ACAMS White Paper

AML Model Validation in Compliance with OCC 11-12: Supervisory Guidance on Model Risk Management

By:
Susan Devine, CPA, CAMS
Senior Consultant, Second Pillar Consulting, LLC

Table of Contents

1 Supervisory Guidance on Model Risk Management

Banks use a range of models to perform quantitative analysis, including estimating exposure, managing capital, and measuring risk. In response to increasing reliance on models, the Federal Reserve and Office of the Controller of the Currency (OCC) issued Bulletin OCC 11-12 that expanded the supervisory guidance in Bulletin OCC 2000-16, "Model Validation," issued May 30, 2000. Model validation remains a core component of OCC 11-12 and this paper demonstrates how OCC 11-12 applies to Anti-money Laundering (AML) models and describes validation strategies and techniques that comply with the guidance.

Models perform mathematical analysis on a set of input data and assumptions to estimate or predict results. OCC 11-12 defines a model as a, "quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques and assumptions to process input data into quantitative estimates."[i] Based on this definition, AML applications qualify as models because they:

Automated transaction monitoring and AML Models can be confused. Automated transaction monitoring focuses on identifying transactions that meet a set basic criteria such as transactions executed by specific individuals. AML Models use complex logic to assess whether the transactions represent unusual or suspicious activity. AML Models do not rely on just one or a few criteria, but rather interpret the transactions based on the originator, recipient, transaction type, amount, risk, and other parameters defined.

- Use quantitative methods, such as aggregating transactions
- Use statistical techniques, such as standard deviations, to identify unusual activities
- Apply AML theories, such as structuring, to identify suspicious activities
- Rely on specific assumptions, such as risk ratings or thresholds, to tailor the level of monitoring applied

OCC11-12 requires banks to assess model risk through a model validation process that poses an "effective challenge" to models. According to OCC 11-12, and effective challenge is a, "critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate change."[i] A model validation serves as an effective challenge to determine whether a model meets defined business objectives within a framework that effectively manages the risks associated with the models. The unique capabilities of AML models and OCC 11-12 require that an AML model validator have AML expertise.

1.1 OCC 11-12 and AML Models

The BSA specifically requires banks to file a Suspicious Activity Report (SAR) for any suspicious activity. The Financial Crimes Enforcement Network provides guidance on suspicious activity.[ii] Generally, suspicious activity is identified as unusual transactions that do not align with the customer's transaction profile and evasion of identity by the customer. The Bank Secrecy Act (BSA) Examination Manual states that, "Suspicious activity reporting forms the cornerstone of the BSA reporting system."[iii] The transaction monitoring performed by AML models is the primary tool banks use to detect suspicious activity. This critical role and recent significant enforcement actions speak to the importance of AML models.

AML models can perform a range of functions, such as calculating customer risk ratings, flagging transactions executed by known terrorists or money launderers, and generating alerts for suspicious activity that requires investigation through transaction monitoring against defined criteria. Transaction monitoring is not feasible without an AML model that can apply a set of complex algorithms to millions of records to produce a subset of transactions that meet the criteria for suspicious activity.

OCC 11-12 requires that banks maintain a model inventory that provides comprehensive information for models in use, under development, or recently retired. The information retained for each model should be commensurate with the model's complexity. Typically, banks prioritize models based on their associated risks. AML models pose significant model risk because they ensure compliance with laws and regulations, specifically the BSA.

Compliance with OCC 11-12 requires that:

- ✓ AML model validators have AML expertise that includes experience in the field of money laundering, detection of suspicious activity and financial investigations, with a background in regulatory compliance, financial auditing or analysis, or financial investigation
- ✓ The AML model is included on the bank's Model Inventory with appropriate information

1.2 Vendor Model Validation

Banks can develop AML models or purchase them from a vendor. OCC 11-12 requires evaluation of the same core elements for vendor models as for internally developed models. OCC 11-12 also requires validators to review the process used to select vendor models and states that vendors should provide information on the model's design, components and capabilities, assumptions, limitations, and ongoing performance monitoring and outcomes analysis.

In addition, the BSA Examination Manual states, "If the system was provided by an outside vendor, request (i) a list that includes the vendor, (ii) application names, and (iii) installation dates of any automated account monitoring system provided by an outside vendor. Request a list of the algorithms or rules used by the systems and copies of the independent validation of the software against these rules."[iv] Frequently, vendors are unwilling to provide model specifications because they consider them proprietary and confidential. However, validators can decipher the model's specifications and logic through testing each logical component as described in Section 5.

Vendors can usually provide some evidence of an independent validation of the product. While these reports can provide some evidence useful in a validation, validators cannot solely rely on these reports because implementation of the model can significantly impact the model's ability to meet its intended business purpose. Selection of installation options and parameters, the transactions subjected to monitoring, monitoring thresholds, and the transaction monitoring rules require that validators review the implemented model. Information in a vendor's validation report can inform the validation approach, but it cannot replace it.

Validation of vendor models:

- ✓ Is required by OCC 11-12
- ✓ Cannot rely solely on a validation provided by the vendor

1.3 Model Validation Core Elements

OCC 11-12 defines three core elements for model validations that are briefly discussed below and fully discussed in the remainder of this paper.

Conceptual Soundness focuses on the design, methodology, and construction of the model. OCC 11-12 states, "This step in validation should ensure that judgment exercised in model design and construction is well informed, carefully considered, and consistent with published research and with sound industry practice."[i]

Ongoing Monitoring verifies that the model is working as intended or meeting the business objectives established for the model. OCC 11-12 states, "This step in validation is done to confirm that the model is appropriately implemented and is being used and performing as intended."[i]

Outcomes Analysis examines the model's output and in the case of an AML model, the alerts generated from transaction monitoring along with the supporting information used for investigation. OCC 11-12 states, "This step involves comparing model outputs to corresponding actual outcomes."[i]

2 Role of AML Risk Assessment in AML Model Validation

Validators should begin with a careful review of the AML Risk Assessment and refer to it throughout the validation. AML models often provide mitigating factors for risks identified, including:

- **Preventative** – identify potential money laundering and protect the bank from legal or compliance issues through due diligence of AML monitoring and reporting, provide information related to investigations, inform decisions about products and customer behavior
- **Detective** – identify suspicious activities or behaviors that are prohibited by law or policy such as transfers to sanctioned countries or aggregation of transactions intended to avoid detection
- **Corrective** – identify internal control weaknesses or errors that allow prohibited transactions to occur, provide information for investigations

Throughout the validation process, the risk mitigations the AML model is intended to provide should be evaluated and confirmed.

