American Bankers Association
Building Success. Together.

Robert G. Rowe, III
Vice President & Senior Counsel
Regulatory Compliance and Policy
Phone: 202-663-5029
E-mail: rrowe@aba.com

Rob Strand
Vice President & Senior Economist
Economic Policy and Research
Phone: 540-424-8600
E-mail: rstrand@aba.com

June 11, 2021

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency 400
7th Street SW, Suite 3E–218
Washington, DC 20219.
Docket No. OCC–2020–0047

Melane Conyers-Ausbrook
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314–3428
Docket No. NCUA–2021–0007
RIN 3133–AF33

Ann Misback
Secretary
Board of Governors of the Federal
Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
Docket No. OP–1744

Policy Division
Financial Crimes Enforcement Network
Post Office Box 39
Vienna, VA 22183
Docket No. FINCEN–2021–0004

James P. Sheesley
Assistant Executive Secretary
Attention: Comments—RIN 3064–ZA23
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429
RIN 3064–ZA23

Re: Request for Information and Comment: Extent to Which Model Risk Management Principles Support Compliance with Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Requirements[1]

Dear Sirs and Mesdames:

The American Bankers Association (ABA)[2] appreciates the opportunity to comment on the request for information on the degree to which the principles discussed in the *Interagency*

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, "Request for Information and Comment: Extent to Which Model Risk Management Principles Support Compliance With Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Requirements," 68 Federal Register 18978, April 12, 2021, www.govinfo.gov/content/pkg/FR-2021-04-12/pdf/2021-07428.pdf.

[2] *The American Bankers Association is the voice of the nation's $22.5 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $18 trillion in deposits and extend nearly $11 trillion in loans.*

Supervisory Guidance on Model Risk Management (*MRMG*) support Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and Office of Foreign Assets Control (OFAC) compliance. Due to the unique nature of BSA/AML and OFAC compliance arising from the variability and highly dynamic nature of risks in those areas, the application of the *MRMG* principles has been challenging for many banks. While ABA recommends that there be no changes to the *MRMG* principles, we believe that additional clarity is needed, such as examples to distinguish between rules and models, when adjustments to models should be considered material, and when and how frequently model validation is necessary. The Interagency Statement also should make clear that BSA/AML and OFAC systems should not be preemptively presumed to be models subject to risk management per the MRMG when a bank can demonstrate that this risk is managed effectively by BSA/AML and OFAC compliance.

<u>Background</u>

On April 4, 2011, the Board of Governors of the Federal Reserve and Office of the Comptroller of the Currency (OCC) released *Supervisory Guidance on Model Risk Management* (*MRMG*) as a set of guidelines for bankers and supervisors to use to assess the management of model risk. The FDIC adopted the *MRMG* on June 7, 2017.[3] From a model risk perspective, the *MRMG* has worked well, and bankers involved in model risk management (MRM) find it helpful and comprehensive.

However, for a number of years, bankers involved with BSA/AML and OFAC compliance have raised questions about the use of various applications in compliance programs. They have sought clarity about how the *MRMG* applies, specifically as to which systems qualify as models under the *MRMG*, the steps needed to review and validate those that qualify as models (as well as those that do not), when seemingly minor changes call for testing, the frequency of testing, and when updates trigger revalidations. Their primary concern has been that, while the *MRMG* is useful, it does not make clear how it applies for the unique attributes of BSA/AML and OFAC compliance.

On April 9, 2021, the Federal Banking Agencies, after consultation with both the Financial Crimes Enforcement Network (FinCEN) and the National Credit Union Administration (NCUA), (collectively, the Agencies) issued a joint statement to address these concerns and explain how the risk management principles of the *MRMG* apply to the systems and models banks use to comply with BSA, AML and OFAC laws and regulations. The *Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance* (*Interagency Statement*)[4] emphasizes that it does not change existing BSA/AML or OFAC expectations; nor does it impose any specific model risk management framework. Instead, its intent is to supplement the *MRMG* with additional information about how the *MRMG* principles apply to the unique attributes of BSA/AML and OFAC compliance.

<u>Key Recommendations</u>

ABA appreciates the Agencies' acknowledgment in the *Interagency Statement* that the *MRMG* does not alter a bank's legal or regulatory BSA/AML or OFAC obligations or establish new supervisory expectations. We also appreciate the Agencies' recognition that not all banks use models or have formalized MRM frameworks, and that banks do not need to change their existing risk management practices if they are effectively managing BSA/AML and OFAC risk.

---

3 *Supervisory Guidance on Model Risk Management*, <u>OCC 2011-12</u>, <u>SR 11-7</u>, and <u>FDIC FIL-22-2017</u>.
4 <u>www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210409a2.pdf</u>

Instead, the *Interagency Statement* is designed to clarify how, in appropriate circumstances, the *MRMG* can be a resource to guide a bank's risk management framework for BSA/AML and OFAC compliance.

Model risk managers believe that the *MRMG* works well and caution against changes, particularly any which would create new supervisory expectations. Bankers responsible for BSA/AML and OFAC compliance agree, but they welcome the additional guidance. However, they have identified issues that they urge the Agencies to elaborate on or add to the *Interagency Statement*.

An overarching purpose for the *Interagency Statement* should be to provide clarification in support of efficient and effective compliance with the BSA/AML and OFAC rules. It should therefore support use of internally developed or third-party systems that employ models, which can be important tools for this compliance. It should also clearly acknowledge that effective compliance systems can be deployed which are not models but rules-based applications. In discussions on this request for information, bankers identified areas where confusion, misguided interpretations, and conflicting guidance for bankers and their supervisors have made use of such systems burdensome, impeded flexible adjustments, and otherwise undermined their effectiveness. ABA recommends the following to forestall misinterpretations and support better compliance with the BSA/AML and OFAC rules.

- The *Interagency Statement* should clearly acknowledge that a bank should decide on its own about the application of the *MRMG* to BSA/AML and OFAC systems because its unique risk profile is best understood internally.

- Examples would help bankers and supervisors understand the distinction between a business rule and a model that is subject to validation and testing under the principles of the *MRMG*.

- Supervisors should not presume that the *MRMG* applies to all of a bank's BSA/AML and OFAC compliance systems, as this may interfere with its ability to effectively and efficiently manage its BSA/AML and OFAC risk.

- A bank should be able to demonstrate when its BSA/AML or OFAC compliance program alone is appropriate to its risk exposure without supervisors presumptively overriding that approach.

- Guidance and clear examples are needed to help bankers determine when a change or adjustment to a BSA/AML or OFAC system that is considered a model is material and requires compensating controls or revalidation.

- Examples of how the *MRMG* principles apply to new and innovative solutions would clarify the steps that are expected when considering a new compliance system.

- More coordination is warranted between the Agencies' supervisors, including between the MRM and compliance teams. In group discussions on the issues at hand, bankers noted conflicting interpretations among supervisors from different Agencies, as well as from MRM *versus* BSA/AML and OFAC supervisors within the Agencies.

Most community banks cannot afford the staff expertise and time to develop BSA/AML or OFAC compliance systems internally, and are therefore, to a certain extent, captive to third-party programs. By necessity, such programs are generic, designed as one-size-fits-all solutions to compliance. While embedded software programs offer some capability for customization, banks cannot request major changes. Requesting even minor changes is difficult and involves much time and expense. As a result, it is infeasible for many banks to avoid reliance on the vendors' typologies for BSA/AML and OFAC compliance.[5] Accordingly, supervisors must understand smaller banks' reliance on third-party systems and have fitting expectations for risk management for vendor-provided systems.

<u>Guidance is to Help Distinguish between BSA/AML and OFAC Business Rules vs. Models</u>

ABA recommends that the Agencies provide in the *Interagency Statement* additional guidance and examples to help bankers and supervisors determine when a BSA/AML or OFAC system is or is not a model subject to the *MRMG* principles.

Determination of whether a BSA/AML or OFAC system is a model should be based on all relevant information. The compliance and/or MRM teams within a bank have the broadest perspective on this, so their judgement should be presumptive.

Some bankers report being required by supervisors to treat BSA/AML or OFAC systems as models. A supervisor should be prepared to defend by reference to the *MRMG* any conclusion that a BSA/AML system is a model. ABA believes that requiring examiners to articulate the rationale for a conclusion that a system constitutes a model will limit this occurrence and improve the overall efficiency of BSA/AML compliance by eliminating unnecessary MRM procedures.

Even though there is no definition of "model" specific to BSA/AML or OFAC purposes, the *MRMG* defines it as "…a quantitative method, system, or approach that applies statistical, economic, or financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates."[6] For example, that definition strongly suggests that transaction monitoring rules are not models since alerts are not "quantitative estimates" that assume probability or make projections and predictions. Similarly, systems that aggregate cash transactions do not apply mathematical theories to process data into quantitative estimates. Instead, they simply aggregate data, and therefore, should not be considered as models.

The *Interagency Statement* explains that the *MRMG* is principles-based and designed to provide flexibility, which ABA finds critical to the application of the *MRMG* to BSA/AML and OFAC compliance programs. According to the *MRMG*, there are three components of a model: (1) information input which delivers assumptions and data; (2) processing components; and (3) reporting components which translate estimates into useful business information. A system should not unavoidably be classified as a model without demonstration that each one of these components is present.

[5] Community banks also raised the point that, as BSA/AML compliance expectations move to a greater assessment of overall effectiveness, it will be difficult to coordinate those expectations with the lack of control over vendor-provided software. This is especially true since these banks frequently lack teams of risk managers or IT specialists to manage these efforts.

[6] *Ibid*

It is important to note, however, that while the *MRMG* definition leaves ample room for interpretation, bank' experiences and supervisory expectations suggest that most systems used for BSA/AML and OFAC compliance are considered models by default without regard to the *MRMG* principles, simply because they are significant components of BSA/AML or OFAC compliance. This focus, however, does not appear to be consistent with the *Interagency Statement*. Additional clarity is critical for banks and supervisors to be able to distinguish between models and rules. This is especially true because the default to characterize systems as models has become ingrained over the past decade, whether the initial characterization was appropriate or not.

In addition, ABA urges the Agencies to consider one other factor for determining whether a BSA/AML or OFAC compliance system is a model: the *Interagency Statement* is clear that a bank need not apply duplicative processes, which raises the question about whether there are existing processes, such as audit, to effectively evaluate the effectiveness of a system without classifying it as a model.

<u>Guidance on When an Alteration to a BSA/AML or OFAC Model System in Material</u>

Bankers note that when a BSA/AML or OFAC compliance system has been correctly characterized as a model, it is not always clear when a change or adjustment should require revalidation of the model. ABA recommends that guidance and examples should be added to the *Interagency Statement* to illuminate when the changes are sufficiently significant or material enough to require full validation.

While BSA/AML and OFAC models tend to be less complex than many other models, their operation is complicated by the variety of risks and constant change of inputs as risks and threats evolve.[7] In order to keep up with clever cybercriminals working to game the system, banks need to be able to adjust BSA/AML and OFAC screening systems frequently – as often as daily for OFAC systems. If these systems are considered to be models, then something as simple as changing the list against which accounts and transactions are screened becomes a change to the model that calls for evaluation of need for compensating controls or revalidation. That evaluation and possibly even revalidation takes time that can delay implementation of the change or even pull models offline pending revalidation, creating a serious impediment to efficient operations. Several bankers reported that, when they are uncertain about whether a system change should be rated as material, under pressure from supervisors they either purposely delay or forego it rather than have to wait for processing.

A change as minor as altering a threshold should require only a high level review while more major changes require deeper review. Basically, risk should be the determinative factor where the identification of what is material is based on risk. Since an institution is responsible for assessment of its own risk exposures, it should be the judge for when a system change is material.

[7] The constant change can be especially challenging for smaller institutions that rely on vendor-provided systems.

Responses to Specific Questions Asked by the Agencies

- *What types of systems do banks employ to support BSA/AML and OFAC compliance that they consider models (e.g., automated account/transaction monitoring, interdiction, customer risk rating/scoring)? What types of methodologies or technologies do these systems use (e.g., judgment-based, artificial intelligence or machine learning, or statistical methodologies or technologies)?*

Banks employ a variety of systems to comply with BSA/AML and OFAC requirements. ABA bankers identified four types of systems employed for these purposes: (1) transaction-monitoring, (2) sanctions and risk list screening, (3) scenarios, and (4) customer risk rating. Some are specialized systems and some are parts of core systems; the variability reflects the variety and breadth of the banking system.

Many, but not all, are appropriately classified as models. For each of the four types listed above, some banks classify their systems as models and some do not – and this is the case for representatives of both small and large banks. One banker reported that examiners determined that its customer risk-rating program is not a model, but OFAC screening (which is essentially an application of a variety of rules based on sanctioned entities and individuals) is a model. Other bankers reported that some transaction monitoring systems are considered models while others are not, and the rationale for the classification is unclear. It is important to understand that bankers almost universally confirm that there is little consistency among supervisors about the determinative factors that identify a model. This inconsistency underscores the need for additional clarity.

Moreover, as all stakeholders are working to improve the effectiveness and efficiency of BSA/AML and OFAC compliance, eliminating unnecessary steps becomes increasingly important. If a system has been inappropriately characterized as a model, the testing and analysis that is being applied may not be necessary.[8]

- *To what extent are banks' BSA/AML and OFAC models subject to separate internal oversight for MRM in addition to the normal BSA/AML or OFAC compliance requirements? What additional procedures do banks have for BSA and OFAC models beyond BSA/AML or OFAC compliance requirements?*

BSA/AML and OFAC compliance systems are tested for compliance and audited to evaluate their performance in the context of BSA/AML and OFAC regulatory requirements. If the system is classified as a model, it is further tested in accordance with the expectations of the *MRMG*. ABA recommends that the totality of these assessments and reviews be considered to determine if the *MRMG* assessment is duplicative, overly restrictive, and unnecessary for some BSA/ALM and OFAC compliance systems.

While reviews *may* be conducted collaboratively by compliance and model risk management teams, this collaboration does not always occur, and the results of compliance analyses are not always considered by the MRM teams. This is especially problematic for community banks. To

[8] For example, one banker reported that the bank's transaction monitoring system has approximately 60 rules which are collectively considered to be a model, and examiners expected each rule to be validated to ensure it is alerting appropriately—an extensive, time-consuming, and burdensome analysis that may not be warranted.

reduce burden, ABA urges the Agencies to emphasize the permissibility of coordination and collaboration by compliance review, MRM, and audit teams.

Overlap between the BSA/AML and OFAC regulations and the *MRMG* principles raise questions as to whether application of both is productive and necessary for a bank. Per standard operating procedures, BSA/AML and OFAC systems routinely undergo high-level annual reviews to evaluate performance, error rates, potential biases, changes, and new features – all subject to effective challenge; they also undergo separate compliance reviews and audits. This process is consistent with the principles of the *MRMG*. Bankers say that applying both the *MRMG* principles and BSA/AML and OFAC compliance rules simply adds levels of checkers checking checkers. None found examples where the additional layers of review detected issues or improved risk management. A bank should be able to demonstrate when BSA/AML or OFAC compliance alone is appropriate to the risk exposure without supervisors presumptively overriding that approach.

The value of this approach is especially important in consideration of the costs of model risk assessments. Model risk management is expensive due to a lack of competition among third-party assessors, the length of reviews, specialization of the analysts, and need for special liability insurance to cover risks incurred in consultant validations. Adding unnecessary and duplicative reviews is a serious drag on resources and detracts from funds that could otherwise be used to combat illicit finance.

Finally, as the focus of BSA/AML and OFAC compliance shifts to place greater emphasis on effectiveness and efficiency, unnecessary duplication of effort becomes a hindrance that detracts from those efforts.

- *To what extent do banks have policies and procedures, either specific to BSA/AML and OFAC models or applicable to models generally, governing the validation of BSA/AML and OFAC models, including, but not limited to, the validation frequency, minimum standards, and areas of coverage (i.e., which scenarios, thresholds, or components of the model to cover)?*

All banks have policies and procedures for BSA/AML and OFAC compliance. All larger institutions and most community banks also have MRM policies and procedures. Most that have both apply their general MRM principles to BSA/AML and OFAC models in the same way that those principles are applied in other areas of the bank. However, some bankers reported having sections of their MRM policies and procedures that are specific to BSA/AML and OFAC models. Bankers from some larger institutions reported that BSA/AML and OFAC systems that are not considered models are subject to separate policies and procedures that are equivalent to the *MRMG* principles.

One larger institution, which is typical of large banks, reported that all models used for BSA compliance are subject to general MRM policies. In this case, models are validated every one-to-three years based on the assessed materiality of risk and there is an annual review of the performance of each model. The validation process includes testing of purpose and use, theory and developmental evidence, implementation, performance, ongoing monitoring, and model governance and controls. In addition to the application of MRM policies, this bank applies additional emphasis on correct implementation, input data, and conceptual soundness when reviewing BSA/AML and OFAC models.

Several bankers reported that, when a bank's MRM team conducts a special assessment of BSA/AML models, the bank usually ensures that the evaluator has been certified in BSA/AML compliance.

- *To what extent are the risk management principles discussed in the MRMG appropriate for BSA/AML and OFAC models?*

The interplay between *MRMG* principles and BSA/AML and OFAC risk management principles is complicated. While the *Interagency Statement* is a step in the right direction, ABA recommends that the Agencies provide additional guidance and examples of the application of *MRMG* principles to promote clarity, understanding, and consistency.

BSA/AML and OFAC risk is driven by the products and services a bank offers and the geographic location of its customers. These risks, in turn, drive the frequency and level of compliance testing and audit. As a result, evaluation of BSA/AML systems focuses more on implementation, controls, and data input than theory. This approach is consistent with the principles in the *MRMG*, and is also dealt with in effective BSA/AML and OFAC analysis, as discussed above. For BSA/AML and OFAC systems, additional review is appropriate for error rates and to guard against potential biases. In these ways, a bank's BSA/AML and OFAC assessment can be more comprehensive than MRM validation and review.

- *Some bankers have reported that banks' application of MRM to BSA/AML and OFAC models has resulted in substantial delays in implementing, updating, and improving systems. Please describe any factors that might create such delays, including specific examples.*

ABA believes that application of the *MRMG* can become an impediment to updating systems and innovation by delaying the process while a model validation takes place.

Concerns have been raised about an expectation that every scenario be validated before implementation, since that slows down processes. One regional bank reported that applying the MRMG to BSA/AML and OFAC procedures has not caused delays, as the MRM team is able to validate new scenarios within an acceptable timeframe. However, other bankers reported considerable delays in putting scenarios into operation unless the BSA/AML team can obtain a policy exception or waiver the scenarios are fully validated. ABA recommends that the Agencies provide examples of situations where exceptions or waivers are appropriate.

- *Some bankers have reported that banks' application of MRMG to BSA/AML and OFAC models has been an impediment to developing and implementing more innovative and effective approaches to BSA/AML and OFAC compliance. Do banks consider MRMG relative to BSA/AML an impediment to innovation?*

ABA believes that elements of the *MRMG* can be impediments to innovation.

There is a growing interest in applying artificial intelligence and machine-learning systems to improve the efficiency and effectiveness of BSA/AML and OFAC compliance. However, imposing a full model validation and assessment into the process can delay and add significant costs. In addition, according to bankers, even after new programs have been subjected to internal assessment and validation before being put into operation, they face challenges explaining the changes and differences to supervisors. Bankers report that these steps become a real impediment to innovation when boards of directors assess the *MRMG* compliance costs as greater than potential improvements from a change.

Another problem that bankers have identified is that examiners are not always sensitive to costs associated with the implementation of new systems. Examiners may layer on costly expectations or requirements for analysis of any new compliance system. For example, examiners often require that new systems be run simultaneously with existing systems to analyze discrepancies and verify the operation of the new model. This parallel operation can run six-to-twelve months or longer. One solution is to allow, and even encourage, banks to use historical analysis for the comparison, relying on existing data to verify the reliability of an innovation, instead of requiring parallel operation for some period going forward.

ABA urges the Agencies to provide guidance and examples to clarify the steps that are expected under the MRMG principles before a new compliance system is implemented. This will become critical as banks are encouraged to apply innovative solutions to improve the efficiency and effectiveness of their BSA/AML and OFAC systems.

- *To what extent do banks' MRM frameworks include testing and validation processes that are more extensive than reviews conducted to meet the independent testing requirement of the BSA? Please explain.*

The *MRMG* requires more time-consuming analysis and testing than application of normal BSA/AML compliance assessments and audits. In addition to the standard technology development and implementation testing of BSA/AML and OFAC compliance, the *MRMG* calls for thorough validations with frequency based on the materiality of risk and annual review of system changes and risk ratings. Internal audit plays a role by reviewing the reporting to ensure that any changes have been properly documented. Much of this is unproductive for systems that should not be defined as models, for which additional clarification would be appreciated.

ABA members reported challenges to avoid excessive and unnecessarily duplicate analysis and review under *MRMG* and BSA/AML compliance. ABA recommends that the Agencies provide examples to help identify the extent of review required.

- *To what extent do banks use an outside party to perform validations of BSA/AML and OFAC compliance systems? Does the validation only include BSA/AML and OFAC models, as opposed to other types of models used by the banks? Why are outside parties used to perform validation?*

Many banks rely on third parties for model validations, including for BSA/AML and OFAC systems. This is particularly true of community banks that lack internal MRM staff, but some larger institutions do the same.[9] All banks, though, report that reliance on external evaluators is to ensure appropriate expertise and experience, although this can be costly and time-consuming. One notable exception, though, is that if a model is classified as low-risk, the analysis is likely to be performed in-house.

Some banks reported outsourcing BSA/AML model review in order to satisfy examiner expectations. This reinforces the need for greater clarity on the degree of scrutiny expected for

[9] Larger banks also report that, even where they currently rely on external experts for BSA/AML reviews, they are taking steps to bring the activity in-house.

BSA/AML and OFAC systems, so that bankers can better understand and defend when they can BSA/AML reviews in-house.

When a large bank conducts the analysis internally, steps are taken to ensure that the staff has the appropriate training and certifications, proper incentives, level of independence, and authority to perform the reviews, as well as authority to require and ensure remediation when needed. This gives BSA/AML and OFAC staff greater confidence that the systems are reliable such that external review is unnecessary.

- *To what extent do banks employ internally developed BSA/AML or OFAC compliance systems, third-party systems, or both? What challenges arise with such systems considering the principles discussed in the MRMG? Are there challenges that are unique to any one of these systems?*

Many banks, particularly community banks, rely on external sources for both BSA/AML and OFAC compliance systems, although others, typically larger banks, develop these compliance systems internally. In particular, larger institutions are likely to develop customer risk-rating systems internally. Much depends on the business model and existing systems that the bank has developed over time. However, bankers also find that vendor systems pose less risk because they have been subjected to appropriate due diligence, and vendors have specialized expertise in developing these systems, and supervisors have often reviewed the vendors' systems and are familiar with their operations.

While banks can "fine tune" vendor systems by setting thresholds and making minor adjustments to factory-set default settings, the ability to make changes is limited. Community banks report that requesting anything more than minimal changes or adjustments to vendor systems can be time-consuming and expensive, if it is even possible.

When using vendor systems, internal audit and frontline staff can verify output and identify necessary actions when false positives are identified. However, one particular challenge with assessing vendor systems is a lack of transparency when vendors are reluctant to disclose the structure of their models for proprietary reasons. This increases the need for output testing.

When a vendor-supplied compliance system is determined to involve a model, this affects the frequency and intensity of internal reviews, which becomes a cost factor to be considered when purchasing and implementing a system.

Even when a BSA/AML or OFAC compliance system is developed internally, banks report that it can be important to ensure that review is performed by a third-party to avoid a situation where the reviewers would be the same personnel as the developers.

- *Specific to suspicious activity monitoring systems, the agencies are gathering information about industry practices.*
    - *To what extent and how frequently do banks validate such systems before implementation?*
    - *What, if any, external or internal data or models do banks use to compare their suspicious activity systems' inputs and outputs for purposes of benchmarking?*
    - *How do banks attempt to compare outcomes from suspicious activity systems with actual outcomes, given that law enforcement outcomes are often unknown?*
    - *How do banks check the impact of changes to inputs, assumptions, or other factors in their systems to ensure they fall within an expected range?*

When suspicious activity monitoring systems are implemented, complete review is generally performed before implementation, with additional review performed after implementation. Quarterly reviews of performance are typical. Banks report that some transaction-monitoring systems are treated as rules-based programs, not models, while other banks report that these systems are treated as models due to their predictive nature. How the system is classified controls the type of review required. This highlights ABA's recommendation that the Agencies should offer examples to demonstrate the difference between a rule-based system and a model. At the same time, the Agencies should affirm that banks can have either a model or rules-based system, depending on the overall business model and risk profile of the institution.

When changes are implemented to a suspicious activity monitoring system characterized as a model, if the change is deemed material it will be validated before use. The ability to quickly implement transaction-monitoring changes will be increasingly important in order to incorporate the new and expected information from FinCEN on threats and priorities. This is another reason that additional clarity regarding what is considered material is important.

Benchmarking BSA/AML models is not deemed productive due to the unique attributes of individual institutions and the idiosyncratic risk model of each institution. In contrast, OFAC models can be benchmarked. Back-testing can be performed against transaction-monitoring and OFAC-screening models using below-the-line testing—*i.e.*, BSA/AML compliance staff determine whether potential hits exist below current thresholds and, in turn, MRM staff adjust existing thresholds using statically sound methodology.

Because BSA models are deterministic systems, there has not been an emphasis on sensitivity testing, with the exception of customer risk-rating models where the maximum and minimum of each risk factor (*e.g.*, transaction risk factor, geographic risk factor) can be assessed to determine its appropriateness. For transaction testing, large increases or decreases are investigated to determine whether changes to underlying data caused the change.

During annual reviews, models are assessed for changes, use and risk, ongoing monitoring, review of any steps for remediation (from prior findings), and a confirmation of controls. To some extent, which is part of the challenge, the response can depend on what defines a model.

<u>Conclusion</u>

ABA believes that the existing *MRMG* provides a solid foundation to analyze risk models. The *MRMG* has worked well for 10 years and does not need to be changed or revised to accommodate BSA/AML or OFAC systems. However, due to the unique nature of BSA/AML and OFAC compliance, additional guidance is needed to clarify how the *MRMG* works in the BSA/AML and OFAC space. The *Interagency Statement* is a step in the right direction, but it raises additional questions. The Interagency Statement should make clear that BSA/AML and OFAC systems should not be preemptively presumed to be models subject to MRMG risk management when a bank can demonstrate that this risk is managed effectively by BSA/AML and OFAC compliance. ABA urges the Agencies to offer examples to clarify the application of the *MRMG*, particularly to distinguish when a system classifies as a model and when an adjustment should be considered material. This distinction is especially important since it appears that, in many instances, model analysis is being applied to what are truly rules or immaterial changes but have been misidentified through a mistaken approach due to examiner encouragement, consultant recommendations, or MRM team interpretations. This approach is incompatible with current efforts to make a BSA/AML and OFAC regime more effective and efficient; requiring model validation where it is not necessary diverts resources from combatting money laundering, terrorist financing, and illicit finance.

Sincerely,

[redacted]

Robert G. Rowe, III
Vice President & Senior Counsel
Regulatory Compliance Policy

[redacted]

Robert Strand
Vice President & Senior Economist
Economic Policy and Research