department should amend the final CDD rule to require beneficial ownership collection *on a risk-based basis* when an existing customer opens a new account, similar to the CIP rule. Institutions would still collect and retain beneficial ownership information for covered legal entity customers. Currently, financial institutions have holistic periodic KYC review processes into which they are currently working to incorporate this new beneficial ownership information collection requirement. However, the final rule's provision that a covered financial institution *identify the beneficial owners of an existing customer each time that same customer opens another account*, places undue burdens on institutions in various contexts. The rule states that "the opening of a new account is a relatively convenient and otherwise appropriate occasion to obtain current information regarding a customer's beneficial owners."[13] We find this assertion problematic, particularly in situations where beneficial ownership information has been collected and there is no triggering event or other risk-indicator to suggest that such information needs to be re-certified when a new account is opened. An example of this is when a large corporate client opens hundreds of accounts at once or over a span of a few days, which would require the customer each time to certify beneficial ownership information *for the same legal entity*.

Once a financial institution has identified the beneficial owners of a legal entity customer, the opening of a new account by that customer should not automatically trigger a requirement to

---

12 *See* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, "Customer Due Diligence–Overview," p. 48, fn. 46.

13 *See* 81 Fed. Reg. at 29,406.

re-identify the beneficial owners. Rather, a financial institution should be able to determine, consistent with the risk-based approach, whether re-identification is necessary based on whether it has a reasonable belief that it has identified the customer's current beneficial owners by ownership criteria at least as stringent as those required by the final rule. We note that this approach is also consistent with the approach taken by FinCEN and the federal banking agencies in the final CIP rule as the definition of customer for purposes of the CIP requirement expressly excludes "a person that has an existing account with the bank, provided the bank has a *reasonable belief* that it knows the true identity of the person" (emphasis added).[14]

Furthermore, while FinCEN's final CDD rule expands the types of entities excluded from the beneficial ownership collection requirement, it does not exclude entities listed on foreign exchanges from the definition of "legal entity customer."[15] The final rule's preamble notes that "[n]umerous commenters urged FinCEN to broaden the proposed exemptions for regulated financial institutions and publicly traded companies in the United States to include their counterparts outside of the United States." FinCEN also notes its agreement with commenters' views that an exclusion should apply to certain foreign financial institutions where information regarding their beneficial ownership and management is available from the relevant foreign regulator, but stays silent on why the agency declined to further exempt counterparts of U.S. publicly traded companies or entities listed on foreign exchanges more broadly.[16]

This position appears to deviate from current practice. The USA PATRIOT Act's foreign bank certification, which seeks to ensure that U.S. financial institutions do not establish correspondent accounts for foreign shell banks, exempts financial entities from the certification requirement when they are "traded on an exchange or an organized over-the-counter market that is regulated by a foreign securities authority as defined in section 3(a)(50) of the Securities Exchange Act of 1934."[17] Using this rationale, FinCEN should further modify the final rule to exclude entities listed on foreign exchanges that are regulated by a foreign securities authority, as defined by section 3(a)(50) of the Securities Exchange Act of 1934.

Additionally, the final rule's preamble affirms the authority of the federal functional regulators to "establish AML program requirements in addition to those established by FinCEN that they determine are necessary and appropriate to address risk or vulnerabilities specific to the financial institutions they regulate."[18] As discussed in both TCH's response to the 2014 notice of proposed rulemaking for the CDD rule and above, BSA compliance examinations should be conducted under standards clearly set by FinCEN and not subject to interpretive discretion by the

---

14 *See* 31 C.F.R. § 1020.100(c)(2)(iii).

15 We note that it also did not provide additional guidance on regulatory expectations around "verifying" when an entity is excluded.

16 *See* 81 Fed. Reg. 29414-29415.

17 *See* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, "Foreign Correspondent Account Recordkeeping, Reporting, and Due Diligence – Overview," p. 112, footnote 121.

18 *See* 81 Fed. Reg. 29,403-29,404.

federal functional regulators.[19] Disparate interpretations and multiple public sector actors create confusion among institutions and inconsistent expectations. Furthermore, the various actors are further incentivized by their statutory remits. Federal banking agency examiners are focused on evaluating BSA/AML policies, procedures and processes at the institutions they supervise in the context of safety and soundness considerations, whereas Treasury and law enforcement officials are focused on using the information supplied by financial institutions to mitigate domestic and international illicit finance threats. Therefore, the Treasury Department, through TFI, should take a more prominent role in coordinating AML/CFT policy across the government to improve prioritization and provide an overarching purpose for the AML/CFT regime. This leadership role should extend to establishing definitive CDD standards to be faithfully implemented by the banking agencies.

In addition, we have concerns related to the fourth prong of a CDD program as established by FinCEN in the final rule – conducting ongoing monitoring for reporting suspicious transactions and, on a risk-basis, maintaining and updating customer information. The final rule cites provisions in the FFIEC Exam Manual around ongoing monitoring, stating that "[b]anks are expected to have in place internal controls to 'provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.'"[20] The banking agencies also provided additional guidance related to transaction monitoring and filtering systems that Treasury's CDD rule appears to incorporate.[21] Given Treasury's decision to formally codify this expectation and its underlying elements within the final CDD rule, we raise our concerns with the current regulatory burdens associated with the requirements set forth in the FFIEC Exam Manual and the federal banking agencies' guidance herein.

Financial institutions employ robust transaction monitoring and filtering programs to detect potentially suspicious transactions, among other items. These alerts are then further investigated and, in some instances, result in SARs. However, current regulatory expectations require financial institutions to monitor transactions for "normal and expected" activity, which is generally provided by the customer at account opening, and therefore could differ from the

---

19 *See* The Clearing House Letter to FinCEN, Re: Notice of Proposed Rulemaking–Customer Due Diligence Requirements for Financial Institutions (RIN 1506-AB-25), (October 3, 2014), *available at* https://www.theclearinghouse.org/-/media/files/association%20related%20documents/20141003%20tch%20comments%20to%20fincen%20on%20cdd.pdf.

20 *See* 81 Fed. Reg. 29420. *See also* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, "BSA/AML Compliance Program–Overview," p. 29-30.

21 The FFIEC Exam Manual provides further guidance on transaction monitoring and filtering program parameters. In addition, financial institutions have also been using the 2011 Board of Governors of the Federal Reserve System Supervisory Letter 11-7/ Office of the Comptroller of the Currency Bulletin 2011-12, Supervisory Guidance on Model Risk Management ("Model Risk Management Guidance"), to determine what BSA/AML tools, if any, would be considered models within the scope of the guidance due to increased regulatory attention in this regard.

actual activity conducted throughout the customer relationship as behavior and financial needs evolve over time.[22]

Transaction monitoring should be focused on actual activity and the evolving nature of the customer relationship, allowing financial institutions to better allocate the appropriate monitoring resources and therefore provide more meaningful information to law enforcement through SAR filings, as generally, institutions' scenarios are calibrated to detect unusual activity patterns. Furthermore, institutions continue to encounter supervisory and examination constraints around the ability to tune transaction monitoring scenarios consistent with the risk-based AML/CFT framework. As discussed in the TCH AML/CFT report "examiners have developed expected ratios of alerts to SARs, though such ratios have never been published for notice and comment."[23] This impacts the incentive structure of the SAR regime as described in the next section and notably dissociates it from an institution's ability to provide targeted leads to law enforcement.

Because of their role in examining financial institutions for BSA/AML compliance, pursuant to the authority delegated by Treasury, the banking agencies have applied their general Model Risk Management Guidance specifically to BSA/AML tools and models, despite the fact that the guidance does not explicitly provide that it is applicable to such tools. Further, the banking agencies have applied this guidance on an inconsistent basis, creating diverse practices throughout the industry.[24] Notably, many of these concerns are, at least in part, driven by institutions' inability to innovate within the current regulatory framework, thereby preventing them from testing, in silos that are separate from their traditional programs and thus not subject to "grading" under the formal examination process, new approaches and technology for transaction monitoring. This would assist institutions in developing better monitoring and other tools to provide more useful leads to law enforcement.[25]

Therefore, Treasury, in consultation with the federal banking agencies, and in accordance with the risk-based nature of the BSA/AML regime, should promulgate guidance that explicitly allows financial institutions to (i) monitor transactions for actual activity versus "expected" or

---

22 *See* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, "Customer Due Diligence–Overview," p. 57.

23 *See* Annex B for further discussion of this issue, pg. 7; direct reference to this example provided on pg. 27, endnote 4.

24 As discussed in footnote 21, banks have long been subject to federal banking agency guidance to determine what BSA/AML tools, if any, would be considered models within the scope of the Model Risk Management Guidance due to increased regulatory attention in this regard. Consistent with the Model Risk Management Guidance, clear processes generally exist within organizations to identify in-scope BSA/AML models and those processes are influenced by each institution's tailored BSA/AML compliance program, thereby creating a diverse set of industry approaches to BSA/AML models and model validation. Furthermore, neither the Guidance nor the BSA/AML Manual provides clear criteria to establish that a particular tool is not a model, which has contributed to the diverse set of BSA/AML model validation approaches among member banks, and more importantly, a diverse set of exam approaches regarding the BSA/AML tools that are considered outside the scope of the Model Risk Management Guidance.

25 *See* 31 U.S.C. § 5311 which state that the BSA's recordkeeping and reporting regime is meant to provide information that has a "high degree of usefulness" to the government.

anticipated activity; (ii) review and test monitoring scenarios periodically; (iii) tune scenarios to further increase their efficiency and effectiveness in identifying suspicious transactions and thereby information useful to law enforcement; and (iv) further innovate within such programs.

Finally, general customer due diligence expectations to screen politically exposed persons ("PEPs") should be tailored. In January 2001, the Treasury Department, along with the federal banking agencies and others issued guidance on managing the risks associated with senior foreign political figures, their families, and their associates.[26] Since then, very little additional guidance has been promulgated thereby making current regulatory expectations regarding PEP identification and screening overly expansive and applicable to individuals that are not considered "high-risk." Furthermore, other jurisdictions, notably the United Kingdom, have recently issued guidance further narrowing the definition of a PEP and including generally applicable timeframes for consideration of an individual as a PEP. The UK guidance states that "A PEP is defined as '*an individual who is or has, at any time in the preceding year*, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person.' This definition only applies to those holding such a position in a state outside the UK, or in a Community institution or an international body. Although under the definition of a PEP, an individual ceases to be so regarded after he has left office for one year, firms are encouraged to apply a risk-based approach in determining whether they should cease carrying out appropriately enhanced monitoring of his transactions or activity at the end of this period. In many cases, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately abated" (emphasis added).[27] Therefore, consistent with a risk-based approach and in line with other jurisdictions, FinCEN, in consultation with the federal banking agencies and other public sector stakeholders, should issue revised guidance (i) narrowing the definition of a PEP and explicitly recognizing that an individual ceases to be a PEP one year after having left office, absent a contrary determination by the firm using a risk-based approach; and (ii) recognizing that due diligence on PEPs is not "one-size-fits-all," and that the level of due diligence with respect to any given PEP

---

[26] *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* https://www.treasury.gov/press-center/press-releases/Pages/guidance.aspx.

[27] *See* The Joint Money Laundering Steering Group, Prevention of money laundering/combatting terrorist financing (2014 Revised Version), *available at* http://www.jmlsg.org.uk/download/9803, pg. 111; 5.5.19 and 5.5.20. *See also* The UK's Financial Conduct Authority's finalized guidance, FG 17/5 The treatment of politically exposed persons for anti-money laundering purposes, (July 2010), *available at* https://www.fca.org.uk/publication/finalised-guidance/fg17-05.pdf, pg. 7; 2.19. We note that the FCA PEP Guidance also discusses: (i) treatment of family members of PEPs (2.24); (ii) lists examples of who should be treated as a PEP (2.16); (iii) notes that the definition of a known close associate of a PEP includes "an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relationship with a politically exposed person" or "an individual who has sole beneficial ownership of a legal entity or a legal arrangement that is known to have been set up for the benefit of a PEP" (2.25); and (iv) that "a known close associate of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP" (2.26).

should be commensurate with the risks presented by that PEP and the nature of the customer relationship.[28]

C. Recommendations

In order to provide additional clarity, reduce unnecessary burdens and promote consistency within the AML/CFT regime, the Treasury Department, through FinCEN and in consultation with the federal banking agencies where applicable, should modify CDD expectations by:

- Further tailoring CDD and related expectations to be more risk-based and applicable in a domestic context only, given the legal barriers to extraterritorial application;
- Amending the CIP regulations, with appropriate controls in place, to allow financial institutions to engage third parties to collect CIP information for all account types;
- Making the following changes to FinCEN's final CDD rule:
  - Allowing financial institutions to identify beneficial owners on a per-customer basis and not a per-account basis;
  - Excluding from the definition of legal entity customer entities registered and licensed under foreign laws comparable to those enumerated in the final rule; and
  - Affirming FinCEN's, rather than the federal functional regulators', ultimate authority to determine CDD standards;
- Promulgating transaction monitoring and filtering and model validation regulations or guidance that explicitly allows financial institutions to:
  - Monitor transactions for actual activity versus "expected" or anticipated activity;
  - Review and test monitoring scenarios periodically;
  - Tune scenarios to further increase their efficiency and effectiveness in identifying suspicious transactions and thereby information useful to law enforcement; and
  - Further innovate within such programs; and
- Revising current PEP guidance to:
  - Narrow the definition of a PEP and explicitly recognize that an individual ceases to be a PEP one year after having left office, absent a contrary determination by the firm using a risk-based approach; and

[28] Of course, consistent with obligations under Section 312.

- Recognize that due diligence on PEPs is not "one-size-fits-all," and that the level of due diligence with respect to any given PEP should be commensurate with the risks presented by that PEP and the nature of the customer relationship.

As financial institutions are currently working to implement the final CDD rule, any changes to the rule should be made prior to the effective date, which should be extended (and enforcement delayed) to allow ample time for the appropriate revisions to applicable processes and programs.

II. Treasury/TFI/FinCEN should reform the BSA/AML reporting regime and expand information sharing authorities to enhance law enforcement's ability to apprehend criminals and counter terrorism in the 21st century.

A. Background

As discussed in the previous section, financial institutions have a statutory obligation under the BSA to provide leads to law enforcement. 31 U.S.C. § 5311 states that the BSA's recordkeeping and reporting regime is meant to provide information that has a "high degree of usefulness" to the government. BSA reporting requirements include Currency Transaction Reports ("CTRs"), Suspicious Activity Reports ("SARs"), and Foreign Bank and Financial Accounts Reports ("FBARs"), among others. The discussion below primarily focuses on changes that could be made to the CTR and SAR frameworks to enhance the effectiveness and efficiency of the reporting regime.