2.1 Model Risk

All models have risk associated with them as they are imperfect representations of reality.[i] The purpose of OCC 11-12 is to provide a framework for assessing model risk with model validation playing a critical role. Risks associated with AML models include:

- **Compliance Risk**: Under reporting transactions and activities that should be reported or operating within an environment with critical internal control weaknesses
- **Legal Risk**: Not detecting illegal activities
- **Operational Risk**: Over reporting transactions and activities that consume resources to investigate alerts
- **Reputational Risk**: Not detecting activities subsequently publically disclosed
- **Earnings Risk**: Product selection and customer qualification can limit the products approved and customers accepted because of the money laundering risks associated with them

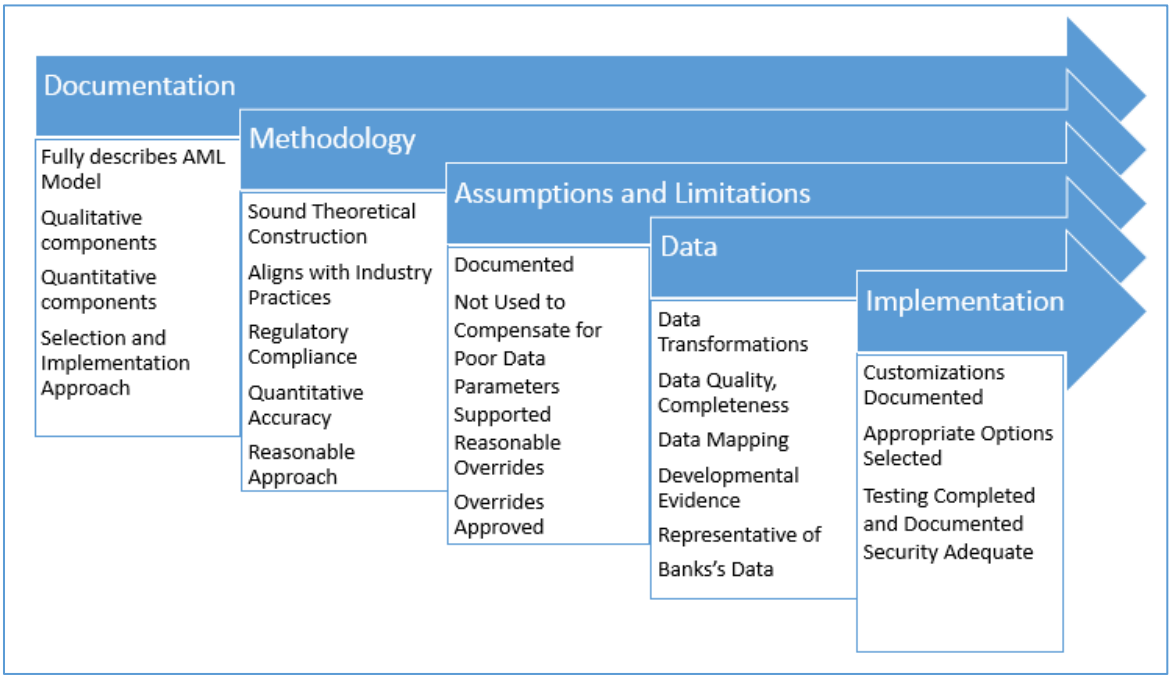
Model risk emanates from several sources, including:

- **Model Error**: The model does not perform correctly, including miscalculations or assumptions that are misleading or inappropriate.[v]
- **Data Error**: The inputs to the model are inaccurate or incomplete.[v]
- **Implementation Error**: The model is not coded so that it correctly specifies the methodology or logic.[v]
- **Usage Error**: The model's outputs are used in unintended ways.[v]

3 Validating the Conceptual Soundness of AML Models

Assessing an AML model's the conceptual soundness assesses the AML model's ability to meet the stated business objectives. The AML Risk Assessment should drive the business objectives, which should drive the requirements for an AML model. If the AML model does not have the capabilities required to address the risks, the business objectives cannot be met.

The documentation is the validator's primary source of information for conceptual design. Analysis focuses on whether the documentation fully describes the AML model components as well as the processes to select and implement the AML model as well as the data used to test the model. The graphic below provides an overview of the primary steps used to validate the conceptual soundness for an AML model.



Overview of Conceptual Soundness Validation Process (Source: Susan Devine)

3.1 Defined Business Objectives

Clear business objectives for the AML model should be defined. The business objectives can encompass a broad range of AML activities such as risk rating customers and transactions, complying with watch lists, monitoring transactions for unusual and potentially suspicious activity, and generating investigation data. An AML model can also be limited to specific transactions or business lines or used to perform limited AML functions such as calculating country risk. Validators need to understand the role the AML model plays in the overall AML program and identify any other models that interface with the AML model. For example, the AML model can rely on customer risk ratings generated by a separate model.

Assessing the AML model's ability to meet the defined business objective includes:

- ✓ Evaluating the process and rationale used to select a vendor model

- ✓ Verifying that the selection process that compared the vendor model's capabilities to the business objectives
- ✓ Determining whether the selection process documentation is adequate
- ✓ Verifying that the business objectives incorporate regulatory and legal requirements
- ✓ Comparing the model's capabilities to the AML Risk Assessment to determine if the model can adequately address the risks identified

3.2 Documentation

The documentation should include evidence of the AML model's capabilities and implementation. The BSA Examination Manual requires documentation throughout the AML process and OCC 11-12 states, "Without adequate documentation, model risk assessment and management will be ineffective. Documentation of model development and validation should be sufficiently detailed so that parties unfamiliar with a model can understand how the model operates, its limitations, and its key assumptions."[i]

The documentation should provide adequate information to allow a full understanding of the AML model, the process used to test and implement the AML model, the data inputs, parameters, and outputs.

At a minimum, the following documentation should be available and reviewed as part of an AML model validation:

- ✓ Developmental evidence that demonstrates how the AML model was tested, the data used in testing, and how the test results show that the model works as intended and meets the business objectives
- ✓ Model methodology that describes the theoretical approach, assumptions used, and known limitations
- ✓ Model specification that includes detailed descriptions of data, formulas, parameters, inputs and outputs, dependencies, processing flow, reports, and interdependencies with other models
- ✓ Data model that describes all data fields used in the model, including transaction codes and customer type identifiers
- ✓ Monitoring methodology that describes the logic provided by the model and selected for use to monitor transactions
- ✓ Risk-scoring methodology for customers, transactions, products, jurisdictions, industries, and other risk factors used
- ✓ Rules or peer grouping logic with accompanying thresholds and calibration data
- ✓ Reports generated
- ✓ Alerts and SARs statistics including metrics that measure the quality of the alerts
- ✓ User procedures that describe the model execution and maintenance processes
- ✓ Compliance procedures that describe how the model's outputs are used

3.3 Methodology

The model methodology describes the approach used to perform the various tasks, such as transaction monitoring. AML models typically use one of two main methodologies:

- Rules Based – Identifies suspicious activity by comparing transactions to rules or scenarios that define thresholds for velocity, value or volume[vi]
- Behavior-Based – Based on composite normal patterns for a customer or a peer group of customers, identifies suspicious activity for transactions that differ as measured by standard deviations[vii]

Validating the model methodology evaluates the:

- ✓ Alignment of the model with the business objective and compliance with regulations
- ✓ Model methodology to ensure verify it includes strategies and techniques to fulfill the mitigating factors ascribed to the model
- ✓ Reasonableness of the rules or behaviors and peer grouping techniques such as inclusion of all relevant customers and transactions and thresholds supported by analysis of the customer base and transactions
- ✓ Reasonableness of risk settings calculated or assigned for customer, product, or jurisdiction risks comradery
- ✓ Accuracy and soundness of mathematical calculations, including use of correct data fields for the calculations
- ✓ Reasonableness of the processing logic to accomplish the defined business objectives
- ✓ Robustness or capability to perform the required executions, including under stressed scenarios such as handling extreme data values
- ✓ Sensitivity and stability of the model's outputs to changes to the model's inputs

Validators can be tempted to short-cut obtaining a full understanding of the model's methodology. At this early stage, it's critical to ensure that the AML model implemented is capable of addressing the risks it's intended to mitigate. Validators should map each risk to specific AML model capabilities to demonstrate how the AML model can be effective in the risk environment.

3.4 Limitations and Assumptions

Models, by definition, are limited in that they cannot provide 100% certainty of the real-world occurrences they aim to represent. Assumptions bridge the gap between what is known and what is unknown. Limitations can emanate from weaknesses in the model due to shortcomings, approximations, and uncertainties or result from assumptions that restrict the model's usefulness to specific circumstances and situations.[viii]

OCC 11-12 recognizes that vendors can be reluctant to provide known limitations and states that a guiding principle for managing model risk is, "critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes."[i] Comparing the limitations to the AML Risk Assessment is critical to ensure that they do not introduce new risks or

compromise mitigating controls provided by the model. "If the model is weak in an area where the bank has a meaningful exposure, then that model is likely not the appropriate choice."[viii] For example, if the model does not provide a feature to identify related customers with different account by comparing addresses or other identifiers, monitoring will be limited. If this is a known risk, then the model would not be able to mitigate this risk.

Overrides for alert reporting are frequently made for established customers and specific transactions. Do Not Compare lists that exclude transactions between a pair of customers or accounts is a form of override and should be reviewed for reasonableness. Management overrides can impact regulatory compliance by eliminating certain transactions from monitoring or suppressing alerts.

Validators should examine the rationale for any overrides applied to parameters, data transformations, or approximations because they can reveal undisclosed limitations.[i,ix]

A validation should include evaluation of the reasonableness of the model's assumptions. Assumptions can be made to compensate for data imported from other models or systems. Assumptions are frequently expressed as variables, which are periodically updated. For example, assumptions can include reliance on customer risk ratings calculated outside the AML model that need to be updated as the bank's risk profile changes. Other variables that implement assumptions include the thresholds set for monitoring and key words used to search for high risk customers.

All variables should be documented, defined, and established based on empirical evidence. Updating variables should fall under a governance framework that ensures they are documented and periodically reviewed for reasonableness and their impact on the model's outputs. Whenever an acquisition occurs, the bank's AML Risk Assessment and assumptions can change. Validators should verify that assumptions and related variables are reviewed and updated as needed in a timely manner whenever the bank's risk profile changes.

Validators should confirm that the bank performs sensitivity analysis and stress testing to determine the how changes to assumptions impact model results. Sensitivity analysis measures the impact of small changes and stress testing measures the impact of large changes. The purpose of sensitivity analysis is to verify that the model's results react as expected to changes in assumptions. For example, if a monitoring threshold for a specific transaction type is lowered, the model is expected to produce more alerts. If the sensitivity analysis shows that the same or fewer alerts are produced, analysis of the underlying data and model logic is needed to determine why. The purpose of stress testing is to verify that the model continues to perform as expected when large changes place the model under stress. For example, if the assumptions used monitor cash transactions increase the time frame from 2 days to 5 days, the model is expected to produce more alerts. If it does not, the model may not be able to correctly process the volume of transactions that support alerts.

OCC 11-12 requires that an effective governance framework provide for clear communication of limitations and assumptions.[i] The governance framework should also ensure that the limitations that impact how the model can be used are documented and that controls are in place to ensure the model is not used when inappropriate.

Validation of model limitations and assumptions includes:

- ✓ Ensuring that known assumptions and limitation are documented
- ✓ Analyzing the limitations to determine if they introduce new risks or compromise mitigating controls
- ✓ Analyzing management overrides and data transformations or approximations to determine if they relate to undisclosed assumptions or limitations
- ✓ Reviewing the approval process for management overrides to ensure appropriate oversight is applied
- ✓ Reviewing the governance framework to ensure that limitations on model usage are enforced

3.5 Data

AML models typically process voluminous and complex data. Customer and transaction data is usually imported from multiple systems and can be transformed to meet processing requirements. AML models also import data from other models or open-source databases such as watch lists.

Data pose difficult challenges for validators for several reasons. AML staff do not always know all the transaction codes in use, how transactions codes are used changes, acquisitions introduce new data and data formats, and most importantly the Know Your Customer (KYC) Program does not enforce standardized customer data.

Data transformation, such as converting data field formats to comply with vendor database requirements, can significantly impact the transaction monitoring. AML models often pull data from multiple systems within a bank's technology infrastructure. When the bank's systems define or format the same data differently, the data must be standardized for use in the AML model. For example, address data can be transformed to standardize abbreviations for street, drive, court, etc. If data proxies are used, they should be fully documented with appropriate rationale for their use.[i] For example, country codes can be used instead of a country name or Customer IDs that combine a customer name with other identifying information such as a birth date can be a proxy for customer.

Data mapping that defines the origination and meaning for specific data values requires in-depth knowledge of a bank's systems and data. It's essential to verify that the data used to identify peer groups is accurate and representative of the transaction profiles of customers and customer segmentation. Data quality, completeness, and accuracy is often assumed. A validation must challenge this assumption and confirm that the data inputs are in fact complete and accurate. For example, reconciling the input data sources and transactions submitted to monitoring can verify that all data is monitored. Prior to beginning transaction testing, the validation should confirm that data is complete and properly formatted. Validators can run queries to identify data missing, such as account numbers and transaction codes for each transaction, originator and beneficiary information on wire transfers, and transaction codes for new products.

The data used to develop, implement, and test the model should resemble the bank's customer and product base and include assumptions used to adjust the data.[i] Derived and external data,

such as country risk ratings, used should also be included in the developmental evidence and testing for implementation.

The data requirements are also driven by regulatory requirements that specify data that must be captured and maintained for use in investigating alerts generated by the AML model. The BSA Examination Manual lists specific data elements required by the BSA. Appendix 1 lists the data items by section. Validators should confirm that the AML model captures these data elements to ensure BSA compliance.

Validation of the data input and processed by an AML model is a critical component and requires detailed documentation of the data sources and individual data elements. Validation of the model's data includes:

- ✓ Reviewing data transformations, proxies, and assumptions for reasonableness
- ✓ Verifying that all data sources, internal and external, are identified and documented
- ✓ Assessing the process used to ensure all input data is subjected to monitoring
- ✓ Assessing the data sources to ensure they provide accurate and complete data in compliance with regulatory requirements
- ✓ Comparing the developmental data to the bank's portfolio to ensure it is representative
- ✓ Verifying that data definitions are completely and correctly mapped to the data in the model
- ✓ Peer groups are defined based on accurate and complete transaction profiles or other empirical data

3.6 Implementation

AML models purchased from vendors usually require customization and always require selection of various implementation options. Implementation is a process that relies on thorough user and operational testing to ensure that the AML model will work in the production environment as intended.

The vendor documentation should provide a comprehensive list of implementation options and each selection should be documented along with the rationale for selection. The vendor documentation should also provide information on the impact the options have on model performance. For example, an AML model may provide a feature to relate customers by address and monitor them as one customer. This feature may be replaced by a relationship data code in the bank's data. In this case, the vendor model option would not be implemented and the monitoring code would have to be customized to use the bank's relationship code. Any customizations should be documented and the developmental evidence should be available.

The quality of the user acceptance and operational testing should be examined to ensure it meets industry best standards and includes:

- A testing plan that describes planned test cases
- All model components
- Comparison of expected and actual results
- Use of data that is representative of the production data

- Training for users performing acceptance testing was provided

The technology environment in which the model is implemented provides the foundation for maintaining the model for continued business use. Three core technology elements should be examined as part of a validation: Data Security, User Security, and Change Management. Data security includes the controls used to protect the data used in the model from unauthorized disclosure, modification, or destruction. The data used in the model is highly sensitive because it contains personal financial information. Unauthorized disclosure risks potentially devastating consequences for the customers and the bank. Data security controls should be implemented by appropriate security administration software that is managed by the IT department. Access to the data used in the model is optimally limited to systems such as the AML model and does not permit access to individual users. Each data feed for the model should be reviewed for appropriate data security. User security includes the controls used to limit the access and level of access for users who have access to the AML model. All authorized users should be documented with a description of the access required to perform their related jobs.

The security methodology for the model should be reviewed to ensure that it provides a feature that can limit access to various model components and provide different access levels. For example, a compliance investigator could have read only access to the transaction data that supports alerts but not have access to update the rules used to generate the alerts. Change management refers to the processes and procedures in place to ensure that any updates made to the model, such as upgrading to a new version, are managed, tested, and implemented to ensure that they do not disrupt continued business use. Consultation with the bank's IT Department is essential to ensure that the AML model and data are appropriately secured.

Review of Internal Audit reports or other model validation reports can also provide information about the overall technology environment, especially known issues.

Validation of implementation of an AML model includes:

- ✓ Evaluation of installation options and customizations
- ✓ Review of the quality of the user acceptance and operational testing
- ✓ Evaluation of the data security
- ✓ Evaluation of the user security
- ✓ Verification that appropriate change controls are in place to ensure that changes made to the model are implemented after thorough testing and approval

3.7 Conclusion

At the conclusion of the review of conceptual soundness of the model, the validator forms an opinion about the bank's risk profile and the model's ability to help mitigate those risks. The validator will understand why a specific AML model was selected or designed and what the specific capabilities of the model are. The adequacy of the model documentation will indicate the strength of the model risk governance framework as the documentation lays the foundation for the implementation and use of the model. The assumptions and limitations will determine whether the model has significant issues in the methodology that can impact the reliance on the results. During review of the data the validator will begin to form an opinion about its integrity that will inform the

transaction testing. For example, extensive data transformations can indicate potential issues with data accuracy or completeness that should be investigated. The results of the testing performed at implementation, or release of the latest version, will also provide insight to the presence or absence of issues that can impact the model's results. In summary, the review of conceptual soundness allows a validator to determine whether:

- ✓ The model selected or designed was based on the known risks using a set of documented assessment criteria.
- ✓ The documentation is sufficient to understand the model, its processing, and its outputs.
- ✓ The model selected or designed has the features and functions capable of meeting the business objectives defined.
- ✓ The limitations and assumptions do not significantly weaken the model's capabilities.
- ✓ The data is adequately defined and its integrity is maintained.
- ✓ The model was implemented using a controlled process that ensured adequate testing.

4 Validating Ongoing Performance of AML Models

Ongoing performance monitoring verifies that the AML model continues to meet the defined business objectives. It provides the opportunity to identify issues and evaluate changes since the last validation more quickly than waiting for the next validation. For example, if a new product and related new transaction code are implement in the quarter following a validation, ongoing monitoring will provide the opportunity to compare the model outputs related to the new product throughout the nine months until the next scheduled validation.

OCC 11-12 states that ongoing monitoring begins when a model is implemented in production for business use.[i] As shown in the diagram below, monitoring should provide continuous feedback about the AML model that can be used to update the model as needed.

Overview of Performance Monitoring Framework

Source: Susan Devine

A framework for ongoing monitoring establishes the requirements and identifies the parties responsible. Assigning responsibility, especially with reporting requirements to senior management, helps ensure that the monitoring is conducted and that the results are communicated so that proactive or corrective actions can be taken.

The validation should confirm:

- ✓ A process is established to routinely and periodically review model performance
- ✓ The monitoring framework includes procedures to identify changes made to the model
- ✓ Responsibility for ongoing process is assigned

4.1 Performance Monitoring and Data Analytics

The ongoing monitoring framework identifies performance standards that are compared to the model performance to determine stability and reliability. Establishing performance standards ensures that a benchmark based on analysis of empirical data is used as a comparison for actual model performance. Without a performance standard, ongoing monitoring cannot be fully assessed.

Determining appropriate performance standards is challenging because AML models process all or most of the bank's transactions, use many data items, and are embedded in a management framework that includes processes external to the model. The following breakdown of performance standards provide a sound framework for identifying and organizing performance standards:

- **AML Program Management** indicates whether the overall AML program is meeting the business objectives. Indicators include findings in independent reviews, regulatory actions, effective and timely processing of alerts, SARs, and investigations resulting in no or minimal backlog of work.[ix]
- **Monitoring Effectiveness** indicates whether the AML model is producing productive alerts, as indicated by the percentage of alerts converted to SARs.
- **Model Accuracy** indicates whether the AML model is producing accurate alerts. Errors identified are fully documented and promptly corrected.[ix]
- **Data Accuracy** indicates that the data submitted for transaction monitoring is complete, accurate, and has not changed since the AML model was implemented. Indicators are consistency between the data submitted for monitoring and the customer base and monitoring results.[ix]
- **Model Effectiveness** indicates that the alerts generated are within expected thresholds. Indicators include false positives exceeding expected thresholds, rules that produce no alerts, and the correlation between transaction volume alerts generated is not maintained.[ix]
- **Emerging Risks** indicates that the AML model identifies potential changes in the assessed risks. Indicators include alerts generated that are intended to expose emerging risks, unexplained changes in the number of alerts or SARs generated, changes in the AML Risk Assessment, changes in the customer or transaction profiles.[ix]

Ongoing performance monitoring depends on a set of metrics or Key Performance Indicators (KPIs) routinely captured and reported. Some AML models provide a dashboard to report KPIs constantly along with a reporting feature. The most important factor is the selection of the KPIs and the process in place to review and react to the information. Selecting the appropriate KPIs begins by determining what is available in the AML model and what information is needed to monitor performance. Some standard KPIs include:

- Number of customers by risk class and product segment
- Transaction volume by various timeframes
- Transaction volume by product, risk class, and product segment
- Alerts generated and false positive alerts generated by rule, transaction type

- Alert conversion rate to SARs
- Open investigations and closed investigations
- Number of rules with NO alerts

For example, the number of false positive alerts can signal thresholds that are too restrictive or too loose. The KPIs should be monitored from period to period using a consistent methodology to be able to observe trends. The trends in KPIs help establish when changes in thresholds may be indicated.

The KPIs should be reviewed holistically with appropriate comparison to determine the impact on the AML program. KPIs about the input data can reveal changes in customers, products, or risks that impact the entire AML program. For example, changes in the distribution or customer types or risk class can be used to generate new rules for monitoring. Changes in volume are helpful for planning resources.

As a final step, the ongoing monitoring results should be used to analyze the AML Risk Assessment. The results will generally confirm the risks identified, but can also show how shifts in customers and transaction types may impact the risks identified. Since the AML Risk Assessment drives the business objectives for the AML model, the ongoing monitoring results should always be compared to the risks identified.

The validation should confirm:

- ✓ Appropriate performance metrics or KPIs are captured and reported for the AML model on a regular basis
- ✓ Reports produced for KPIs and alerts provide supporting detailed transactions to allow full evaluation
- ✓ KPIs are reviewed and analyzed by appropriate management to identify trends and emerging risks
- ✓ Overrides are tracked and examined to determine if they indicate issues with the model meeting the business objectives
- ✓ Data errors are investigated for root cause and appropriately addressed
- ✓ The AML Risk Assessment is updated as needed based on ongoing monitoring results

4.2 Tuning and Calibration

Tuning or calibration is one of the more complex aspects of managing an AML model due to the number of thresholds and parameters used in transaction monitoring. Increasing the complexity is how the various thresholds and parameters work together. Few, if any, rules are designed using one parameter. Most rules involve a customer type, transaction type, time frame, and a dollar value or transaction volume. For example, international wire transfers can use thresholds for transaction amount, transaction counts, timeframes, aggregated transaction amounts, aggregated transaction counts, each set to different levels for customer type, jurisdiction, and risk class. Tuning the rules for these transactions requires understanding how each parameter affects the results. This process of isolating each parameter for tuning is tedious, but provides the best results. Sensitivity testing results, discussed in Section 3.5, can also provide useful information for the tuning effort.

Thresholds are used to eliminate or filter some transactions from generating alerts. The purpose of thresholds is to suppress alerts that should be generated based on the monitoring rules, but clearly do not indicate suspicious activity, which are referred to as false positives. Thresholds should be based on data analytics and KPIs to ensure they are appropriate and do not suppress suspicious activity that should be converted to SARs. Setting thresholds is a balance between over reporting alerts that can misuse resources required to investigate them and under reporting alerts that can present business, legal, or compliance risks. The tuning framework serves as the strategy to ensure that a reasonable level of suspicious activity is reported. Defining a reasonable level can be developed by examining the conversion ratio of the number of alerts converted to SARs. If the conversion ratio does not change as a threshold increases, it is reasonable to conclude that suspicious activity is reasonably detected.

Data analytics are the foundation for tuning an AML model. Statistical analysis can refine the information and allow users to make conclusions about the entire population based on a specified confidence level. However, simpler analyses, can also be informative. Distribution analysis groups items, such as transactions, across a defined scale. A distribution of transactions and customers can provide insight into the transaction and customer bases and the associated risk classes. Alerts are typically reported by rule or scenario, but the ability to analyze alerts by customer type, transaction type, location and risk class can help AML managers set thresholds and identify normal activity.

Validation of the tuning and calibration includes:

- ✓ Monitoring thresholds are documented and approved
- ✓ Monitoring thresholds are defined based on analysis of appropriate data
- ✓ Trends in KPIs and other data analytics are captured and reviewed as part of the tuning process

4.3 Conclusion

Throughout the review of ongoing performance, the validator will form an opinion of how well the model is managed and the stability of its performance. The validator will be able to assess the controls in place to periodically review the operational effectiveness of the model. Not completing scheduled performance monitoring may indicate that the AML department is not assessing the model for changes in the bank's risk profile, customer base, or transaction base. In addition, lack of capturing and reporting KPIs may indicate that senior management is not providing sufficient oversight or support for the monitoring activities. Tuning the model is challenging and time consuming. It can be deferred as a lower priority, which can significantly degrade model performance. In summary, the review of ongoing performance allows a validator to determine whether:

- ✓ The model is managed on a scheduled, preventative basis or if performance is assumed to be adequate until an issue arises and forces a performance review.
- ✓ The bank and the AML department emphasize controls that relate to model management.
- ✓ Key metrics are captured and reported on a timely basis to appropriate levels of management, which indicates adequate oversight.
- ✓ Processes and procedures are in place to prevent issues with model performance from developing.

5 Validating Outcomes Analysis

Outcomes analysis examines the AML model's results to verify that they are accurate and complete. Accuracy relates to ensuring that the alerts reported are supported by the transaction data. Accuracy is a test for overstatement or "above-the-line" testing because it tests the accuracy of a reported number of alerts. Testing for completeness determines whether all alerts that should have been generated were generated. Testing for completeness is a test for understatement or "below-the-line" testing because it tests for unreported alerts. To validate an AML model's outcomes, both above-the-line and below-the-line testing are required and are considered best practice. Other approaches, such as random sampling alerts and tracing them to supporting data or randomly selecting transactions and evaluating them for potential alerts, are alternatives that cannot provide the same assurance as the corollary above-the-line and below-the-line approach. This section outlines a transactions testing approach for validation of each core element of OC 11-12 based on the AML model's outcomes.

"Above-the-line" testing starts with the alerts reported and traces them to the supporting transactions. "Below-the-line testing starts with the transaction data and traces it to the alerts reported.

The BSA Examination Manual includes a section on Systems to Identify, Research, and Report Suspicious Activity and states that, "Suspicious activity reporting forms the cornerstone of the BSA reporting system."[iv] The BSA Examination Manual notes that it is unrealistic to expect a bank to detect and report all potentially illicit transaction and that examiners should focus on the bank's policies, procedures, and processes to identify SARs.[iv] However, validators cannot solely rely on policies, procedures, and process reviews to provide assurance that the AML model is working as intended.

Multiple approaches can be used for testing transaction monitoring. Statistical sampling transactions for verification is a standard approach used in financial transaction testing. However, statistical sampling is most effective when testing a reported transaction balance. Statistical sampling selects individual transactions based on a selected confidence level. This approach is inappropriate for AML models because alerts can be generated from a combination of transactions as in structuring. Using statistical sampling would not identify the various transaction combinations. An AML model doesn't report transaction balances, but uses transaction patterns to discern suspicious activities. Random sampling of alerts can be used for above-the-line testing. However, the alerts selected may not include all of the monitoring logic performed leaving some of the monitoring untested. In addition, below-the-line testing with random alerts is infeasible as a set of transactions would have to be compared to every rule to assure no alerts were unreported.

Using an approach that focuses on the logic used in transaction monitoring, allows validators to test the logic for a sample of rules or behaviors that is duplicated in the other rules or behaviors that use the same logic. By identifying all the logical components of the monitoring and testing the accuracy and completeness of each logical component provides a comprehensive test of the monitoring. Testing each logical component does not require testing every rule or behavior pattern. AML models reuse the same logic. For example, aggregating cash transactions within a specified timeframe works the same for aggregating check transactions. Thus, testing aggregation as a logical component can be applied to all transaction types. Using a testing methodology that confirms the accurate processing of logical components can be effective and efficient. When

several hundred rules incorporate the same logical component, the validator can test a limited number of the rules to confirm that the logic is working and have assurance that the logic works in the other rules not tested. Testing based on logical components requires that each component is identified and tested. This requires a detailed analysis of each rule so that all logical components are identified. Again, vendors are frequently reluctant to disclose the exact logical operations used and a validator will often have to deduce the logic and order of operations by iterative testing. The following sections

5.1 Transaction Testing Planning and Resource Requirements

Regardless of the transaction testing approach used, significant planning needs to identify data requirements, security for data, analytical tools, and analysts required. The planning also includes determining the testing period and preparing the data extraction request for use in transaction testing.

The validator, who has AML expertise, needs to provide direct, hands-on, supervision and review of the data analyst's work who does not have AML expertise.

The technology requirements for the transaction testing are based on estimated transactions for the validation period. Even with a medium sized bank, a typical validation requires review of tens of millions of transactions, even for a quarter. It is not necessary to subject a full year's transactions if a quarter or month covers all the logical components. A data analyst with expertise in database queries is usually required to code the queries on the data. However, the validator is responsible for directing and reviewing the data analyst's work. The validator, who has AML expertise, must perform most of the planning and analysis and rely on the data analyst to extract the data. The validator must examine the data extracts and compare them to the full data set to ensure that the extraction was performed correctly. One approach for accomplishing this is to obtain the full set of transactions for a customer that triggered an alert and manually confirm that the data supports the alert and was correctly extracted.

To plan for the transaction monitoring:

1. Determine the most recent changes to the rule / behavior set. The testing period should be limited to a stable set of rules / behaviors to ensure that the logical components and thresholds work identically.
2. Determine the testing period, which should cover at least two months to ensure that month-end cut-offs are handled correctly. The testing period should be considered based on the timeframes defined in the rule set to ensure that the testing period covers at least the longest timeframe.
3. Based on review of the input data, identify key data fields used by the AML Model for monitoring. The BSA Examination Manual, Appendix O: Examiner Tools for Transaction Testing provides a base set of data fields required for transaction testing that is consolidated below:[x]
    - The customer information file (CIF) number, Social Security number(SSN), taxpayer identification number (TIN)
    - The teller and branch or other applicable identifying information

- The customer's full name, country of residence, and BSA/AML risk rating, if applicable
- The date, amount, transaction type, and account number of each transaction
- For funds transfers originator's name, beneficiary's name, country, financial institutions, and account numbers
- Date the account was opened
- Type of account

4. Obtain a sample of data for a subset of customers to confirm that the data fields identified are the data fields used by the AML Model. Confirm that the data extraction includes all data needed to verify the accuracy and completeness of the monitoring logic.
5. Estimate for storage of the data extracted for secure transfer.
6. Obtain the data for all customers for the testing period.
7. Verify the completeness of the data in the full data set. Query for missing data and NULL entries on the key data fields identified to ensure that the monitoring can be effective.
8. Verify the consistency of the data in the full data set. Query for basic formatting characteristics such as non-numeric data in transaction amount fields and unknown transaction codes or customer types.

5.2 Analyze Monitoring Rules and Parameters

Transaction testing can be a most effective tool for assessing conceptual soundness. The components of an AML model are complex with too many parameters to review in isolation. One rule usually has multiple parts that perform in a strict order to siphon the transactions considered suspicious. Thus, it is not just the individual components of a rule, but also the order in which the components are executed that drives transactions identified as suspicious. Added to this are filters and thresholds that eliminate some customers or transactions and aggregate transaction amounts.

The complexity prohibits a full model replication and validators must develop alternative testing approaches. Examining the accuracy of the logic used to monitor transactions can provide a comprehensive review. The following table lists and describes examples of logical components used in monitoring.

Logic	Potential Parameters	Used to Test
Customer Type	Individual, Business, Foreign National, Employee, Peer Group Id	Customer segmentation Peer group High risk customers Employee transactions Money flow
Business Type	High Risk, NAICS Code, Money Service Business	Customer segmentation Peer group High risk customers Money flow
Jurisdiction	Country, state/province, zip code, street	Watch lists High risk jurisdictions High risk transactions

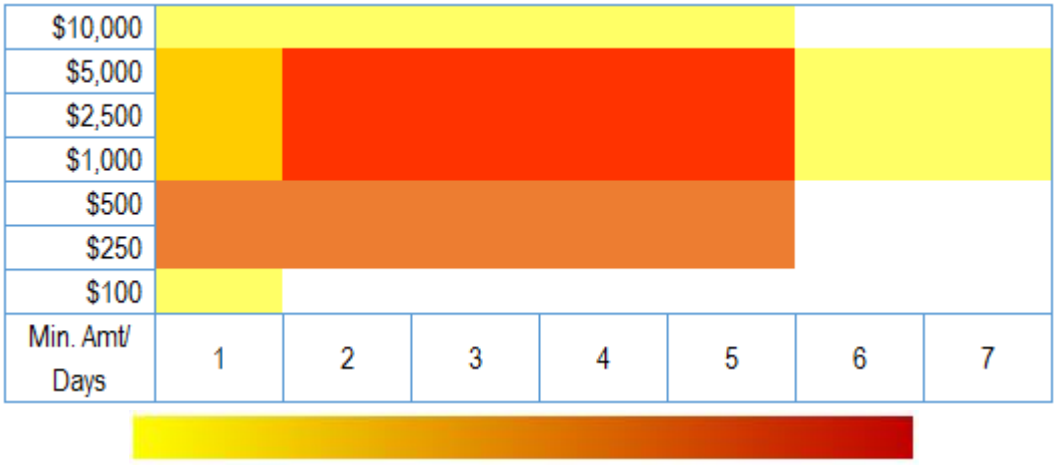
Logic	Potential Parameters	Used to Test
Transaction Type	Cash, Check, ATM, ACH, Wire Transfer, Transfer, Credit Card, Monetary Instrument, Loan Transaction Type vs. Transaction Type	Money flow Structuring High risk transactions
Transaction Volume	Count of transactions	Money flow Structuring
Transaction Value	Dollar amount of transaction or transactions Minimum transaction amount Maximum transaction amount	Money flow Structuring SARs, CTRs
Transaction Velocity (Timeframe)	X Days Between Within X Days	Money flow Structuring SARs, CTRs
Money Flow	Inflow, Outflow, Inflow vs. Outflow	Money flow Structuring SARs, CTRs
Transaction Aggregation	Multiple Transaction Types Total Transactions Value Multiple Customers	Money flow Structuring SARs, CTRs
Originator / Beneficiary	Originator or Originators vs. Beneficiary or Beneficiaries	Funds transfers SARs, CTRs Sanctions, watch lists
Jurisdiction / Location	Country, State, Country, Branch, Teller, ATM	Funds transfers Sanctions, watch lists
Prior Period Activity	Average account balance, average inflow, average outflow, average transaction count, average transaction volume by transaction type	Customer behavior

Using the logical components and parameters in the table above, hundreds or thousands of monitoring rules are used for monitoring, which makes it difficult to identify gaps in monitoring or duplicated rules. Breaking down the logical components allows the validator to review the coverage and concentration the monitoring provides. The coverage and concentration can be graphed using a chart or heat map. For example, the graphic below depicts the coverage for the following three rules:

A graphical depiction of the transactions covered by monitoring can identify both gaps in monitoring and duplications of monitoring.

- Within 1 day an Individual deposits Cash in 1 transaction totally minimum $5,000.
- Within 5 days an Individual deposits Cash in 2 or more transactions with a minimum deposit amount of $250 totally minimum $10,000
- Between 2 and 7 days an Individual deposits Cash in 5 or more transactions with a minimum deposit of $1,000 totally minimum$5,000.

The graphic below depicts the monitoring concentration. The transaction that are monitored by more rules are reflected with darker shades.



Monitoring Rules Coverage and Concentration for Cash Transaction

Using graphical representations are most useful when a validator is concerned that the monitoring rules do not provide adequate coverage. The graphic above shows that transactions of less than $100 are not monitored within 2-7 days and transactions between $1,000 and $5,000 are subjected to the most monitoring rules within 2-5 days. It also shows that transactions above $5,000 are not monitored within 6-7 days, indicating a gap in monitoring. Transactions less than $250 are monitored only within 1 day and transactions between $1,000 and $5,000 are monitored more than other dollar ranges, but only within 5 days. More complex rules can be created with 3-D graphics available.

5.3 Select Rules for Testing

Breaking down each rule into the logical components used then allows a validator to identify the rules that rely on each piece of logic. Selecting rules to test specific pieces of logic ensures that all the logic used in monitoring is tested. Rules selected should include both rules that generated alerts for above-the-line and below-the-line testing and rules that didn't generated alerts to confirm that they are implemented.

To perform transaction testing related to conceptual design:

1. Obtain the entire set of rules or scenarios.
2. Analyze each rule independently to ensure it is properly defined. For example, verify that the thresholds are correct and that filters are not set above the thresholds. Verify that the rules are correctly entered in the AML model.
3. Identify the logical components / peer group parameters and thresholds. Identify the timeframe used to calculate average activity for peer groups or individual customers.
4. Select a subset of rules for above-the-line and below-the-line testing to include:
    - All logical components and parameters and thresholds
    - All rules generated alerts during the testing period
    - All customer types

- Customers from all risk classes if appropriate and businesses identified as high risk
- All transaction types
- Timeframes that cross months or quarters as appropriate based on timeframes defined in the rules

5. Select a subset of rules solely for below-the-line testing to include:
   - Rules that did not generate any alerts during the testing period
   - Rules that did not generate any alerts for each conceptual component
6. Select a subset of any new rules implemented since the prior validation.
7. Assess adequacy of logical capabilities for features to monitor watch lists.
8. Verify watch lists are updated by comparing them to current lists.

5.4 Above-the-Line Testing

The purpose of the above-the-line testing is to confirm that alerts generated are supported by the transactions based on the logic used. Above-the-line testing begins with alerts reported and reconciles them to the transactions. It is not adequate to examine the AML model's detailed list of supporting transactions because they may not reflect all of the transactions. In addition, unusual transactions such as correcting entries or transfers between one customer's accounts, may be counted twice or not at all.

To perform above-the-line testing:

1. Review the process and documentation used to reconcile the data extracted from the bank's core system to the data submitted for transaction monitoring to ensure that all intended data is included.
2. For each rule selected, select one or more customers and extract the customers' transactions using the same logical components used in the rule.
3. Compare the transactions that generated the alerts to the transactions extracted and resolve any differences, including nuances in the logical component.
4. Continue to compare extracted transactions for each customer until the logical components used in the rule are confirmed to be operating as intended.
5. Trace the customers reviewed to relevant reports.

5.5 Below-the-Line Testing

The purpose of below-the-line testing is to confirm that all alerts that should have been generated were generated and reported. Below-the-line testing begins with the data, applies the logic for a rules, and confirms that the alerts were generated as appropriate. Below-the-line testing also confirms that alerts that did not generate any alerts are operating as intended. Below-the-line testing is more complex because the logical components have to be re-engineered using queries or other extraction processes.

To perform below-the-line testing:

1. For each rule selected design a query to extract customers who meet the logical components of the rule.

2. Subject the entire data extraction to the query. Resolve any disparities by reviewing the transactions for the customers who meet the criteria defined in the query.
3. Design queries for minimum regulatory requirements: CTRs and SARs.
4. Design queries for BSA Red Flags that are reflected in the Risk Assessment.
5. For peer groups, review algorithm to group customers for a selected peer group. Extract historical data for customers to confirm appropriate peer group assignment.
6. For selected subset of customers, confirm calculation of customer risk scores is accurate if calculated by the model.

5.6 Model Outputs and Reports

The model outputs consist of several components that are provided in reports that contain various levels of detail and frequently dashboards that summarize the model results and metrics. Throughout testing, especially transaction monitoring testing, the alerts reported are tested for accuracy. However, compliance staff need supporting information for the alerts to investigate the alerts and potentially file SARs.

The validation should include a review of the reports to verify that they include required information for investigations, including transactions that triggered the alert and data required for the SAR. Reports at the summary level can be supplemented with access to the supporting transactions through the model's interface as well.

The model should also provide metrics about the customer and transaction base so that the productivity of alerts can be calculated and correlation between alerts and the data can be assessed. The metrics should cover the entire monitoring lifecycle, including

- Statistics on customers with transactions, preferably by risk level
- Transaction volumes, preferably by transaction code
- Alerts generated by customer and by transaction code
- Alerts referred to investigation and ultimately converted to SARs

This type of information should be used to manage the AML department by estimating the staffing requirements and staff productivity. Trend analysis can be maintained that tracks the monitoring results and can be an early indicator of changes in the bank's risk profile.

5.7 Conclusion

Validating the outcomes of an AML model is challenging due to the large volume of transactions and complex logic used to generate alerts. The volume of transactions requires IT resources and a data analyst with expertise in writing queries. The complexity of the logic used is difficult to comprehend at a detailed level and vendors are frequently reluctant to release detailed explanations of the logical processing. Using an approach that focuses on identifying and testing the logic used has several advantages over using statistical or random sampling, including:

- Comprehensive review of all rules to identify all logical components
- Ability to test all logical components by testing a subset of rules

Despite the investment in IT resources and time required to conduct a validation based on logical components, it can provide a high degree of assurance that the model is working as intended and identify issues with the model.

Appendix 1: BSA Data Requirements

The following data requirements are excerpted from the BSA Examination Manual.[iv]

BSA Data Requirements

BSA Section	Data
Purchase and Sale of Monetary Instruments Recordkeeping — Overview	If the purchaser **has a deposit account** with the bank: • Name of the purchaser. • Date of purchase. • Types of instruments purchased. • Serial numbers of each of the instruments purchased. • Dollar amounts of each of the instruments purchased in currency. • Specific identifying information, if applicable. If the purchaser **does not have a deposit account** with the bank: • Name and address of the purchaser. • Social Security or alien identification number of the purchaser. • Date of birth of the purchaser. • Date of purchase. • Types of instruments purchased. • Serial numbers of each of the instruments purchased. • Dollar amounts of each of the instruments purchased. • Specific identifying information for verifying the purchaser's identity (e.g., state of issuance and number on driver's license).
Funds Transfers Recordkeeping — Overview	• Name and address of the originator. • Amount of the payment order. • Date of the payment order. • Any payment instructions. • Identity of the beneficiary's institution. • As many of the following items as are received with the payment order: –Name and address of the beneficiary. –Account number of the beneficiary. –Any other specific identifier of the beneficiary. If the originator is not an established customer of the bank, in addition, the originator's bank must collect and retain other information, depending on whether the payment order is made in person. If a payment order is not made in person, the originator's bank must obtain and retain the following records: • Name and address of the person placing the payment order. • The person's TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack there • Information retained must be retrievable by reference to the name of the originator.

BSA Section	Data
Funds Transfers Recordkeeping — Overview Travel Rule Requirement	For funds transmittals of $3,000 or more, the transmitter's financial institution must include the following information in the transmittal order at the time that a transmittal order is sent to a receiving financial institution (1010.410(f)(1)): • Name of the transmitter, and, if the payment is ordered from an account, the account number of the transmitter. • Address of the transmitter. • Amount of the transmittal order. • Date of the transmittal order. • Identity of the recipient's financial institution. • As many of the following items as are received with the transmittal order: –Name and address of the recipient. –Account number of the recipient. –Any other specific identifier of the recipient. • Either the name and address or the numerical identifier of the transmitter's financial institution. **Responsibilities of Beneficiary's Banks** Recordkeeping Requirements For each payment order of $3,000 or more that a bank accepts as a beneficiary's bank, the bank must retain a record of the payment order. **Proceeds Delivered in Person** • Name and address. • The type of document reviewed. • The number of the identification document. • The person's TIN, or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. • If the institution has knowledge that the person receiving the proceeds is not the beneficiary, the institution must obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's identification. **Proceeds Not Delivered in Person** If proceeds are not delivered in person, the institution must retain a copy of the check or other instrument used to effect the payment, or the institution must record the information on the instrument. The institution must also record the name and address of the person to whom it was sent.

End Notes

[i] Board of Governors of the Federal Reserve System Office of the Comptroller of the Currency, "Supervisory Guidance on Model Risk Management," http://www2.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf (April 4, 2011)
[ii] Financial Crimes Enforcement Network, "Suspicious Activity Reporting Guidance," https://www.fincen.gov/news_room/rp/sar_guidance.html
[iii] Federal Financial Institutions Examination Council, "Bank Secrecy Act Anti-Money Laundering Examination Manual, Overview," https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_015.htm
[iv] Federal Financial Institutions Examination Council, "Bank Secrecy Act Anti-Money Laundering Examination Manual, Appendix H: Suspicious Activity Reporting," https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf
[v] Cognizant White Paper, "Models, Model Risk and Running Effective Model Management Programs," http://www.cognizant.com/InsightsWhitepapers/model-risk-and-running-effective.pdf (April 2015)
[vi] SAW Center for Financial Studies, Industry Working Paper Series 07-02, "The Future of AML/CFT – Technology, Data, People," Rohan Bedi, NUS Business School, National University of Singapore, https://bschool.nus.edu/Portals/0/images/SAW/docs/future-aml_edit.pdf
[vii] Nancy E. Lake, CAMS, "What Auditors Should Know and Ask About BSA/AML Software Before a Successful Audit Can Be Conducted," http://www.acams.org/aml-white-paper-software/
[viii] Dallas M. Wells, "A Practical Guide for ALM Model Validation," Financial Managers Society White Paper, http://www.fmsinc.org/documents/membercenter/whitepapers/apracticalguideforalmmodelvalidation.pdf
[ix] protiviti Risk & Business Consulting, "Measuring the Right Metrics and Leveraging Risk and Performance Indicators to Enhance End-to-End Transaction Monitoring Program," http://www.protiviti.com/en-US/Documents/POV/POV-Using-Metrics-To-Enhance-the-TM-Program-Protiviti.pdf
[x] Federal Financial Institutions Examination Council, "Bank Secrecy Act Anti-Money Laundering Examination Manual, Appendix O: Examiner Tools for Transaction Testing" https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf