


**From:** Christine Barton <CBarton@bayvanguard.com>  
**Sent:** Thursday, April 15, 2021 2:04 PM  
**To:** Comments  
**Subject:** [EXTERNAL MESSAGE] RIN 3064-ZA23  
**Attachments:** FDIC request for information 4-2021.docx

Christine P. Barton, CRCM/ACAMS  
SVP, Compliance  
[BayVanguard Bank](#)  
532 Eastern Blvd  
Baltimore, MD 21221  
Phone: (410) 686-5940 X1038  
Fax: (410) 574-3426  
Email: [cbarton@bayvanguard.com](mailto:cbarton@bayvanguard.com)



FDIC: You may submit comments on the request for information and comment using any of the following methods: • Agency Website: <https://www.fdic.gov/regulations/laws/federal/>. Follow the instructions for submitting comments on the agency's website. • Email: [Comments@fdic.gov](mailto:Comments@fdic.gov). Include RIN 3064-ZA23 in the subject line of the message.

1. 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)?

BayVanguard uses the following systems:

NuMonitor – automated AML transaction monitoring software integrated as part of the core – alerts are produced based on a set of preset parameters built into the software – amounts over a certain \$value - \$amounts outside preset profile limits – transactions over a specific \$amount when compared to last 90 day average amount.

WatchDog – automated OFAC monitoring software integrated as part of the core – system automatically searches lists based on individual or batch inquiry. A manual process is in place to ensure the list updates are entered in a timely manner.

2. 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?

NuMonitor/WatchDog are included in our annual BSA independent Audit and CSI (core provider) provides SOC1 documentation. Compliance Department staff looks for any inconsistencies when reviewing the daily alerts and annually the alerts are reviewed for effectiveness. Compliance Department staff review the OFAC list updates and compares to Watchdog updates to ensure timely entry when lists are updated.

3. 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)?

The portion completed by the Compliance Department staff is included in Banks Policies and Procedures. Portions completed by internal audit company are included in audit scope.

4. To what extent are the risk management principles discussed in the MRMG appropriate for BSA/AML and OFAC models? Please explain why certain principles may be more or less appropriate for bank operations of varying size and complexity? Are there other principles not discussed in the MRMG that would be appropriate for banks to consider?

The risk management principles provide clear definitions and suggestions for enhancing your program. I feel the principles would remain consistent across all risk levels, the policies and procedures would need to be more complex based on the risk level.

5. 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.

We have not experienced substantial delays.

6. Some bankers have reported that banks' application of MRM 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 MRM relative to BSA/AML an impediment to innovation? If yes, please describe the factors that create the impediments, including specific examples.

No

7. 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.

We do not use more extensive processes.

8. 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?

Because the AML software use is part of the core and not an integration – we do not have a third party model validation performed. We use the documentation provided by the core's validation and our last FDIC exam was fine with that. Our annual independent BSA audit does include review of alerts vs transactions for our systems.

9. 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?

We use third party systems for the majority of monitoring. Have not identified any specific challenges to date.

10. To what extent do banks' MRM frameworks apply to all models, including BSA/AML and OFAC models? Why or why not?

MRM frameworks would apply to most models and would assist in providing a consistent review practice.

11. Specific to suspicious activity monitoring systems, the agencies are gathering information about industry practices. The agencies welcome responses to the following, regarding individual bank and common industry practices.

a. Suspicious activity monitoring system validation:

i. To what extent do banks validate such systems before implementation?

NuMonitor has preset alerts with variable thresholds. The validation of these alerts were completed prior to them being available for use.

ii. Are banks able to implement changes without fully validating such systems? If so, please describe the circumstances.

The Bank can make changes to the thresholds within the alert and can add new custom alerts. Custom alerts can only be validated once alerts are producing.

iii. How frequently do banks validate after implementation?

The Bank can validate the next day after implementation provided alerts were produced.

iv. To what extent do banks validate after implementing changes to existing systems (e.g., new scenarios, threshold changes, or adding/changing customer peers or segments)? Please describe the circumstances in which you think this would be appropriate.

The Bank may add new alerts based on industry information (new alert for unemployment fraud based on the current environment) when a new product is rolled out more stringent alerts compared to a seasoned product. Merger modifies the current customer base. Alerts can be changes and reviewed the next day to ensure they are working as expected.

v. How do banks validate such systems?

Manual review of data output.

vi. What, if any, compensating controls do banks use if they have not had an opportunity to validate such systems?

Changes are made with anticipated results, if the change does not provide the expected results additional modifications can be made.

b. Suspicious activity monitoring system benchmarking: 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?

The Bank relies on recommendations provided from the provider based on other Bank's input, current industry trends, bank's risk appetite and prior monitoring system data.

c. Suspicious activity monitoring system back-testing: How do banks attempt to compare outcomes from suspicious activity systems with actual outcomes, given that law enforcement outcomes are often unknown?

When conducting investigations, a look back of alerts produced can provide information that shows if alerts were produced to aid in the identification of suspicious activity.

d. Suspicious activity monitoring system sensitivity analysis: 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?

The alerts have specific definitions. If the Bank identifies weaknesses or areas that need stronger thresholds, the Bank can enhance or request a new alert.

12. To what extent do banks calibrate the scope and frequency of MRM testing and validation for BSA/AML and OFAC models based on their materiality? How do they do so?

The Bank would calibrate the scope and frequency based on system changes. We would review the changes and assess the impact on current practices and based on risk make modifications.