As an initial matter, a financial institution must electronically file a CTR for 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."[29] CTRs have seen various iterations since their inception, however, currently over 15 million CTRs are filed in the United States per year.[30]

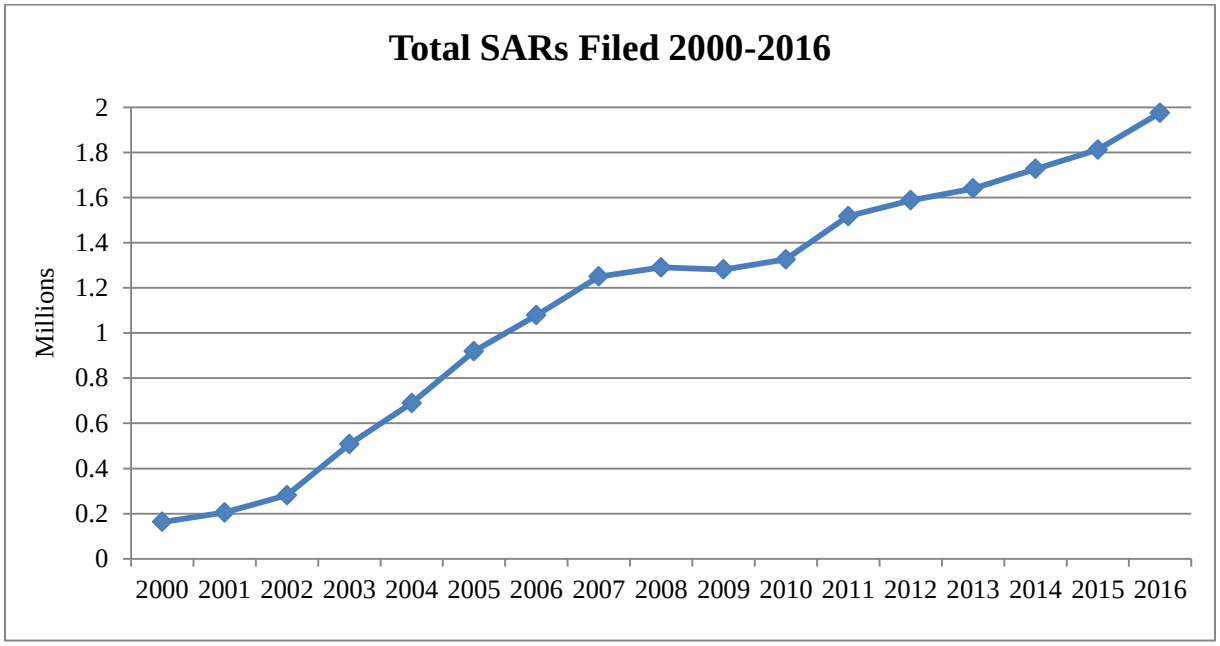
Furthermore, in April 1996 the SAR regime went into effect. As required by the BSA, its intended use is to allow financial institutions to submit leads on "suspicious activity" to law enforcement. Current regulations dictate that, financial institutions are required to file a SAR on criminal violations that: (i) involve insider abuse; (ii) total at least $5,000 in which a suspect can be identified; or (iii) total at least $25,000, regardless of whether a suspect can be identified; *as well as* 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;

---

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

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

(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. Over the last 16 years, the number of SARs filed has grown astronomically, reaching almost 2 million in 2016, as shown below.[31]



The reasons for this exponential growth are due in part to defensive SAR filings by institutions out of an abundance of caution and fear of regulatory criticism. Furthermore, the current system does not include mechanisms for law enforcement feedback on the SARs filed, which could assist financial institutions in refining their SAR filings accordingly to provide information that is of the greatest use to law enforcement.

Financial institutions are motivated to assist the government in understanding and identifying financial crime and are constantly working to develop new methods to thwart money laundering and terrorist financing. They use diverse investigative methods, including through the establishment of financial intelligence units ("FIUs"), to assist them in their efforts to provide leads to law enforcement. Many large financial institutions operate FIUs, which are generally staffed by former law enforcement personnel with significant expertise and strong motivations to help their former colleagues in the government. They typically have broad mandates to evaluate client relationships and the risks they may pose to the institution and the financial system itself. FIUs are most effective when they can be agile and adapt in real-time to threats as they develop, which is paradoxical to the SAR regime.

---

[31] *See* The Heritage Foundation, Backgrounder No. 3157, "Financial Privacy in a Free Society," Table 1: Suspicious Activity Reports and Cash Transaction Reports, 2000–2015," at 10, (September 23, 2016), *available at* http://thf-reports.s3.amazonaws.com/2016/BG3157.pdf. 2015 and 2016 SAR data acquired from FinCEN's SAR Stats, *available at* https://www.fincen.gov/reports/sar-stats.

B. Burdens Imposed

As an initial matter, we propose a review of the BSA/AML reporting regime in order to de-prioritize the investigation and reporting of activity of limited law enforcement or national security consequence. The current regime is built on bilateral reporting mechanisms (i.e. CTRs and SARs), grounded in the analog technology of the 1980s, rather than the more interconnected and technologically advanced world of the 21st century. Many of our recommendations below are intended to modernize this paradigm. In addition, the current regime does not appropriately prioritize information that is of the most use to law enforcement. Given the number of CTRs and SARs that are filed annually, and the financial institution resources that are dedicated to these efforts, further streamlining expectations could allow for the redistribution of AML/CFT resources to areas of greater efficiency and effectiveness. In addition, Treasury, in coordination with the federal banking agencies, should encourage innovation and further incentivize institutions to provide useful information to law enforcement, including by providing institutions with "credit" in the examination and enforcement context.[32]

CTR expectations impose significant requirements on financial institutions, notably the aggregation component, given the changes to the nature of customer activity since the inception of the program. This requirement becomes particularly difficult given the broad regulatory language that an institution is expected to file a CTR if it "has knowledge that [the multiple transactions] are *by or on behalf of* any person and result in either cash in or cash out totaling more than $10,000 during any one business day" (emphasis added).[33] We note that while financial institutions have avenues to pursue CTR filing exemptions, the regulatory framework surrounding such exemptions is so burdensome that they typically opt to instead continue to file CTRs. Therefore, we support streamlining CTR expectations as, when coupled with the SAR regime, many may be of low law enforcement or national security value.

Furthermore, the ideal SAR is a well-researched, carefully-written summary of suspicious activity, which requires significant employee time and effort to produce. Yet, the current regime promotes the filing of SARs that may never be read, much less followed up on as part of an investigation. As described above, in the current regulatory and enforcement climate, compliance officers have powerful incentives to trigger as many alerts and file as many SARs as possible, because those "defensive" SAR filings protect them (and their examiners) in the event that the financial institution is used by the companies or individuals ultimately found to have committed a crime. What gets measured gets done, and under the current regime, providing valuable intelligence to law enforcement or national security agencies does not get measured; writing policies and procedures and filing SARs does.[34] So, almost two million SARs are filed

---

32 *See* Annex B for further discussion of the misalignment in the current BSA/AML exam and incentives structure in the United States, pg. 7-8.

33 *See* 31 CFR § 1010.313 (2011). *See also* FinCEN Guidance, "Currency Transaction Report Aggregation for Businesses with Common Ownership," (March 16, 2012), *available at* https://www.fincen.gov/sites/default/files/shared/FIN-2012-G001.pdf.

34 *See* article by Bob Werner and Sabreen Dogar, "Strengthening the Risk-Based Approach," in TCH Q3 2016 Banking Perspectives issue; *available a*: https://www.theclearinghouse.org/research/banking-perspectives/2016/2016-q3-banking-perspectives/strengthening-the-rba.

per year. There are two embedded issues that contribute to this trend: the first is the type of conduct that merits a SAR filing; the second is the level of suspicion or evidence of that conduct that should trigger a filing. As described above, financial institutions are required to file a SAR based on two broad categories of conduct.

Therefore, we provide the following thoughts on the current regulatory framework governing SAR submissions. First, the filing of SARs is required for "transactions with no apparent economic, business, or lawful purpose."[35] Given the various incentives discussed above and those embedded in the transaction monitoring and filtering requirements applied through CDD expectations, FinCEN should clarify this filing requirement. SARs should not be filed simply because a transaction appears to have no economic, business or lawful purpose, without a further link to suspicious activity. Broad interpretations of this provision have contributed to the culture of defensive SAR filings. In addition, FinCEN should eliminate the requirements to file SARs (i) when there are single instances of structuring activity and (ii) under the 90 day continuing activity review requirements. In single instances of structuring, such activities are generally not indicative of illicit activity. In addition, given the robust program controls employed by financial institutions, continuing activity reviews add little value and generally serve the same purpose as transaction monitoring alerts. Finally, FinCEN should substantially reduce the number of fields deemed "critical" to SAR and CTR filings, as each one imposes associated regulatory expectations and burdens with varying benefits.

As part of the review of the regime, FinCEN should review, revise or retract as necessary all existing SAR guidance to ensure it establishes appropriate priorities and communicates clear expectations to financial institutions. For example, FinCEN should reconsider its October 2016 "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime" (the "Cyber Advisory"). Institutions are facing significant challenges in working to implement the Cyber Advisory and have considerable concerns that have yet to be resolved, including: the overbroad definition of "transaction;" the absence of an agreed method of determining "funds at risk" and thereby ensuring compliance with dollar reporting thresholds; elimination of the requirement that there be a transaction associated with the reportable event as has customarily been the case in FinCEN's SAR rules; the likely diminished law enforcement value of the resulting reports as a function of both increased volume and lower quality content in addition to the repetition of information that is also likely provided to the Financial Services Information Sharing and Analysis Center ("FS-ISAC"); and other compliance implications including the cost of implementation.

Similarly, FinCEN should also reconsider its September 2016 "Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes" (the "E-Mail Advisory"). We note that it does not appear to take into account the degree of automation in funds transfers that is necessary to execute large volumes of payments quickly and efficiently and is therefore inconsistent with

---

[35] The relevant SAR filing category is discussed in this letter. However, we note that 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."

the current state of commercial funds transfer processing. Specifically, many of the "red flags" included in the E-Mail Advisory suggest that a financial institution ought to have front-end anomaly detection for funds transfers, which is not feasible without one-by-one reviews of the circumstances surrounding each payment instruction a customer sends. Not only is such a review incompatible with the volume and speed of commercial activity, but it is also contrary to the after-the-fact nature of transaction monitoring and reporting that is core to AML programs. It should be noted that the vast majority of these frauds are authorized transactions (i.e., authorized and authenticated through security procedures agreed between a financial institution and its customer) and the legal framework that sets the responsibilities and liabilities of parties to the payments does not require institutions to undertake the kinds of review required to identify the advisory's "red flags." Therefore, financial institutions should not be expected to incorporate the "red flags" into their AML programs, but should instead use them on a risk-basis to further their investigations.

If instead, there was a system that facilitated real-time information flow and analysis using modern data capabilities, while adhering to privacy and civil liberty concerns as well as managing for other risks, then perhaps it could counter and potentially mitigate some of the challenges institutions currently face in implementing SAR regulations and guidance, such as FinCEN's Cyber and E-Mail Advisories. The provision of raw data to FinCEN has been considered before – though in a limited capacity.[36]

In this instance, the ideal outcome is not each institution analyzing bulk data for a given customer and using resources to aggregate CTR information or draft an elaborate and heavily audited SAR narrative. Rather, a middle ground would be a utility that allows institutions to share bulk data and have it analyzed. An alternative approach would be to have bulk data deposited at FinCEN and analyzed by law enforcement and intelligence community professionals, with a mechanism for regular feedback to be provided to institutions to enable them to target their internal monitoring and tracking mechanisms to better serve the goals of law enforcement and intelligence officials. Providing such data on suspicious activity in bulk directly to FinCEN would modernize the SAR regime from one built for the 20th century, where financial institutions were generally equipped to filter data, to one appropriate for the 21st century, where big data analytics could enable law enforcement to effectively sift through data without requiring as much assistance from financial institutions in investigating illicit activity. Policymakers should consider this as part of their review of the BSA/AML reporting regime.

Furthermore, as the current SAR regime is supported by institutional investigations, policymakers should better protect SAR investigatory information from discovery given some recent court decisions that "information that would reveal the existence of a SAR" does not

---

[36] In 2006, FinCEN published a Congressional report on the Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the BSA in compliance with Section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004. At the time, the report found that simply implementing a cross-border funds transfer reporting requirement would require significant investment from both the public and private sectors. In particular, it was estimated that FinCEN would need approximately $32.6 million and three and a half years to make sure its system was capable of receiving such information. However, in 2015, FinCEN completed an IT Modernization Project that has likely impacted that original estimate.

cover certain investigatory materials.[37] The disclosure of SAR information in private litigation could undermine the ability of financial institutions to effectively combat financial crimes by compromising ongoing investigations, chilling financial institutions' willingness to file detailed SARs, and revealing financial institutions' processes for analyzing and reporting such data. Thus, further legislative or executive action could help both to allow financial institutions to continue filing the most helpful SARs possible and protect bad actors from discovering their methods for doing so. One approach would be for FinCEN, in consultation with the federal financial regulators, to issue guidance that would make clear that SAR investigatory materials are to be treated as confidential, particularly in private litigation.[38]

In addition, barriers to SAR sharing should be removed in order to further facilitate enterprise-wide and cross-border sharing of suspicious activity information.[39] There are inarguable benefits to removing these barriers and we note that many authorities, including the FATF, are working to further promote information sharing within and between financial institutions. Treasury should continue to advocate for the adoption of policies that apply a substantially consistent standard for information sharing among jurisdictions. We note that FATF's recently released *Draft Guidance for Private Sector Information Sharing* highlights the importance of information sharing, including that sharing underlying SAR information "is required for an effective group-wide compliance programme."[40] FinCEN's rules permit SAR sharing within U.S. financial institutions' corporate organizational structure for purposes consistent with the BSA as determined by regulation or guidance. In 2006, FinCEN and the federal banking agencies issued guidance providing that a U.S. depository institution may share SAR information with its controlling company (whether foreign or domestic), and that a U.S. branch or agency of a foreign bank may share SAR information with its foreign head office.[41] FinCEN reaffirmed portions of this guidance in 2010 when it issued new guidance permitting U.S. depository institutions to share SAR information with affiliates subject to U.S. SAR regulations.[42]

---

37 *See* Annex B for further discussion of court decisions that have interpreted "information that would reveal the existence of a SAR" to exclude SAR investigatory materials, pg. 20-22.

38 Alternatively, Congress could enact legislation to this end.

39 *See* Annex B for further discussion of barriers to cross-border information sharing, pg. 16-18. *See also* The Clearing House Letter to Former FinCEN Director Jennifer Shasky Calvery, Re: Improving the Ability of Banking Organizations to Use Suspicious Activity Report Information for Enterprise-wide AML Compliance Purposes, (March 13, 2015), *available at* https://www.theclearinghouse.org/-/media/files/association%20related%20documents/20150313%20cross%20border%20sar%20letter.pdf.

40 *See* the Financial Action Task Force's *Draft Guidance for Private Sector Information Sharing* at pg. 11, *available at* http://www.fatf-gafi.org/media/fatf/documents/publicconsultation/Consultation-Guidance-Private-Sector-Information-Sharing-Jun17.docx.

41 *See* Interagency Guidance, "Sharing Suspicious Activity Reports with Head Offices and Controlling Companies," (January 20, 2006), *available at* https://www.fincen.gov/resources/statutes-regulations/guidance/interagency-guidance-sharing-suspicious-activity-reports.

42 *See* FinCEN Guidance "Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates," (November 23, 2010), *available at* https://www.fincen.gov/sites/default/files/shared/fin-2010-g006.pdf.

Accordingly, FinCEN, in consultation with the federal banking agencies, should clearly authorize U.S. financial institutions to share SARs with a foreign branch or affiliate, in countries that have complementary AML/CFT regimes and practices, as determined by the public sector. Furthermore, FinCEN should confirm that when information from underlying facts, transactions, or documents have been included in a SAR, it does not cause that information to fall under the general prohibition against disclosing a SAR or information that would reveal the existence of a SAR.

Further improving information sharing within the regime would also enable institutions to develop a more holistic view of potential threats, thereby allowing them to provide law enforcement with more useful data. Thus, FinCEN should clarify and expand the voluntary information sharing program established by Section 314(b) of the USA PATRIOT Act. Section 314(b) allows financial institutions to voluntarily share with each other information relevant to potential money laundering or terrorist financing investigations. In 2009, FinCEN issued guidance explaining that financial institutions are covered by the safe harbor provisions of Section 314(b) when they participate in a program that "share[s] information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities ('SUAs')" as long as the purpose of the information sharing is to identify and report activities that may involve terrorist activity or money laundering.[43] However, this standard is vague and limited given the illicit finance risks facing financial institutions. Such sharing, whether through utilities or other mechanisms, should be permissible even before there is already-formed, formal suspicion of money laundering or terrorist financing. Relatedly, FinCEN should: (i) clarify that financial institutions can discuss the filing of a SAR when they are working on a case of mutual interest; and (ii) encourage financial institutions to jointly file SARs as applicable. Currently, financial institutions can jointly file SARs, but given regulatory mandates around an institutions' ability to discuss SAR filings with each other, they have generally not utilized such authorities.

Finally, as a result of a streamlining of the BSA/AML reporting regime as described above, financial institutions would then have the flexibility to allocate various AML/CFT resources to high-priority threat mitigation areas. Therefore, Treasury should propose a rule stating that where applicable, financial institutions are encouraged to innovate in an FIU "sandbox" outside the strictures of regular BSA/AML policies, procedures and examinations in order to develop new and better ways to deliver substantive leads to law enforcement.

C. Recommendations

In order to strengthen the United States' AML/CFT regime and eliminate burdens that do not enhance the regime's effectiveness, Treasury/TFI/FinCEN should revise and streamline the current BSA/AML reporting regime, in consultation with the federal banking agencies and law enforcement. We support public sector efforts to:

---

[43] In a 2012 administrative ruling, FinCEN elaborated on this guidance and distinguished between information sharing that satisfies the purpose if this authority and other sharing arrangements that are not covered by Section 314(b).

- Conduct a review of the current BSA/AML reporting regime and de-prioritize the investigation and reporting of activity of limited law enforcement or national security consequence, while increasing the feedback from law enforcement, to allow financial institutions to re-allocate resources to higher value AML/CFT efforts;

- Encourage innovation and further incentivize institutions to provide useful information to law enforcement, including by providing institutions with "credit" in the examination and enforcement context;

- Streamline CTR expectations as, when coupled with the SAR regime, many may be of low law enforcement or national security value;

- Provide guidance further clarifying that a SAR is not required simply because a transaction appears to have no economic, business or lawful purpose;

- Eliminate requirements to file SARs when there are single instances of structuring activity and under the 90 day continuing activity review requirements;

- Substantially reduce the number of fields deemed "critical" to SAR and CTR filings, as each one imposes associated regulatory expectations and burdens with varying benefits;

- Review, revise or retract as necessary all existing SAR guidance to ensure it aligns with the priorities of law enforcement and the regime more broadly and clearly communicates expectations to institutions, including FinCEN's 2016 E-mail Compromise and Cyber Advisories;

- Further facilitate the provision of raw data from financial institutions to law enforcement;

- Provide guidance that further clarifies that SAR investigatory materials are to be treated as confidential, particularly in private litigation;

- Remove barriers to SAR sharing in order to further facilitate enterprise-wide and cross-border sharing of suspicious activity information by:

    - Clearly authorizing U.S. financial institutions to share SARs with a foreign branch or affiliate, in countries that have complementary AML/CFT regimes and practices, as determined by the public sector;

    - Confirming that when information from underlying facts, transactions, or documents have been included in a SAR, it does not cause that information to fall under the general prohibition against disclosing a SAR or information that would reveal the existence of a SAR; and

    - Encouraging other jurisdictions to adopt policies that apply a substantially consistent standard;

- Expand the voluntary USA PATRIOT Act's Section 314(b) safe harbor provision to address barriers to information sharing;

- Clarify that financial institutions can discuss the filing of a SAR when they are working on a case of mutual interest and encourage financial institutions to jointly file SARs as applicable; and

- Propose a rule encouraging financial institutions to innovate in an FIU "sandbox" and that FIUs may operate outside the strictures of regular BSA/AML policies, procedures and examinations.

III. Treasury/TFI/FinCEN, in consultation with the federal banking agencies, should address the drivers of de-risking to minimize further damage to critical U.S. policy interests.

A. Background

The USA PATRIOT Act and the Treasury Department's implementing regulations impose significant requirements on U.S. banks with respect to their correspondent banking activities, including: (i) insuring that services are not being used to indirectly provide banking services to foreign shell banks;[44] (ii) obtaining ownership information for private foreign banks;[45] (iii) applying risk-based due diligence policies, procedures and controls to correspondent accounts maintained for foreign financial institutions;[46] and (iv) undertaking enhanced due diligence with respect to accounts maintained for high risk foreign banks.[47]

Correspondent banking is an integral part of the international payments system, but we also recognize that the nature of correspondent banking makes the system uniquely vulnerable to criminal activity, including, in particular, money laundering and terrorist financing activities. In the international attempt to balance these competing attributes, the de-risking phenomenon has been widely discussed as a serious problem that threatens to hinder financial inclusion and drive money laundering and terrorist financing into informal, less secure and less visible channels. In July 2017, the Financial Stability Board submitted a report to the G20 noting that correspondent banking relationships ("CBRs") continue to decline around the world. The report states that "[a] range of reasons explain the terminations of CBRs, including industry consolidation, lack of profitability, the overall risk appetite, and various causes related to anti-money laundering and countering the financing of terrorism (AML/CFT) or sanctions regimes. The countries where financial institutions are most affected by exits of foreign correspondent banks tend to be small

---

44 31 C.F.R. § 1010.630.

45 *Id.*

46 31 C.F.R. § 1010.610.

47 *Id.*

economies or jurisdictions for which the compliance with AML/CFT standards is insufficient or unknown."[48]

Association members operate a significant portion of the correspondent banking network worldwide and recognize the importance of correspondent banking to the smooth functioning of the international financial system.[49] We share the concerns around de-risking in correspondent banking and agree that the perpetuation of such a phenomenon could lead to significant consequences, including affecting the ability of certain countries and industries to send and receive international payments and driving some payment flows underground. We also note that de-risking is in part a reaction to government and supervisory characterizations of correspondent banking as a high risk business and the evolving standards within the international community. The following comments reflect these concerns and seek to provide constructive recommendations on further refining the regulatory framework, to be more risk-based, and therefore address the drivers of de-risking.

B. Burdens Imposed

31 C.F.R. § 1010.605(c) generally defines a correspondent account as an account established for a foreign financial institution or bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such a foreign financial institution or bank.

We are concerned that this broad definition encompasses relationships where banks deal with one another as principals, rather than when they provide third-party services to one another, such as clearing payments or processing other transactions involving a correspondent bank customer's customers. The necessary risk analysis when a bank acts as a principal is fundamentally different from that required when a bank processes third-party payments. When dealing as a principal, a bank assesses AML/CFT risk based on the characteristics of the other bank. Engaging with a bank that is acting on behalf of a third party requires an assessment of an additional layer of AML/CFT risk posed by the indirect involvement of another party with whom the bank has no relationship, but which carries its own set of AML/CFT risk factors. Many "banking services" provided by one bank to another may not entail these additional risks. For

---

48 *See "*FSB action plan to assess and address the decline in correspondent banking –Progress report to G20 Summit of July 2017" (July 4, 2017), available at http://www.fsb.org/wp-content/uploads/P040717-3.pdf. *See also* for more granular information on the decline in correspondent, the FSB's *Correspondent Banking Data Report*, (July 4, 2017), *available at* http://www.fsb.org/wp-content/uploads/P040717-4.pdf.

49 In this regard, TCH has been actively participating in efforts to identify and manage the money laundering and terrorist financing risk of correspondent banking, including through its publication of the *Guiding Principles for Anti-Money Laundering Policies and Procedures for Correspondent Banking* and co-sponsorship of the *Statement on Payment Message Standards* to allow for greater transparency in payment messages. *See* The Clearing House, *Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking* (February 2016), *available at* https://www.theclearinghouse.org/issues/articles/2016/02/20160216-tch-guiding-principles-for-aml. *See also* Wolfsberg Group, *Clearing House Statement on Payment Message Standards* (2007), *available at* http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_(2007).pdf.

example, interest rate and foreign exchange swaps among banks and financial institutions, when used as tools to hedge risk, do not involve the processing of transactions on behalf of third parties and, as such, may not present the same degree of AML/CFT risk. Yet, this activity, despite the different risk profile, is encompassed by the current definition of correspondent account.

We note that the Basel Committee on Banking Supervision recently recognized the third-party nature of correspondent banking in Annex 2, on correspondent banking, of its *Sound management of risks related to money laundering and financing of terrorism*. The guidance states that it "focuses on higher-risk correspondent banking relationships, in particular cross border correspondent banking involving the execution of third-party payments."[50] U.S. regulators should narrow the definition of correspondent banking to encompass only activities that generate particular AML/CFT risks, notably the execution of third-party payments.

Furthermore, de-risking is very often the result of a bank's prudent assessment of its own risk tolerance in light of its own risk management and regulatory expectations—and that, in this respect, de-risking is a function of government policy and supervisory practices. As described in the previous section, U.S. AML/CFT regulatory expectations require financial institutions to identify suspicious activity through correspondent accounts, thereby impacting an institution's risk assessment of both a client and a business line. Additionally, internal audits of regulatory compliance, which occur more frequently than regulatory examinations, also contribute to de-risking, as adverse audit findings may be as impactful, disruptive and expensive to resolve as an adverse regulatory finding. This effect is particularly acute in the U.S. where financial institutions are required to have independent testing procedures as a part of their AML/CFT programs, which banking regulators may rely on in regulatory examinations. Therefore, in order to effectively address the de-risking phenomenon, U.S. regulators should continue to clarify regulatory expectations in consultation with the correspondent banking community,[51] and should provide banks with greater certainty that the banks' good-faith application of clear regulatory guidance and expectations will ensure that banks are found by their regulators and auditors to be in compliance with those requirements.

Finally, the term Know-Your-Customer's-Customer ("KYCC") has been the cause of substantial confusion throughout the correspondent banking community. Last year, the Treasury Department and the federal banking agencies published a joint fact sheet stating that in the U.S. "there is no general requirement for U.S. depository institutions to conduct due diligence on an FFI's customers."[52] While a helpful first step in clarifying U.S. regulatory expectations, we note

---

50 *See* Basel Committee on Banking Supervision, *Sound management of risks related to money laundering and financing of terrorism*, (June 2017) at 23, *available at*: http://www.bis.org/bcbs/publ/d405.pdf.

51 We also support efforts to require certain information to be in payment messages that are received by intermediary banks be developed at the industry level in consultation with all financial market infrastructures including CHIPS, Fedwire and SWIFT.

52 *See* U.S. Department of the Treasury and Federal Banking Agencies Joint Fact Sheet on Foreign Correspondent Banking: Approach to BSA/AML and OFAC Sanctions Supervision and Enforcement, (August 30, 2016), *available at* https://www.treasury.gov/press-center/press-releases/Documents/Foreign%20Correspondent%20Banking%20Fact%20Sheet.pdf.

that the FATF Guidance devotes a paragraph to clearly establishing that "[t]here is no expectation, intention or requirement for the correspondent institution to conduct customer due diligence on its respondent institution' [sic] customers." We understand that regulators currently expect correspondent banks to obtain a general knowledge and broad overview of respondent banks' activities and types of customers and consider the risk of the categories of customers served by its respondent bank customers, including when a respondent bank has downstream banking relationships with banks in high-risk jurisdictions. However, particularly in the context of downstream banking relationships, correspondent banks are necessarily reliant on the AML programs of their respondents, and can realistically evaluate only the respondent's program for evaluating its downstream respondents, but not the downstream respondents themselves. Given the confusion the KYCC concept has caused, for clarity and for consistency with the FATF Guidance, we suggest that FinCEN, along with the banking agencies, explicitly acknowledge that there is no KYCC requirement for correspondent banks, including with respect to downstream banking relationships.

C. Recommendations

In order to reduce burdens, ensure consistency, and emphasize the risk-based nature of the AML/CFT regime, Treasury/TFI/FinCEN should, in consultation with the federal banking agencies:

- Narrow the definition of correspondent banking to encompass only activities that generate particular AML/CFT risks, notably the execution of third-party payments;

- By regulation or guidance, indicate that institutions that make a good faith effort to monitor transactions and identify suspicious activity with regard to domestic and foreign correspondent accounts should not be penalized for failures to identify specific instances of suspicious activity; and

- Encourage banks' general understanding of respondent banks' customer bases, rather than requiring more detailed information about those customers, by adopting FATF's October 2016 language that "[t]here is no expectation, intention or requirement for the correspondent institution to conduct customer due diligence on its respondent institution[s]' customers."

IV. Treasury/TFI/OFAC should increase the efficiency and effectiveness of sanctions compliance, and further recognize a risk-based approach to compliance.

A. Background

OFAC sanctions programs are a vital tool to U.S. foreign policy and therefore it is essential that compliance expectations are risk-based and communicated consistently in order to avoid inconsistent application of program requirements. Therefore, Treasury, TFI, and OFAC should take a more prominent role in coordinating sanctions policy across the government.

Administered under the International Emergency Economic Powers Act[53] and other statutes, the President is granted broad authority to impose economic sanctions against countries and parties which 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.[54]

B. Burdens Imposed

In accordance with the application of the risk-based approach to compliance within the U.S. sanctions regime, OFAC should provide further guidance on sanctions screening expectations and engage with the industry on such programs. One example where the tailoring of expectations would be helpful is with low dollar payments – both national and international – that from a sanctions perspective present minimal compliance risks. In addition, OFAC should recognize that domestic, bank-to-bank payments are low risk and that the speed of commerce that is enabled by innovative services should not be choked by outdated screening expectations. This is particularly important given the new faster and information-rich payment services that are coming to market to better meet the needs of U.S. businesses and consumers. OFAC's ability to work with the industry as it seeks to bring new payment capabilities to market will ultimately impact the competitive standing of U.S. financial institutions. Therefore OFAC should clarify that a risk-based approach to sanctions screening is permitted and appropriate and that screening is not required for purely domestic wires and other payment products (similar to guidance already issued regarding domestic ACHs).

U.S. sanctions programs, imposed by Executive Order, are often broad and contain key terms that are not defined in either the underlying Executive Orders or in the implementing regulations. For financial institutions that often serve as the "front lines" in implementing economic sanctions, this absence of a definition can cause uncertainty as to what their compliance obligations are and lead to interpretative deviations across financial institutions, which impact their ensuing compliance controls.[55] However, sanctions regulations are often further supplemented with *Frequently Asked Questions* ("FAQs") releases that provide additional guidance and examples in an effort to enhance private sector understanding and compliance with OFAC's expectations. Therefore, as an initial matter, OFAC should standardize, to the extent possible, definitions, prohibitions, interpretations, authorizations and exemptions across OFAC

---

53 50 U.S.C. 1701 et seq.

54 *See* "Remarks of Secretary Lew on the Evolution of Sanctions and Lessons for the Future at the Carnegie Endowment for International Peace," (March 30, 2016), *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl0398.aspx. In those remarks former Treasury Secretary Lew stated that "[t]he sanctions we employ today are different [– t]hey are informed by financial intelligence, strategically designed, and implemented with our public and private partners to focus pressure on bad actors and create clear incentives to end malign behavior, while limiting collateral impact."

55 Industry sometimes collaborates to address inconsistencies or gaps in guidance. For example, *see* The Bankers Association for Finance and Trade and The Clearing House paper, "Guiding Principles for Sanctions Issues Related to Shipping and Financial Products," (February 2017), *available at* https://www.theclearinghouse.org/-/media/tch/documents/tch%20weekly/2017/20170206_baft_tch_guiding_principles_sanctions_issues_related_to_shipping_and_financial_products.pdf.

regulations. Furthermore, concepts and examples generally embodied in FAQ documents should be incorporated directly into the applicable regulations.

With regard to general license programs established by OFAC in concert with sanctions programs, revisions should be made to all general licenses to specify within the license whether the general license only applies in situations where the underlying activity is being performed by U.S. persons or within the jurisdiction of the U.S., or if the license extends to all transactions relating to the activity, regardless of whether a U.S. person is involved in the underlying transaction. In instances where OFAC general licenses are silent on their applicability to activity conducted by non-U.S. persons, U.S. financial institutions face risks associated with implementing such licenses and therefore are often forced to unnecessarily block or reject transactions, or seek guidance from OFAC.

In addition, we note that sanctions programs that target certain regions or sectors of a foreign 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 nor restricted from engaging in other activities throughout the U.S. financial systems.

Notably, the Ukraine/Russia-related Sectoral Sanctions ("SSI sanctions") program, which was implemented through four Directives pursuant to Executive Order 13662, is difficult for U.S. financial institutions to implement. In December 2014, TCH along with a number of other trade associations sent a letter to then OFAC Director Adam Szubin discussing core compliance challenges facing financial institutions with regard to the Ukraine-related sectoral sanctions program.[56] Those challenges stemmed from: (i) the size of the Russian economy and the application of sectoral sanctions to not only Russian financial institutions, energy companies and defense companies (the "sectoral sanctions identifications" or the "SSIs"), but also entities that are majority-owned, through the application of the "50% Rule," to one or more of these companies; and (ii) the focus on specific types of prospective debt and equity transactions.

While OFAC did not respond to the requests made in the letter, they have issued more than 50 FAQs to outline and clarify the requirements of the SSI sanctions. While these FAQs have been useful in helping U.S. financial institutions understand and comply with the sanctions, published regulations would enhance legal certainty and provide greater clarity to the regulated community. Therefore, US financial institutions are often left guessing whether their actions are in compliance with Executive Order 13662 and the accompanying Directives.

As discussed above, we support the further codification of sanction FAQs in regulations, which would bring much needed clarity to this complex sanctions program and would greatly enhance U.S. financial institutions' ability to comply with the sanctions. In addition, as the 50%

---

[56] *See* The Clearing House Association, the American Bankers Association, the Institute of International Bankers, and the Securities Industry and Financial Markets Association Letter to Adam Szubin, Re: Ukraine-Related Sectoral Sanctions, (December 11, 2014), *available at* https://www.theclearinghouse.org/-/media/files/association%20related%20documents/20141211%20tch%20comments%20to%20ofac%20on%20sectoral%20sanctions.pdf.

Rule applies in the context of both comprehensive and sectoral sanctions programs, OFAC should clarify that financial institutions are expected to apply sanctions to a subsidiary of a person listed on a relevant OFAC list when there is a reason to know that the entity is a majority-owned subsidiary of a listed person, such as when the subsidiary (i) is a customer of the financial institution or (ii) is listed as a subsidiary on an OFAC list.

Relatedly, OFAC should publish the names of all known targeted persons to allow financial institutions to properly screen for and interdict prohibited transactions.[57] Currently, financial institutions are often tasked with identifying entities that are owned by the governments of OFAC sanctioned countries (e.g., Iran, North Korea, Syria, etc.), or that are owned in the aggregate by multiple SDNs. That is not a practical approach to compliance and financial institutions are not in a position to conduct extensive research to identify entities that are owned by other SDNs, particularly when aggregation principles are applied and there is no relationship with an existing customer. Additionally, the U.S. government has access to intelligence that is not available to financial institutions and the private sector more generally. For a financial institution's direct client, the financial institution may request percent ownership depending on the risk associated with the client, but even this level of due diligence may not mitigate all identification risks. Therefore, it is ineffective and impractical to expect financial institutions to comply with the 50% Rule for all possible transactions.

Furthermore, OFAC should standardize the information in the various sanctions lists published by OFAC, including the SDN list by: (i) establishing minimum data requirements for new additions to the SDN and other sanctions lists (i.e. person's name, date of birth, passport or national ID number, or, for corporations company name, address, registration number or tax ID, etc.); and (ii) removing historical entries with little to no identifying information or poor strong and weak aliases. Lack of identifying data in sanctions list entries makes it extremely difficult for financial institutions to determine whether an alert generated through screening is a false positive or a true match to the sanctions list entry. Establishing minimum data requirements for sanctions list entries will significantly decrease the number of false positives generated by sanctions screening software and enhance overall sanctions compliance.

In addition, OFAC should amend the Voluntary Self Disclosures (VSD) program to (i) further clarify the nature of the program as there is currently no industry standard in the interpretation of "voluntary," which leads to overfilling[58] and (ii) broaden the definition of VSDs to allow such disclosures to be considered VSDs if the subject person has previously disclosed the information to another U.S. Government agency. Finally, we recommend that the reporting requirements for blocked and rejected transactions be changed to a monthly batch reporting process rather than ten days after the block or rejection. This will allow financial institutions to submit a more consolidated report and would reduce the volume of submissions to OFAC, thereby alleviating administrative burdens.

---

[57] Relatedly, we also encourage further coordination on sanctions lists between the U.S. and other bodies that publish lists, including the United Nations.

[58] *See* 31 C.F.R. Part 501, Economic Sanctions Enforcement Guidelines (Enforcement Guidelines), Appendix A.

C. Recommendations

Treasury/TFI/OFAC should, to the extent possible, engage in further dialogue with the private sector on sanctions programs and their implementation. In addition, in order to reduce burdens and increase the efficiency and effectiveness of sanctions compliance, and further recognize a risk-based approach to compliance, OFAC should:

- Provide guidance, or to the extent possible, incorporate into regulation that (i) a risk-based approach to sanctions screening is appropriate and expected (i.e. certain low dollar payments); and (ii) screening is not required for purely domestic wires and other payment products (similar to guidance already issued regarding domestic ACHs);

- Standardize, to the extent possible, definitions, prohibitions, interpretations, authorizations and exemptions across OFAC regulations;

- Incorporate, to the extent possible, concepts and examples generally embodied in the FAQ document directly into the applicable regulations;

- Revise all general licenses to explicitly specify within the license whether the general license only applies to situations where the underlying activity is being performed by U.S. persons or within the jurisdiction of the U.S., or if the license extends to all transactions relating to the activity regardless of whether a U.S. person is involved in the underlying transaction;

- Clarify that financial institutions are expected to apply sanctions to a subsidiary of a person listed on a relevant OFAC list when there is a reason to know that the entity is a majority-owned subsidiary of a listed person, such as when the subsidiary (i) is a customer of the financial institution or (ii) is listed as a subsidiary on an OFAC list;

- Publish the names of all known sanctioned parties on OFAC-published lists to allow financial institutions to properly screen for and interdict prohibited transactions;

- Standardize the information in the various sanctions lists published by OFAC, including the SDN list by: (i) establishing minimum data requirements for new additions to the SDN and other sanctions lists (i.e. person's name, date of birth, passport or national ID number, or, for business entities, name, address, registration number or tax ID, etc.); and (ii) removing historical entries with little to no identifying information or poor strong and weak aliases;

- Amend the Voluntary Self Disclosures (VSD) program to (i) further clarify the nature of the program as there is currently no industry standard in the interpretation of "voluntary;" and (ii) broaden the definition of VSDs to allow such disclosures to be considered VSDs if the subject person has previously disclosed the information to another U.S. Government agency; and

- Change reporting requirements for blocked and rejected transactions to a monthly batch reporting process rather than ten days after the block or rejection.

* * * * *

The Associations would welcome the opportunity to provide any additional assistance or input with regard to this request for information. If you have any questions, please contact Angelena Bradfield at 202-649-4608 or angelena.bradfield@theclearinghouse.org

Respectfully submitted,

Angelena Bradfield
Vice President and Senior Policy Specialist,
AML/CFT & Prudential Regulation
The Clearing House Association L.L.C.

Richard Foster
Senior Vice President and Senior Counsel for
Regulatory and Legal Affairs
Financial Services Roundtable

ANNEX A

The Clearing House. The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates back to 1853. The Clearing House Association L.L.C. is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system. Its affiliate, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Payments Company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume.

The Financial Services Roundtable. FSR represents the largest integrated financial services companies providing banking, insurance, payment, investment and finance products and services to the American consumer. FSR member companies provide fuel for America's economic engine, accounting for $54 trillion in managed assets, $1.1 trillion in revenue and 2.1 million jobs.

ANNEX B

The Clearing House®

At the Center of Banking Since 1853®

A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement

February 2017

A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement

February 2017

Table Of Contents

Introduction

In April and October 2016, a group of approximately 60 experts came together to discuss how to improve the U.S. framework for anti-money laundering/countering the financing of terrorism (AML/CFT) as it applies to financial institutions. The group included senior former and current law enforcement, national security, bank regulatory and domestic policy officials; leaders of prominent think tanks in the areas of economic policy, development, and national security; consultants and lawyers practicing in the field; FinTech CEOs; and the heads of AML/CFT at multiple major financial institutions. The first meeting focused on problems with the current regime; the second focused on a review of potential solutions. The consensus on both is set forth in this paper. It was prepared with the assistance of The Clearing House's special counsel, Wilmer Cutler Pickering Hale and Dorr LLP.

The stakes here are high. The United States leads the world in shaping and enforcing international standards of financial integrity and accountability and has demonstrated the importance of the AML/CFT regime to combating and preventing financial crime and protecting international security. Nevertheless, substantial challenges to the systemic effectiveness and sustainability of the current regime have emerged and require urgent attention.

Under the current AML/CFT regime, the nation's financial firms are effectively deputized to prevent, identify, investigate, and report criminal activity, including terrorist financing, money laundering and tax evasion. The largest firms collectively spend billions of dollars each year, amounting to a budget somewhere between the size of the ATF and the FBI.[1] Yet the conclusion of the vast majority of participants in the process is that many if not most of the resources devoted to AML/CFT by the financial sector have limited law enforcement or national security benefit, and in some cases cause collateral damage to other vital U.S. interests – everything from U.S. strategic influence in developing markets to financial inclusion. Thus, a redeployment of those resources has the potential to substantially increase the national security of the country and the efficacy of its law enforcement and intelligence communities, and enhance the ability of the country to assist and influence developing nations.

Executive Summary

The current AML/CFT statutory and regulatory framework is outdated and thus ill-suited for apprehending criminals and countering terrorism in the 21st century. In particular, the following are core problems with the current AML/CFT regime that must be resolved:

STRATEGIC PROBLEMS

» **ABSENCE OF PRIORITIZATION.** Law enforcement, national security and development officials have little to no input into how financial institutions allocate their AML/CFT resources. Rather, compliance is assessed primarily by bank examiners, essentially functioning as auditors, who are focused on preventing the institutions they supervise from suffering financial loss or reputational embarrassment, and ensuring that there is rigorous adherence to all written policies and procedures. Thus, for example, while financial intelligence units within the banks are of great benefit to law enforcement and national security officials, and focus on real risks, the examination process tends to result in banks prioritizing other, more readily auditable processes.

» **ABSENCE OF OVERARCHING PURPOSE.** For approximately the past 15 years, regulators described "preserving the integrity of the financial system" as the primary goal of the AML/CFT regime, but the notion has no statutory basis or clear definition. It implies an overarching goal of keeping money out of the financial system, but another goal should be and sometimes is the tracking of money once it is in the financial system and providing financial services to developing nations and underserved U.S. communities. Thus, the current examination and enforcement regimes have encouraged financial institutions to exclude (or "de-risk") accounts from a customer, industry or country that is perceived to have heightened risk of engaging in criminal activity; meanwhile, those concerned with international development and diplomacy, and financial inclusion, have little voice in the examination process.

» **OUTDATED SAR REGIME.** The original purpose of the suspicious activity report (SAR) regime was for financial institutions to provide leads to law enforcement agencies, but government agencies now could develop the technical resources and sophistication to mine financial data, significantly reducing the need for SARs as they are currently constructed. Yet the SAR remains the focus of the system.

OPERATIONAL PROBLEMS

» **COUNTERPRODUCTIVE EXAMINATION STANDARDS AND PROCESSES.** National security, law enforcement, and intelligence agencies—the end users of AML/CFT information—focus on the quality of information they receive from financial institutions, while those who grade the financial institutions focus on auditable processes. Thus, there are disincentives for financial institutions to develop innovative methods

for identifying criminal behavior. Firms receive little or no credit for proactive, aggressive cooperation with law enforcement – focusing on real risk – because examiners generally are unaware of such actions and in any event have no method for weighing such behavior against any policy or operational shortcomings within the confines of the examination framework.

» **SIGNIFICANT BARRIERS TO INFORMATION SHARING.** Existing rules prevent efficient and effective sharing of information among financial institutions and between financial institutions and law enforcement.

» **INEFFICIENCIES.** Financial institutions devote vast resources to activities that could easily be performed centrally by government or some other party or not at all – for example, constant monitoring of media for adverse stories about customers, or multiple firms engaging in customer due diligence on the same customers. With these tasks de-prioritized or executed collectively, resources could be deployed to more sophisticated and productive approaches designed to detect real risks.

Set forth below are clear and actionable responses to these problems, divided into two groups: areas for immediate reform and areas for further study.

Areas for Immediate Reform

- The Department of Treasury, through its Office of Terrorism and Financial Intelligence (TFI), should take a more prominent role in coordinating AML/CFT policy across the government;

- The Financial Crimes Enforcement Network (FinCEN) should reclaim sole supervisory responsibility for large, multinational financial institutions that present complex supervisory issues;

- Treasury/TFI/FinCEN should establish a robust and inclusive annual process to establish AML/CFT priorities;

- Congress should enact legislation, which was proposed in various forms during the 114th Congress and is expected to be re-introduced in the 115th Congress, that requires the reporting of beneficial owner information at the time of incorporation;

- Treasury TFI should strongly encourage innovation, and FinCEN should propose a safe harbor rule allowing financial institutions to innovate in a Financial Intelligence Unit (FIU) "sandbox" without fear of examiner sanction;

- Policymakers should de-prioritize the investigation and reporting of activity of low law enforcement or national security consequence;

- Policymakers should further facilitate the flow of raw data from financial institutions to law enforcement to assist with the modernization of the current AML/CFT technological paradigm;

- Regulatory or statutory changes should be made to the safe harbor provision in

the USA PATRIOT Act (Section 314(b)) to further encourage information sharing among financial institutions; and

- Policymakers should enhance the legal certainty regarding the use and disclosure of SARs.

Areas of Reform Requiring Further Study:

- Enhancing information sharing through the establishment of AML/sanctions utilities.
- Establishing better protections from discovery for SAR information;
- Clarifying and balancing responsibility for AML/CFT between the public and private sector;
- Establishing a no action letter-like system within the regime to assist with AML/CFT compliance;
- Providing financial institutions with clearer AML/CFT standards;
- Allowing for better coordination of AML/CFT and sanctions policy goals, supervision and enforcement; and
- Modernizing the SAR regime.

Assessment of the Existing Regime

BACKGROUND

The current AML/CFT regulatory framework is an amalgamation of statutes and regulations that generally derive from the Bank Secrecy Act, which was passed by Congress in 1970 with iterative changes since, and added to (but not reformed by) the USA PATRIOT Act, which was passed in 2001. This 45-plus year regime has not seen substantial changes since its inception and is generally built on individual, bilateral reporting mechanisms (i.e. currency transaction reports and suspicious activity reports), grounded in the analog technology of the 1980s, rather than the more interconnected and technologically advanced world of the 21st century.

In particular, the Bank Secrecy Act imposes requirements that can be in tension with each other and need to be considered in tandem as part of a risk-based system. Financial institutions are required to (i) report on suspicious activity and (ii) keep out customers that could generate suspicious activity. These conflicting requirements are further magnified by the wide-reaching and complex network of state and federal government actors who are responsible for implementing, enforcing and utilizing the information produced by the regime.[2] Generally, each entity has different missions and incentives, which has led to the development of competing and sometimes conflicting standards for institutions to follow.

Outlined below are what was determined by the group as fundamental problems with the current regime as well as recommendations for reform and items for further study.

FUNDAMENTAL PROBLEMS

Participants in the first symposium identified several fundamental problems with the current AML/CFT regime:

ABSENCE OF PRIORITIZATION. In law enforcement, it is routine for the Justice Department and other agencies to establish priority enforcement areas, set qualitative and dollar thresholds for the cases they are willing to bring, and generally manage the process of law enforcement. Aware of their limited budgets, these agencies choose which crimes to prosecute and which ones to let pass. However, financial institutions operating AML/CFT compliance programs receive little guidance on these matters, and are not able to exercise sufficient discretion within the current regulatory framework to themselves identify priorities. Thus, although the government may want financial institutions to prioritize cases involving, for example, terrorist financing, nuclear proliferation and human trafficking, in practice, there is little to no policy guidance to the financial sector on these priorities.[3] The reason is simple: the representatives of government that face financial institutions and have the ability to set the AML/CFT priorities for these institutions (most frequently, bank examiners) are not engaged with the law enforcement or intelligence communities, and thus lack the knowledge and authority to set such priorities on their behalf. Rather, they are focused on preventing the institutions they supervise from suffering financial loss or reputational embarrassment, establishing auditable policies and procedures, and ensuring rigorous adherence to those policies and procedures. This focus, plus a near-zero tolerance for error, necessarily focuses financial institutions on recordkeeping rather than developing imaginative and innovative approaches to identifying important threats to our country.

OUTDATED NATURE OF THE SAR REGIME. When it was first established in the 1990s, the goal of the SAR regime was for financial institutions to provide leads to law enforcement agencies; those agencies had little insight into the financial system, and no technical ability to mine data. Today, government agencies could develop resources to mine financial data, and rely less on financial institutions to provide robust, individual reports on suspicious activities or transactions. Also, as financial institutions have been incentivized by regulatory enforcement actions to file increasing numbers of suspicious activity reports (SARs), a declining percentage provide value to law enforcement.[4] Yet those regulators examining banks for AML compliance continue to emphasize the importance of financial institutions developing carefully crafted, highly-detailed SARs, with little to no feedback provided on such submissions, either from themselves or those government authorities who utilize the data.

COUNTERPRODUCTIVE EXAMINATION STANDARDS. Although financial institutions have been developing innovative methods for identifying criminal behavior, they face regulatory criticism for taking unconventional or innovative actions that seemingly deviate from policy and may not be readily auditable. The job of examiners is to check compliance against current standards, and they tend to disfavor imaginative deviation from those standards – particularly as they are cut off from information about the benefits of such deviations, given that law enforcement and national security officials

do not include them in investigations. As a result, financial institutions have begun to innovate less. Law enforcement and national security officials most value the work done by FIUs at financial institutions, which are laboratories dedicated to developing new and frequently outside-the-box methods of detecting illegal or dangerous conduct. Yet, several institutions reported shifting resources away from FIUs towards compliance staff, because of explicit or implicit examiner insistence that resources be devoted to demonstrating compliance with existing policies and procedures and ensuring the auditability of those mechanisms. Compliance officers, in turn, have received increasing pressure to ensure 100% compliance, and are increasingly at risk of personal liability or dismissal in the event of deviation from regulatory expectations; they thus have greater incentives to "work to the rule" rather than encourage innovation.

In sum, under the current regime, national security, law enforcement, and intelligence agencies—the end users of AML/CFT information—focus on outcomes, while those who grade the financial institutions for compliance focus on auditable processes.

BROADER CONFLICTING POLICY INTERESTS. The examination and enforcement regimes for the Bank Secrecy Act have incentivized financial institutions to exclude (or "de-risk") accounts from any customer, industry, or country that has relatively higher potential to engage in criminal activity: for example, to de-risk money service businesses or correspondent banks in developing or high-risk countries where public corruption, narcotics, or terrorist activity is prevalent. On the other hand, policymakers concerned with income inequality want banks to serve poor and underserved populations; development experts want multinational U.S. banks to serve developing countries; intelligence officials and law enforcement want multinational U.S. banks to stay engaged abroad in order to establish leads on nefarious activity; and national security and diplomatic officials want multinational U.S. banks to remain engaged abroad, rather than ceding those markets to other, less transparent, actors. Because a bank's AML/CFT regime is evaluated solely by bank examiners, these other policy interests generally are not considered. When they have been considered – for example, in recent OCC guidance – the response has been to require banks to develop policies and procedures for documenting their decision to de-risk rather than to encourage them to manage the risk more effectively.

BARRIERS TO INFORMATION SHARING. Significant barriers to information sharing are embedded in the system – for example, rules or interpretations limiting the ability of financial institutions to share within their own corporate structure, and with other financial institutions. These barriers block the flow of relevant information among financial institutions and between financial institutions and law enforcement. Some of these barriers serve legitimate privacy concerns that must be balanced against any potential benefits from greater sharing, but in many instances the barriers are simply the result of basic policy errors that have not been remedied over time.

INEFFICIENCIES. Financial institutions devote vast resources to activities that could easily be performed centrally by government or some other party. One example is the lack of an established reporting requirement for

beneficial owners of corporations, forcing financial institutions to research such information when it should be readily available upon incorporation. Another is filing SARs on activity that existing prosecution handbooks make clear will never be prosecuted – for example, low-dollar crimes committed against banks. A third is the tracking of politically exposed persons (PEPs), the definition of which is subject to multiple and changing standards across agencies and jurisdictions.

ALTERNATIVE APPROACH TO INFORMATION SHARING

The group also reviewed an alternative approach to information sharing that offered real promise: the UK's Joint Money Laundering and Intelligence Task Force (JMLIT).[5] JMLIT brings together financial institutions, law enforcement, and trade associations to discuss current AML/CFT risks and is underpinned by legislation that enables the UK National Crime Agency (NCA) to act as the gatekeeper for the information provided, and facilitate the exchange of information between the public and private sectors. Following completion of a one-year pilot program, an independent review determined that JMLIT had met its core objective to prevent, detect, and disrupt money laundering.

The JMLIT process has attributes that could help to resolve several problems identified with the current U.S. regime. The current SAR regime fails to provide feedback from law enforcement to the private sector about SAR efficacy, while JMLIT allows banks to follow-up on SAR activity. In addition, the JMLIT structure provides the dialogue about prioritization that U.S. financial institutions currently do not receive. Furthermore, JMLIT uses an operational priority structure which focuses on "(i) understanding and disrupting the funding flows linked to bribery and corruption; (ii) understanding and disrupting trade based money laundering; (iii) understanding and disrupting the funding flows linked to organized immigration crime and human trafficking; and (iv) understanding key terrorist financing methodologies." While U.S. policymakers might choose different priorities, and those priorities might change over time, they currently do not communicate any priorities with this degree of clarity.

POTENTIAL REFORMS

Set forth below are reforms that would: (i) make the AML/CFT regime more effective as a tool for law enforcement and national security; and (ii) reduce the collateral damage imposed by the current AML/CFT regime—generally, needlessly—on other important national priorities such as the projection of U.S. influence globally, the alleviation of poverty in less developed countries, and the availability of banking services in underserved communities in the United States. Possible reforms can be divided into two groups:

AREAS FOR IMMEDIATE REFORM: These reforms are clearly warranted and are of high priority. On these reforms, there was clear consensus of symposium participants on both the immediate need for the reforms and their wisdom.

AREAS OF REFORM REQUIRING FURTHER STUDY: These reforms warrant further consideration, because potential solutions may involve difficult tradeoffs or would benefit from the input of other stakeholders.

Areas for Immediate Reform

I. RATIONALIZE THE SUPERVISION OF MULTINATIONAL, COMPLEX FINANCIAL INSTITUTIONS

A. FinCEN should reclaim sole supervisory authority for large, multinational financial institutions that present complex supervisory issues.

BACKGROUND. FinCEN was granted authority to examine for compliance with the Bank Secrecy Act. However, over 20 years ago, it delegated its supervisory authority to the federal banking agencies, while retaining enforcement authority. In addition, in 1986, Congress granted the federal banking agencies authority to prescribe regulations requiring banks to comply with the Bank Secrecy Act, and examine for such compliance.[6]

At the time the delegation was made, FinCEN's decision was logical, even inevitable. The agency had few resources, and insufficient knowledge of the banking system. Furthermore, the nation had over 10,000 banks,[7] and those banks were more alike than different. Restrictions on interstate banking meant that there were no truly national banks, and U.S. banks generally were not internationally active. As a result, there was no real basis by which FinCEN could distinguish among banks. Given the choice between supervising 10,000 banks or none, it logically chose none.

RECOMMENDATION.

(1) FinCEN should revoke its delegation of examination authority for large, internationally active financial institutions[8] and any others it designates as presenting important and significant issues with respect to national security, law enforcement, and global development priorities. This would include not only banks but also large money service businesses and other significant non-bank financial institutions. As discussed below, FinCEN should assemble sufficient staff to conduct rigorous Bank Secrecy Act examinations of such institutions.[9]

(2) FinCEN, in coordination with relevant Treasury Department offices (i.e. TFI, Domestic Finance, and International Affairs), should create a multi-agency advisory group to: (i) establish priorities for each financial institution on an annual basis; (ii) review progress with the institutions on a quarterly basis; and (iii) oversee any examination of the institutions.

(3) The advisory group should include senior officials representing the FBI, DHS (Secret Service and other relevant personnel), OFAC, State Department, Defense Department, the intelligence community, and select financial regulators.

BENEFITS. The advantages of centralizing supervision and examination of AML/CFT compliance for complex institutions would be numerous:

» It would allow for the creation of a core, centralized examination team that could

work cooperatively with law enforcement, national security, and diplomatic officials, receiving the necessary security clearances (which bank examiners currently lack) and establishing the necessary trust, to understand the full picture.

» Such an examination team would reward rather than hinder innovation, emphasizing results rather than process. Financial institutions would be instructed to shift resources away from box checking and reporting petty offenses toward law enforcement, national security and global development priorities. As one participant in the symposium noted, "what gets measured gets done."

» Performance evaluations for a FinCEN examination team would be driven by the quality of the information identified and reported by its supervised institutions, and the strength of their analyses, rather than the auditability of its processes, or the number of alerts generated or SARs filed by the institutions. These evaluations would include feedback given by senior national security and law enforcement officials who are now absent from that process.

» The examination team should be well trained in technological innovations, including big data, and work across the financial services industry to leverage those concepts to detect illegal or threatening activity. Such a team could draw on resources at the Defense Advanced Research Projects Agency and elsewhere in the U.S. government.

» The examination team should be fully engaged in the whole range of AML/CFT activities at the institutions it supervises, including working with other agencies to support the institutions' investigations. It would also be knowledgeable about international financial services and money laundering typologies.

» Finally, a centralized supervision and examination function for large, internationally active institutions would contribute to the tailoring of the AML/CFT regulatory regime to participating institutions' risk profiles.

ISSUES. A centralized examination team would require resources. One alternative would be appropriated funds, which would be money well spent. Another would involve FinCEN assessing financial institutions for examination costs in the same way as banking regulators; existing statutory authority appears to allow for such an assessment.[10] Affected institutions would see a corresponding reduction in the assessment they currently pay to prudential regulators for supervision of this function. A third alternative would be to establish a centralized team funded *pro rata* by each of the affected agencies but reporting directly and solely to the Director of FinCEN.

Alternatively, but not ideally, each regulatory agency could designate personnel to serve as members of a joint team to conduct a review of Bank Secrecy Act compliance on its behalf.[11] This approach could leverage the existing cooperation model of the Federal Financial Institutions Examination Council (FFIEC) to create a joint national exam team for AML/

CFT and sanctions issues. The team would still report to FinCEN and would otherwise function as described above. There would also necessarily be some coordination among the exam team and the other regulators, who would remain responsible for safety and soundness examination.

B. FinCEN should institute a process to establish AML/CFT priorities for all covered institutions.

The multi-agency advisory group described above, and led by Treasury and FinCEN, should also establish priorities for the many institutions, including non-banks, that are not subject to centralized exams. FinCEN should communicate that guidance to those regulators that continue to exercise delegated authority for their use in establishing examination standards for the coming year. In addition, FinCEN should meet regularly with the regulators to review progress on priorities.

II. ENACT BENEFICIAL OWNERSHIP LEGISLATION

Federal regulations require financial institutions to know their customers and conduct ongoing monitoring of account information. FinCEN's new customer due diligence rule will soon require financial institutions to collect beneficial ownership information from certain legal entity customers. Yet there is currently no requirement that states record the beneficial ownership of the legal entities they incorporate. This makes it easier for money launderers and terrorist financiers to obscure their identities from both law enforcement and the financial institutions with which they deal. Indeed, the Financial Action Task Force ("FATF") recently criticized the gaps in the legal framework in the United States that prevent access to accurate beneficial ownership information in a timely manner and recommended that the United States take "steps to ensure that adequate, accurate and current [beneficial ownership] information of U.S. legal persons is available to competent authorities in a timely manner, by requiring that such information is obtained at the Federal level."[12] Due to the lack of easily accessible beneficial ownership information, financial institutions allocate significant resources to investigating the ownership of their customers.

Congress should enact legislation—forms of which were pending in both the House and Senate during the 114th Congress and are expected to be re-introduced in the 115th Congress—that would require the collection of beneficial ownership information at the time of incorporation and whenever such information changes, and ensure that such information is provided to relevant stakeholders including FinCEN and law enforcement. In addition, any legislation should clarify that financial institutions performing customer due diligence can obtain access to reported beneficial ownership information upon account opening and on an ongoing basis, and can rely on that information in complying with any obligation to know their customers. Under the current regime, many if not most of the resources devoted to identifying money laundering and terrorist financing are provided by financial institutions; denying them access to this important information would significantly undermine the goals of any bill.

III. ESTABLISH A CLEAR MANDATE IN SUPPORT OF INNOVATION

BACKGROUND. Financial institutions are motivated to assist the government in understanding and identifying financial crime and are constantly developing new methods to thwart money laundering and terrorist financing. One significant example is the establishment of FIUs within large financial institutions. FIUs are often staffed by former law enforcement personnel with significant expertise and strong motivations to help their former colleagues in the government. They generally have broad mandates to evaluate client relationships and the risks they may pose to the institution and the financial system itself. FIUs are most effective when they can be agile and adapt in real-time to threats as they develop. FIUs should be given latitude by regulators to operate outside the compliance regime, giving them the agility needed to aid law enforcement.

RECOMMENDATION. To this end, FinCEN should propose a rule stating that financial institutions are encouraged to innovate in an FIU "sandbox," and that FIUs may operate outside the strictures of regular policies and procedures.

BENEFITS. This proposal may be superfluous for financial institutions designated for FinCEN supervision, as the establishment of priorities and direct communications with the end users of SAR data would naturally cause such institutions to shift resources to priority areas like FIUs. But for any firms not so designated, the current need for prioritization would continue.

IV. DE-PRIORITIZE THE INVESTIGATION AND REPORTING OF ACTIVITY OF LIMITED LAW ENFORCEMENT OR NATIONAL SECURITY CONSEQUENCE

BACKGROUND. The goal of the SAR regime is to provide useful information about money laundering and terrorist financing to law enforcement. The ideal SAR is a well-researched, carefully-written summary of suspicious activity, which is likely to require significant time and energy on behalf of a financial institution's staff. Unfortunately, the current regime promotes the filing of SARs that may never be read, much less followed up on as part of an investigation.[13] Any diversion of resources from creating quality SARs does not truly serve the interest of law enforcement. The SAR regime should produce SAR filings that actually advance law enforcement and other national security goals.

There are two embedded issues: the first is the type of conduct that merits a SAR filing; the second is the level of suspicion or evidence of that conduct that should trigger a filing. We make recommendations with regard to the former here because there was consensus on the reforms needed. The latter is a more complicated question, and is discussed in the next section as an area in need of further review.

Presently, financial institutions are required to file a SAR on two broad categories of conduct. The first encompasses criminal violations that: (i) involve insider abuse; (ii) total at least $5,000 in which a suspect can be identified; or (iii) total at least $25,000, regardless of whether a suspect can be identified. The second encompasses 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 Bank Secrecy Act 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 (and, after examining the available facts, the financial institution knows of no reasonable explanation for the transaction).

RECOMMENDATION:

» The SAR dollar thresholds, which were set in 1996, should be raised.

» The standards for insider abuse should be eliminated. Financial institutions are the victims of these crimes, and therefore have an incentive to report any serious misconduct. Under the current standard, however, they allocate significant resources to investigating employee misconduct leading to termination and establishing a paper trail to justify a decision not to file a SAR, or an investigative record in support of a SAR. As no federal prosecutor will ever follow up on such a SAR, these resources are misallocated.[14]

» FinCEN should review all existing SAR guidance to ensure it establishes appropriate priorities. For example, FinCEN should reconsider its just-issued guidance requiring SAR filings for cyber attacks. Large financial institutions experiencing cyber attacks are already in regular, and frequently real-time communication with law enforcement and other government organizations. They are members of the Financial Services Information Sharing and Analysis Center, which is designed to facilitate cyber and physical threat intelligence analysis and sharing between stakeholders. The relevant governmental organizations will derive few incremental benefits from the filing of a post-hoc SAR; other governmental organizations will make no use of it. But financial institutions will now be taking resources away from responding to cyber attacks to documenting them in regulatory filings that may never be read.

V. PROVIDE MORE RAW DATA TO FINCEN AND FEEDBACK TO FINANCIAL INSTITUTIONS

BACKGROUND. FinCEN's e-filing system provides a common format for suspicious activity reporting, but additional data that could be useful to law enforcement are not provided in a consistent format or in real time. Furthermore, in choosing which information to include in a SAR, financial institutions necessarily bias the data available to law enforcement. For example, since each bank uses different procedures for filing SARs, the combined data set has massive amounts of noise and little information of use to law enforcement. To date, the database is used for federated searches only, and a different approach could identify strategic trends of value to law enforcement and national security personnel.

Furthermore, financial institutions generally provide underlying raw data only at law enforcement request following a SAR filing, but a better approach would facilitate real-time information flow and analysis using modern data capabilities, while adhering to privacy and civil liberty concerns as well as

managing for other risks. The provision of raw data has been considered before – though in a limited capacity. In 2006, FinCEN published a Congressional report on the *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act* in compliance with Section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004. At the time, the report found that simply implementing a cross-border funds transfer reporting requirement would require significant investment from both the public and private sectors. In particular, it was estimated that FinCEN would need approximately $32.6 million and three and a half years to make sure its system was capable of receiving such information. However, in 2015, FinCEN completed an IT Modernization Project that has likely impacted that original estimate.[15]

The ideal outcome is not each bank analyzing bulk data for a given customer and using resources to draft an elaborate and heavily audited SAR narrative. Rather, a middle ground would be a utility that allows banks to share bulk data and have it analyzed. But the best outcome would be to have bulk data deposited at FinCEN and analyzed by law enforcement and intelligence community professionals, with a mechanism for regular feedback to be provided to institutions to enable them to target their internal monitoring and tracking mechanisms to better serve the goals of law enforcement and intelligence officials.

RECOMMENDATION. Facilitate the flow of raw data from financial institutions to law enforcement, and between financial institutions, under safe harbor protections. FinCEN should require a financial institution to provide a broader set of raw data once the institution has determined that the underlying activity is suspicious. For instance, raw data about the parties to a transaction, including transaction history and such information on their other counterparties, could be shared to form clearer pictures of complex relationships, and the attributes of the parties to the transaction. Any such proposal would need to be crafted with privacy issues in mind: any potential solution would require scrubbing the data of personal identifying information, and inserting a generic identifier in its place. Current technology allows for the sharing of encrypted or hashed unique identifiers, allowing analytical integrity to be preserved while protecting personally identifiable information.

BENEFITS. Providing such data in bulk, directly to FinCEN upon the filing of a SAR, would modernize the SAR regime from one built for the 20th century, where financial institutions were comparatively better equipped to filter data, to one appropriate for the 21st century, where big data analytics could enable law enforcement to effectively sift through large quantities of data without requiring as much assistance from financial institutions in investigating illicit activity. Financial institutions could then reallocate associated resources to FIUs or other higher value activities.

VI. CLARIFY AND EXPAND THE SCOPE OF INFORMATION SHARING UNDER SECTION 314(B)

BACKGROUND. Section 314(b) of the USA PATRIOT Act provides an avenue for financial institutions to share with each other information relevant to potential money laundering or

terrorist financing investigations. In 2009, FinCEN issued guidance explaining that financial institutions are covered by the provisions of Section 314(b) when they participate in a program that "share[s] information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities ('SUAs')" as long as the purpose of the information sharing is to identify and report activities that may involve terrorist activity or money laundering.[16] In a 2012 administrative ruling, FinCEN elaborated on this guidance and distinguished between information sharing that satisfies the purpose requirement and other sharing arrangements that are not covered by Section 314(b).[17] However, the current standard requiring that information shared pursuant to 314(b) must relate to potential money laundering or terrorist financing is vague and limited given the current illicit finance risks facing financial institutions and would benefit from additional clarification.

RECOMMENDATION. Regulatory or statutory changes should encourage additional use of the 314(b) safe harbor.

» FinCEN should clarify that financial institutions can share information about clients as part of their attempt to identify suspicious activity. Such sharing should be permissible even before there is already-formed, formal suspicion of money laundering or terrorist financing. This would not be a wholesale license for financial institutions to broadly share information, but rather would be useful in situations in which one financial institution has incomplete information about a customer's AML/CFT risk and another can provide additional information that produces a fuller picture of the situation – for example, with respect to client on-boarding.

» Congress should expand the 314(b) safe harbor to cover the sharing of information related to illicit finance activities beyond money laundering or terrorist financing. For example, the safe harbor could be revised to permit sharing also for the purpose of identifying and reporting a specified unlawful activity (as defined in 18 U.S.C. 1956(c)(7)). As the Federal crimes listed in 18 U.S.C. 1956(c)(7) include crimes related to computer fraud and abuse, such a revision would protect sharing regarding cybercrimes and identity theft without requiring that financial institutions first determine whether the crime also involves money laundering or terrorist financing.

» Congress should also expand the safe harbor to cover technology companies and other nondepository institutions, to provide greater freedom to experiment with information-sharing platforms.

VII. ENHANCE LEGAL CERTAINTY REGARDING THE USE AND DISCLOSURE OF SARS

To facilitate better information flow on suspicious activity among public and private institutions, financial institutions must be confident in the current confidentiality regime for SAR-related data, including at the enterprise-wide level and across borders.

BACKGROUND. FinCEN regulations generally prohibit the disclosure of SARs and information

that would reveal the existence of a SAR ("SAR information"), with an exception for sharing "within the bank's corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act as determined by regulation or guidance."[18] In 2006, FinCEN and the federal banking agencies issued guidance providing that a U.S. depository institution may share SAR information with its controlling company (whether foreign or domestic), and that a U.S. branch or agency of a foreign bank may share SAR information with its foreign head office.[19] FinCEN reaffirmed portions of this guidance in 2010 when it issued new guidance permitting U.S. depository institutions to share SAR information with affiliates subject to U.S. SAR regulations (i.e., U.S.-based affiliates).

FinCEN regulations explicitly provide that depository institutions are not prohibited from disclosing the underlying facts, transactions, and documents upon which a SAR is based within the bank's corporate organizational structure.[20] Thus, on its face, the regulations would appear to permit depository institutions to share such information with foreign branches and foreign affiliates. Such sharing should be allowed, particularly where the foreign affiliates are subject to confidentiality agreements or located in FATF-member countries. However, FinCEN guidance does not permit U.S. depository institutions to share SAR information with foreign branches, and, in light of commentary by FinCEN on this topic, the scope of the exception for disclosing underlying information is not entirely clear. For example, in a 2010 final rule, FinCEN indicated that "[d]ocuments that may identify suspicious activity but that do not reveal whether a SAR exists (e.g., a document memorializing a customer transaction, such as an account statement indicating a cash deposit or a record of a funds transfer), should be treated as falling within the underlying facts, transactions, and documents upon which a SAR may be based, and should not be afforded confidentiality."[21] Yet, other language in the Supplementary Information might be read as limiting the exception to information produced in the ordinary course of business.[22] Thus, there is confusion about the extent to which the exception covers facts, descriptions of transactions, and documents that both: (i) underlie a SAR; and (ii) are recited or referenced in, or attached to, a SAR, including with respect to sharing such underlying facts, transactions, and documents with foreign branches and foreign affiliates.[23]

The issue here is not limited to lack of clarity in the U.S. regime, and negotiation with foreign regulators would be important to rationalizing the process.

RECOMMENDATION. FinCEN should:

» By regulation, clearly authorize U.S. depository institutions to share SARs with a foreign branch or affiliate if the branch or affiliate is located in a country that is a member of the FATF.

» For non-FATF countries, establish a clear standard (or list of approved or disapproved countries) that would allow institutions to share SARs within such a country if the U.S. depository institution enters into a written confidentiality agreement with the branch or affiliate that is consistent with the 2006 interagency guidance for SAR

sharing with controlling companies and head offices.[24] While there may be countries of sufficient concern that any information shared could be interdicted and misused, the general presumption should be towards information sharing within an institution.

» By regulation, clearly authorize U.S. depository institutions to share the underlying facts, transactions, and documents upon which a SAR is based with foreign branches and foreign affiliates.

» Encourage other FATF-jurisdictions to adopt policies that apply a substantially consistent standard. [25]

BENEFITS. A less restricted flow of AML information within a banking enterprise would result in:

- better transaction monitoring;
- higher quality SARs;
- better information for law enforcement investigations;
- better knowledge of international money laundering and terrorist financing trends;
- easier implementation of a risk-based, enterprise-wide approach to AML, including mitigating the risk of illicit actors abusing different entities within multinational institutions; and
- efficiencies in the process of preparing SARs, greater uniformity in SARs filed by a banking enterprise, and minimization of duplicative SAR filings.

ISSUES. The major concerns motivating SAR-sharing restrictions relate to the importance of protecting the confidentiality of SARs, which is a legitimate policy goal. However, globally active banking organizations are able and required to employ increasingly sophisticated controls to protect the confidentiality of sensitive information, and those controls have proven effective. Thus, the benefits of allowing institutions to share SARs within their organizations and information that would reveal the existence of a SAR clearly outweigh the risks of such information being inappropriately released.

Areas of Reform Requiring Further Study

The following are reforms that would bring substantial benefits, but warrant further study and the input of a wide array of stakeholders. In some cases—for example, the standard for SAR filings—the issue is extremely complex; in others—for example, the use of utilities — concerns with privacy and data security would need to be resolved.

I. ENHANCE INFORMATION SHARING

BACKGROUND. The theory behind the SAR regime is that financial institutions have vast amounts of information about their customers and are thus best positioned to identify and report suspicious activity. However, the current system encourages stove-piping of information that inhibits the dynamic flow of information among authorities and institutions and limits the ability of any one institution to see the bigger picture. Visibility into information from authorities and peer institutions would provide helpful context to financial institutions and law enforcement.

RECOMMENDATION. Establish AML/Sanctions utilities for information sharing beyond 314(b) sharing. A utility-like database of AML and/or sanctions information gathered from multiple public and private sources has the potential to make the sharing of information among financial institutions and law enforcement more efficient and effective. An AML/sanctions utility would facilitate the bulk screening of transactions against sanctioned and suspect parties and the detection of patterns of potentially suspicious transactions on a real-time basis across multiple financial institutions. This model could have a government agency, such as FinCEN, at the center, or it could rely on a private-sector actor or consortium acting as a clearinghouse. To support such a utility and other outcomes, consideration should be given to the creation of industry forums through which banks and other stakeholders may share resources and collaborate to: (i) address new risks and regulations in a consistent, cost effective manner; (ii) engage in efforts to benchmark with each other, share ideas, and harmonize standards; and (iii) incubate and test collaboration and utility ideas. Such forums could also serve as the vehicle for public/private cooperation on the development of industry utilities.

BENEFITS. Both public and private sector participants have suggested that AML or sanctions utilities have the potential to: (i) better detect illicit or prohibited activity by looking at a wider set of data, including, for example, by examining both sides of a transaction or comparing transactions across multiple financial institutions; (ii) allow the industry to shift resources to more productive uses; and (iii) improve efficiency and enable more consistent compliance approaches across financial institutions of all sizes. A KYC utility could, for instance, be responsible for running adverse media searches on clients, rather than imposing such a duty on every financial institution at which the relevant party holds an account; such an approach would be more efficient, cost-effective, and allow for resources to be allocated to more fruitful investigations.

ISSUES. While there has already been some success in implementing utilities such as Clarient and SWIFT's KYC Registry, efforts to establish utilities have been hampered by regulatory concerns, implementation and operational challenges, and liability concerns as well as the need for further regulatory support and oversight.

» **REGULATORY CONCERNS.** One regulatory concern is reliance. In order to be effective, financial institutions must be able to rely on the information and functions provided by a utility. Time and resources required

to re-validate information or re-perform functions coming from a utility will reduce efficiency, which is a key benefit of utilities. Another is potential regulatory criticism. Financial institutions should be afforded an opportunity to experiment with processes and controls that leverage collaboration and utility models. Without some regulatory flexibility and protection of experimentation, the long-term gain that could be achieved by a utility may be stifled by short-term regulatory risk. Potential solutions to this problem include placing the KYC utility within FinCEN's jurisdiction or making it a government entity.

» **IMPLEMENTATION AND OPERATIONAL CHALLENGES.** The purpose and functionality of a utility must be clearly defined to ensure the utility will be more efficient than individual, in-house systems. Financial institutions must resolve differences in standards, definitions, and processes, and align on technology and data in order for utilities to operate efficiently.

» **LIABILITY CONCERNS.** One possible issue with either a public or private database is potential liability associated with inaccurate information, including in the context of negative news. The impact of such inaccurate information may be multiplied by the tacit endorsement it would receive from its inclusion in the utility or the reports generated by the utility. A safe harbor could be of help here.

» **REGULATORY SUPPORT AND OVERSIGHT.** Utilities will not be effective unless regulators provide meaningful assurance that financial institutions can rely on the information provided by utilities for the fulfillment of certain of their compliance obligations. Regulatory encouragement of and oversight over utilities would provide confidence to the financial services industry and facilitate reliance on such a system. The FFIEC's Multi-Regional Data Processing Servicer program could serve as a model for regulatory oversight of an AML/sanctions utility.

II. PROVIDE BETTER PROTECTION FROM DISCOVERY FOR SAR INFORMATION

BACKGROUND. As the agencies have stated in the FFIEC BSA/AML Examination Manual, under the current regime, the provision of suspicious activity information by financial institutions "is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. . . . [and] the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system."[26] The effectiveness of this monitoring and reporting system depends in large part on the confidentiality restrictions and protections afforded SARs and related materials.[27] Banks take seriously their obligation to help law enforcement, but to perform their job under the current regulatory framework, they need to prepare investigatory materials for the purpose of identifying suspicious activity and determining whether to file a SAR ("SAR Investigatory Materials"). SAR Investigatory Materials include, but are not limited to:

- documents representing drafts of SARs;

- documents memorializing communications that are a part of the investigation of unusual or potentially suspicious activity;

- reports of or internal communications related to unusual or potentially suspicious activity on which SAR reporting may be required (whether generated automatically or manually);

- documents and forms generated by a bank as part of its internal process of determining whether to file a SAR;

- documents relating to a bank's monitoring and investigations to detect unusual or potentially suspicious activity, including descriptions of SAR filing procedures and descriptions of suspicious activity monitoring and investigation policies, procedures, methods and models;

- information about technology and about system alerts used by a bank for suspicious activity monitoring;

- any documents created for the purpose of informing, assessing or reporting (internally) on the bank's SAR investigatory process; and

- pre- and post-SAR communications with law enforcement, including hold harmless letters, law enforcement requests for back-up documentation, and grand jury subpoenas.

Several courts have interpreted "information that would reveal the existence of a SAR" to mean more than documents that indicate whether a SAR has been filed, but others continue to misinterpret this standard on the mistaken belief that documentation produced in the ordinary course of business is not entitled to confidentiality protection even if the business at hand is investigating suspicious activity or potential SAR filings.[28] Therefore, banks are increasingly wary that information about their efforts to identify criminal behavior will be revealed, including through litigation or arbitration. Further, these decisions are likely to ultimately: (i) inhibit the robust investigative processes that banks undertake today in an effort to make their SARs as useful as possible to law enforcement; and (ii) undermine the industry's ability to effectively detect and report suspicious activity by revealing the techniques and processes they use.

RECOMMENDATION. Congress should enact legislation making clear that SAR Investigatory Materials are to be treated as confidential, particularly in private litigation.[29] An alternative approach could be the issuance of guidance to this end by FinCEN jointly with the federal financial regulators.

BENEFITS. The disclosure of SAR information in private litigation could undermine the ability of financial institutions to effectively combat financial crimes by compromising ongoing investigations, chilling financial institutions' willingness to file detailed SARs, and revealing the financial institution's process for analyzing and reporting such data. Thus, this legislation could help both to allow financial institutions to continue filing the most helpful SARs possible, and protect bad actors from discovering their methods for doing so.

ISSUES. Some believe that litigants and others have a right to information potentially contained in SAR Investigatory Materials for a variety of reasons, some of which could be considered in the proposed legislation.[30]

III. CLARIFY AND BALANCE THE RESPONSIBILITY OF THE PUBLIC AND PRIVATE SECTOR TO DETECT AND PREVENT FINANCIAL CRIME

BACKGROUND. The current AML/CFT statutory and regulatory regime does not clearly allocate responsibility for detecting and preventing financial crime between the public and private sectors. The current system creates incentives for financial institutions to de-risk, thereby withdrawing financial services to already underserved populations and pushing transactions out of the traditional financial services sector into shadow banking channels that are not monitored for suspicious activity. The result of this de-risking is to deprive law enforcement of valuable intelligence. De-risking may also perpetuate political and economic instability in already unstable regions, potentially giving rise to terrorism and criminal activity in the absence of legitimate economic opportunities.

Government intervention is needed to reverse the de-risking trend and better allocate money laundering and terrorist financing risk. For instance, in recent months, Treasury and the federal banking agencies have issued a joint fact sheet on foreign correspondent banking and AML/CFT and sanctions supervision and enforcement.[31] The OCC followed with a Bulletin on *Risk Management Guidance on Periodic Risk Reevaluation of Foreign Correspondent Banking*.[32] These statements indicate a recognition of the problems caused by de-risking, but do not provide a workable solution. Rather than providing assurances that an enforcement action will not result from maintaining accounts for customers based in countries considered high risk, these proposals could be read as imposing, without a basis in law, a new legal obligation, and potential liability: not to de-risk.

As noted above, the most effective way to reduce inappropriate de-risking is to change the way internationally active banks are supervised, giving voice to the numerous government agencies that would prefer that U.S. banks remain engaged abroad – whether in correspondent banking, facilitating payments through money-service businesses, or supporting NGOs. We believe that step is necessary and may even be sufficient. However, the below initiatives could also better align responsibility and encourage innovation in the financial sector.

IV. ESTABLISH A PROCEDURE AND RESOURCES FOR NO-ACTION LETTERS

BACKGROUND. There is no established mechanism by which financial institutions can query FinCEN about certain actions and receive, if warranted, confirmation that no enforcement would be initiated if they are undertaken. The SEC has established such a procedure, the no-action letter, to ensure that the financial institutions it regulates have access to the government's perspective on complicated issues.[33]

RECOMMENDATION. FinCEN should provide a no-action letter mechanism for financial institutions to pose compliance questions in a format designed to promote efficiency. Regulators would be empowered to grant a prospective shield from liability on a question posed, provided that the facts represented are substantially accurate and any conditions set are followed. In considering the response, regulators and law enforcement would discuss the merits of particular inquiries.

BENEFITS. While rulemaking and the issuance of guidance are cumbersome processes that do not always promote innovation or dialogue with the industry, a no-action letter process could be more effective. It would (i) allow individual financial institutions to ask particular questions about actions they plan to take, thereby spurring innovation; (ii) provide quick answers, thereby promoting dynamism; and (iii) increase the flow of information from industry to FinCEN about new technologies and procedures, thereby improving information for FinCEN's rulemaking and enforcement purposes.

ISSUES. Although such a proposal would protect against the risk of enforcement by FinCEN, OFAC, and the federal examiners for potential violations of the Bank Secrecy Act or OFAC sanctions, it would not necessarily eliminate liability from state or foreign regulatory authorities. However, coordination through bilateral negotiations or forums such as the FATF might encourage global cooperation that would provide real assurance to financial institutions willing to certify their AML compliance programs. In addition, FinCEN would likely need to be provided with additional resources to implement such a mechanism – though such a change would ultimately achieve efficiency gains for the broader regime. Consideration should also be given to whether there are areas where state law should be preempted.

V. PROVIDE CLEAR STANDARDS TO FINANCIAL INSTITUTIONS

BACKGROUND. Financial institutions currently operate under a strict liability, post-hoc regulatory standard that is both opaque and constantly changing. As a result, they have been forced, in many cases, to deemphasize innovation and the pursuit of real AML/CFT risk, and instead focus on adherence to examiner-approved policies and procedures. They "work to the rule" in the worst sense, because this is the best way to insulate themselves from liability. The AML/CFT regime should be geared toward law enforcement outcomes, not only compliance processes.[34]

In addition to the above proposed reforms to the supervision of financial institutions, other steps could be taken.

RECOMMENDATION.

1. FinCEN should establish by regulation a clearer definition of what constitutes a reasonable AML/CFT program, including what conduct will result in an enforcement action or prosecution. If a financial institution engages in compliance conduct that a regulator deems acceptable ex ante and illicit financial activity still occurs, the issue can be addressed through discussions between financial institutions and their regulators, with no enforcement action taken.

2. FinCEN could also provide clear assurances that any sanction imposed will come only after a holistic review of the financial institutions' overall performance, and in no case be based on the failure to file a single SAR, unless the failure to file was found to be willful. Rather, any significant sanction should be based on a pattern or practice of noncompliance.

Additional, detailed guidance from FinCEN is necessary with respect to the following topics:

- **DUE DILIGENCE ON CUSTOMERS OF CUSTOMERS.** Although FinCEN's recent customer due diligence rule explains the circumstances in which financial institutions must identify beneficial owners of legal entity customers, there is still considerable confusion about the extent of due diligence financial institutions must conduct on the customers of their customers in order to conduct what examiners consider a reasonable AML compliance program.

- **RELIANCE.** Similarly, FinCEN could clarify the extent to which a financial institution can reasonably rely on work done by another financial institution, or by a utility or collection of institutions; absent a clear safe harbor, the examination process is likely to nullify any efficiency gains by requiring that work be duplicated.

- **MONITORING FOR CONTINUING SUSPICIOUS ACTIVITY.** FinCEN has issued guidance on when financial institutions should file SARs on suspicious activity of a continuing nature, but the financial industry would benefit from additional, more detailed guidance about FinCEN's expectations for ongoing monitoring for the purpose of detecting and reporting continuing suspicious activity. In other words, what specific monitoring, if any, should financial institutions do, above and beyond their regular transaction monitoring once they have filed a SAR on a given customer or account, in order to determine whether the activity reported in the initial SAR is of a continuing nature.

- **WHEN DOES A FINANCIAL INSTITUTION HAVE REASON TO SUSPECT A TRANSACTION IS SUSPICIOUS?** Financial institutions are required to file SARs when they "know, suspect, or have reason to suspect" that a transaction is suspicious. But if a financial institution does not actually know or suspect that a transaction is suspicious, under what circumstances can a regulator infer that the financial institution had reason to suspect a transaction was suspicious? FinCEN should provide guidance on this important issue.

BENEFITS. Unclear standards result in financial institutions devoting compliance and legal resources to divining regulators' meaning, instead of focusing on investigating and reporting suspicious activity. Such unclear standards lead any rational actor to err on the side of caution, resulting in the defensive filing of SARs at the expense of higher value compliance activities and law enforcement outcomes. These concerns are sharpened in the current enforcement environment, which increasingly focuses on holding individuals liable for alleged programmatic issues.

VI. BETTER COORDINATE AML/CFT AND SANCTIONS POLICY GOALS, SUPERVISION AND ENFORCEMENT

BACKGROUND: The AML and sanctions compliance regimes are increasingly interdependent, even if their aims are not always consistent. Regulators treat AML and OFAC compliance as related, as demonstrated by the FFIEC BSA/AML Examination Manual, which contains a section on OFAC compliance and examination procedures. A recent regulation issued by the New York State Department of Financial Services addresses both AML transaction monitoring programs and OFAC filtering programs.[35] Examiners and auditors often test both AML and sanctions compliance programs together, and enforcement actions frequently allege violations of both the Bank Secrecy Act and OFAC sanctions.

This has led many large financial institutions to treat AML and OFAC compliance as related disciplines that, along with anti-bribery and corruption, fall within the realm of financial crimes compliance. They employ similar tools to deal with both AML and OFAC compliance. For example, customer due diligence procedures must address screening customers against sanctions watch lists and for indicia of money laundering or terrorist financing risk.

At the U.S. Treasury, both FinCEN and OFAC are housed within TFI, reporting to its undersecretary. Prior to 2002, when Section 361 of the USA PATRIOT Act made FinCEN a separate bureau of the Treasury, both FinCEN and OFAC were sister offices within Main Treasury. Today, FinCEN is a bureau, while OFAC is still a Main Treasury office. The Office of Terrorist Financing and Financial Crimes (TFFC)—also a component of TFI within Main Treasury—is responsible for coordinating policy with respect to the full spectrum of illicit finance threats. Over time, some of the prior synergies between FinCEN and OFAC may have been lost as FinCEN has become increasingly independent.

Additionally, the aims of the sanctions and AML/CFT regimes can, at times, also work at cross-purposes, excluding from the financial system the very bad actors most likely to conduct suspicious activity that is ultimately reported to law enforcement.

RECOMMENDATION: Better coordination would help reconcile competing U.S. government priorities and align their effect on financial institutions, while creating efficiencies.

For example, Treasury could speak with one voice regarding regulatory expectations with respect to illicit finance, helping to better address the competing policy goals of excluding certain bad actors from the financial system while also providing valuable financial intelligence to law enforcement.

As noted above, one way to accomplish these aims would be to strengthen TFI, particularly with respect to its oversight of FinCEN and OFAC. Empowering TFI to truly coordinate policy and enforcement across both FinCEN and OFAC would ensure that Treasury policy goals all move in one direction with little drag. TFI could also be given a more visible role in industry outreach.

VII. MODERNIZE THE SAR REGIME

BACKGROUND. As described in an earlier recommendation, standards for SAR filings have incentivized filing SARs on activity that prosecutors are unlikely to pursue. We recommend changing the type of activity that merits a SAR filing. An equally important, but more complicated question, is the level of suspicion of that activity that should merit a filing. Obviously, that could vary from merest suspicion to absolute certainty, and it is a difficult but important task to determine where on that spectrum the standard should be set.

RECOMMENDATION. Another approach would be for FinCEN to further elaborate on the reporting criterion for what is deemed "suspicious" – whether it be illicit activity, criminal activity, or activity that is clear evidence of one of these categories. Furthermore, it would be helpful if the aforementioned guidance also provided contours for SARs that should not be filed. Further elaboration of the SAR-filing standard would relieve financial institutions of the need to file SARs on activity that is merely suspicious without an indication that such activity is illicit. Whether a financial institution perceives an activity as "suspicious" is inherently subjective, and a bright-line approach would take the subjective guesswork out of SAR filing. However, there are some significant drawbacks, requiring SAR filings only in cases of a more objective standard—such as illicit or criminal activity—requires legal analysis that is not currently required and may actually prove to be more burdensome than the current regime.

Changing the SAR filing thresholds would also require modifying multiple statutes, including the Bank Secrecy Act and the Federal Deposit Insurance Act, and implementing regulations thereunder.

Conclusion

As decribed above, the stakes are high. Under the current AML/CFT statutory and regulatory regime, the nation's financial firms play an integral role in preventing, identifying, investigating, and reporting criminal activity, including terrorist financing, money laundering and tax evasion. Yet, today, most of the resources devoted to AML/CFT compliance by the financial sector have limited law enforcement or national security benefit, and in some cases cause collateral damage to other vital U.S. interests. A redeployment of these resources could substantially increase the national security of the country and the efficacy of its law enforcement and intelligence communities, and enhance the ability of the country to assist and influence developing nations.

Endnotes

1 *See* PwC Global Anti-Money Laundering, *available at:* **http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/anti-money-laundering.html** ("According to new figures from WealthInsight, global spending on AML compliance is set to grow to more than $8 billion by 2017"); FBI FY 2017 Budget Request at a Glance, *available at:* https://www.justice.gov/jmd/file/822286/download; ATF FY 2017 Budget Request at a Glance, *available at* **https://www.justice.gov/jmd/file/822101/download**.

2 *See* The Center for Global Development's report entitled "Unintended Consequences of Anti-Money Laundering Policies for Poor Countries," Table 1, found on Page 8, for a sampling of some of the federal government entities involved in AML/CFT. In addition, many state government entities are imposing standards.

3 While various documents are released by governmental and multinational entities providing guidance on AML/CFT issues or further elaborating on the current state of AML/CFT risks, like the U.S. Treasury's *2015 National Money Laundering Risk Assessment*, diffuse FinCEN guidance and FATF typologies, none provides a clear set of priorities for U.S. financial institutions as they seek to assist law enforcement in their AML/CFT efforts.

4 Multiple participants reported that examiners have developed expected ratios of alerts to SARs, though such ratios have never been published for notice and comment.

5 *See* National Crime Agency, Joint Money Laundering Intelligence Taskforce, **http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit**. While in the United States, the Treasury Department has a Bank Secrecy Act Advisory Group (BSAAG), it has not taken on an operational role.

6 *See* 31 C.F.R. § 1010.810. "Overall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter, is delegated to the Director, FinCEN." *Id*. § 1010.810(a). *See* also 12 U.S.C. § 1818(s).

7 *See* Commercial Banks in the U.S., Economic Research of the Federal Reserve Bank of St. Louis, *available at:* **https://fred.stlouisfed.org/series/USNUM**.

8 While FinCEN would be free to adopt its own definition and decision, existing banking law already provides ways of making such a determination; in other words, this is not a novel concept.

9 It should be noted that even if FinCEN were to revoke its delegated exam authority, the federal banking agencies would have additional statutory authorities under which they would likely still be required to conduct exams for AML/CFT compliance. However, in order to further streamline and centralize the examination of large multinational institutions, there appears to be no reason why they would not be able to delegate such authorities to FinCEN.

10 The Independent Offices Appropriation Act provides general authority for a government agency to assess user fees or charges by administrative regulation, based on the value of the service to the recipient. *See* 31 U.S.C. § 9701. OMB Circular No A-25 provides further guidance regarding "user fees" ("A user charge . . . will be assessed against each identifiable recipient for special benefits derived from Federal activities beyond those received by the general public."). *See* OMB Circular No. A-25 Revised.

11 *See*, e.g., 12 U.S.C. §§ 1786(q), 1818(s)(2).

12 *See* FATF Anti-money laundering and counter-terrorist financing measures, Mutual Evaluation of the United States, December 2016, pg. 11; *available at:* **http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf**. FATF also noted that "deficiencies in [customer due diligence] requirements (in particular [beneficial ownership] requirements) can undermine the usefulness of SARs," FATF 2016 Mutual Evaluation of the United States, pg. 58.

13 As noted in note 12, FATF found that "deficiencies in [customer due diligence] requirements (in particular [beneficial ownership] requirements) can undermine the usefulness of SARs" in the United States. FATF 2016 Mutual Evaluation of the United States, pg. 58.

14 An alternative mechanism for reporting insider abuse to the banking regulators could be established, as necessary.

15 In a speech in October 2015, former FinCEN Director Jennifer Shasky Clavery stated that through the IT modernization program "(1) we assumed responsibility for maintaining our own data in a FinCEN system of record; (2) we supported a significant shift from the paper filing of BSA reports to the electronic filing of BSA data; (3) we developed a new IT system for our many law enforcement and regulatory partners to search, slice, and dice BSA data; and (4) we provided advanced analytics tools to FinCEN's analysts to enhance their capabilities to make sense of the data. *Available at:* **https://www.fincen.gov/news/speeches/jennifer-shasky-calvery-director-financial-crimes-enforcement-network-4**."

16 FinCEN, *Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act*, FIN-2009-G002 (June 16, 2009).

17 FinCEN, *Administrative Ruling Regarding the Participation of Associations of Financial Institutions in the 314(b) Program*, FIN-2012-R006 (July 25, 2012) ("[I]nformation shared for the purposes of identifying fraud or other specified unlawful activity that is not related to a transaction involving the possibility of money laundering and/or terrorist financing is not covered by the statutory safe harbor.").

18 31 C.F.R. § 1020.320(e)(1)(ii)(B).

19 Interagency Guidance, Sharing Suspicious Activity Reports with Head Offices and Controlling Companies (Jan. 20, 2006).

20 31 C.F.R. § 1020.320(e)(1)(ii)(A)(2).

21 75 Fed. Reg. 75593, 75595 (Dec. 3, 2010).

22 *Id*. at n. 13 ("As one commenter correctly suggested, information produced in the ordinary course of business may contain sufficient information that a reasonable and prudent person familiar with SAR filing requirements could use to conclude that an institution likely filed a SAR (e.g., a copy of a fraudulent check, or a cash transaction log showing a clear pattern of structured deposits). Such information, alone, does not constitute information that would reveal the existence of a SAR.")

23 For avoidance of doubt, please note that this group is not requesting guidance with respect to the confidentiality of SARs themselves, or even draft SARs, or documents produced in the course of a depository institution's transaction surveillance procedures or investigation of whether to file a SAR – all of which are confidential under 31 C.F.R. § 1020.320(e)(1)(i).

24 Interagency Guidance, Sharing Suspicious Activity Reports with Head Offices and Controlling Companies (January 20, 2006).

25 FATF has advised the U.N. Security Council that the need for enhanced information sharing globally is critical in order to enhance the ability to combat terrorism and, in particular, to defeat ISIL. *See* **http://www.fatf-gafi.org/publications/fatfgeneral/documents/importance-urgent-action-to-implement-fatf-standards-counter-terrorist-financing.html**

26 FFIEC BSA/AML Examination Manual (2014), 60.

27 *See* 31 U.S.C. § 5318(g)(2) and 31 C.F.R. § 1020.320(e); 12 C.F.R. § 21.11(k).

28 *See* 31 C.F.R. § 1020.320(e); 12 C.F.R. § 21.11(k). FFIEC BSA/AML Examination Manual (2014), 73 ("A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill Bank Secrecy Act obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR"). *See also Cotton v. PrivateBank & Trust Co*., 235 F. Supp. 2d 809, 814-15 (N.D. Ill. 2002) (holding that documents representing drafts of SARs or other work product or privileged communications that relate to the SAR itself are confidential); *Whitney National Bank v. Karam*, 306 F. Supp. 2d 678, 683 (S.D. Tex. 2004) (holding that SAR confidentiality protects "discussions leading up to . . . the preparation of filing of a SAR or other form of report of suspected or possible violations."); *but see First Am. Title Ins. Co. v. Western Bank, No. 12-CV-1210*, 2014 U.S. Dist. LEXIS 121063 at *5 (E.D. Wis. August 29, 2014) (allowing production of fraud alerts, including information automatically generated by fraud monitoring software, because "[n]ot all means or methods a bank may use to detect fraud or other financial irregularity are privileged simply because they might culminate in a SAR."); *Freedman & Gersten, LLP v. Bank of America, N.A.*, 09-cv-5351, 2010 U.S. Dist. LEXIS 130167 at *10 (D.N.J. Dec. 8, 2010)(holding that "general policies and procedures concerning the handling of suspicious activity," and "any memoranda or documents drafted in response to the suspicious activity" are not entitled to protection because they merely reflect the bank's "standard business practice" for investigating suspicious activity).

29 The term "bank" as used in this section has the meaning given to it in 31 C.F.R. § 1010.100(d).

30 *See* , e.g., Wultz v. Bank of China, 56 F. Supp. 3d 598, 602-603 (S.D.N.Y. 2014) (case brought by Wultz family against Bank of China for terrorist-related death of family member, alleging that a customer of BOC, Said al-Shurafa ("Shurafa"), was a senior operative of the terrorist group responsible for the bombing and that BOC assisted Shurafa by executing dozens of wire transfers on his behalf totaling several million dollars).

31 *See* "Joint Fact Sheet on Foreign Correspondent Banking," August 30, 2016. *Available at:* **https://www.treasury.gov/press-center/press-releases/Documents/Foreign%20Correspondent%20Banking%20Fact%20Sheet.pdf**.

32 *See* OCC Bulletin 2016-32, "Risk Management Guidance on Foreign Correspondent Banking," October 5, 2016. *Available at:* **https://www.occ.gov/news-issuances/bulletins/2016/bulletin-2016-32.html**.

33 FinCEN has established a process for issuing "administrating rulings." FinCEN has explained that "[i]n conformance with the procedures outlined at 31 CFR § 1010.710-717, we will issue administrative rulings interpreting regulations contained in Chapter X either unilaterally or in response to specific requests made and submitted to us consistent with the procedures outlined at 31 CFR § 1010.711. Administrative letter rulings . . . are issued pursuant to our authority as the administrator of the Bank Secrecy Act, if the facts and circumstances, issues, and analyses that appear in an administrative letter ruling are of general interest to financial institutions then the letter ruling is published on our website. Published letter rulings often express an opinion about a new issue, apply an established theory or analysis to a set of facts that differs materially from facts or circumstances that have been previously considered, or provide a new interpretation of Title 31 of the United States Code, or any other statute granting FinCEN authority. *See* **https://www.fincen.gov/sites/default/files/shared/regrelease.pdf** . By contrast, the SEC has explained that "[a]n individual or entity who is not certain whether a particular product, service, or action would constitute a violation of the federal securities law may request a "no-action" letter from the SEC staff. Most no-action letters describe the request, analyze the particular facts and circumstances involved, discuss applicable laws and rules, and, if the staff grants the request for no action, concludes that the SEC staff would not recommend that the Commission take enforcement action against the requester based on the facts and representations described in the individual's or entity's request." *See* **https://www.sec.gov/answers/noaction.htm**

34 In its Mutual Evaluation of the United States, FATF concluded that "there is a need for more and ongoing guidance from supervisors to industry on their regulatory expectations." FATF 2016 Mutual Evaluation of the United States, pg. 135.

35 *See* New York State Register Notice, *Regulating Transaction Monitoring and Filtering Systems Maintained by Banks, Check Cashers and Money Transmitters*, New York Department of Financial Services, July 20, 2016.

ABOUT THE CLEARING HOUSE

The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates back to 1853. The Clearing House Association L.L.C. is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system. Its affiliate, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Payments Company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume.