Preventing Board and Management Liability for Violations of AML Rules

Navigating New Rules and Regulations That Place Increased Responsibility on Boards and Compliance Officers for the State of Institutional Compliance Programs

A WHITE PAPER FROM SURVEILLENS and QUATTRO PROCESSING SERVICES

AUGUST 2017

Contents

Introduction

Banks and other financial institutions have long been subject to rules requiring compliance with Bank Secrecy Act ("BSA"), anti-money laundering ("AML") and Office of Foreign Assets Control ("OFAC") rules. As a result of the associated financial (e.g., fines and penalties for non-compliance) and non-financial effects of non-compliance with these rules, transaction risk remains a primary concern for banks and financial institutions.

In June 2016, NYS' Department of Financial Services ("DFS") raised the bar in mandated BSA/AML compliance efforts by issuing Part 504 of the NYDFS Superintendent's Regulations ("DFS Rule 504")[1].

While DFS Rule 504 is one of the first of its kind, it is likely to be the next step in the monitoring and compliance of financial institutions that will see regulators placing increased (i) scrutiny on the structure and sophistication of the regulated institutions' monitoring and watchlist systems, and (ii) responsibility and accountability on senior management and the Board of Directors for the design and implementation and maintenance of a compliance program that satisfies the regulators' increasing demands.

Other jurisdictions, both domestics and foreign, have also recently signaled their intent to move in this direction. Most recently, in 2016, the UK's Financial Conduct Authority ("FCA") issued the Senior Managers and Certification Regime which created increased individual accountability for decision making and conduct of senior management of banks and other financial institutions which did not meet the FCA's standards.

Accordingly, the compliance and monitoring functions of banks and other covered institutions should not be surprised to see other domestic and foreign jurisdictions increasingly instituting laws similar to DFS Rule 504, and thus forcing their Boards and Compliance officers to be intimately involved in the maintenance of the institutions' proactive compliance programs. This wind of change in the payment world has amplified the need to have a robust and effective end-to-end enterprise risk management model.

Quatrro Processing Services and SurveilLens have teamed up to deliver next generation analytic solutions with an advanced suite of fraud mitigation and end-to-end enterprise fraud risk management. The alliance integrates Quatrro's advanced algorithm and dynamic rule management with SurveilLens unmatched anomaly detection and monitoring capabilities, extending the breadth of fraud management.

This White Paper published jointly by Quatrro Processing Services and surveilLens will discuss the impact DFS Rule 504 and similar legislation will have on covered institutions as well as offering insights into the steps Boards and Compliance Officers can take to make sure they achieve compliance and avoid personal and institutional liability.

[1] Part 504 of the DFS Superintendent's Regulations), http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf.

The Impact of DFS Rule 504 and Similar Rules

DFS Rule 504 requires that regulated financial institutions[2]:

- maintain Transaction Monitoring and Filtering Programs reasonably designed to
  - monitor transactions after their execution for compliance with BSA/AML laws and regulations, including suspicious activity reporting requirements; and
  - prevent unlawful transactions with targets of economic sanctions administered by OFAC."[3]
- incorporate risk assessments and testing into its programs;
- have members of senior management and/or the Board of Directors annually certify that they have taken the necessary steps to comply with the Final Rule's Transaction Monitoring and Filtering Program requirements and that, to the best of their knowledge, the Program complies with the Final Rule.[4] In other words DFS Rule 504 requires that senior management and/or the Board assume responsibility for the validation of the financial crime surveillance system.

The DFS Rule is effective as of January 1, 2017, with the first annual certification and compliance findings due by April 15, 2018.[5]

While most financial institutions may already have processes in place that may in spirit comply with its provisions, DFS Rule 504 contains specific provisions that will require institutions to update or rework existing systems to meet its requirements.

The Transaction Monitoring and Filtering Program

The starting point of any financial institution compliance program begins with a transaction monitoring and watch-list filtering program which analyzes transactional information for the purposes of identifying suspicious behaviors. Indeed, DFS Rule 504 focuses on the implementation and maintenance of transaction monitoring and filtering programs with the following certain minimum desirable attributes[6]:

[2] Under DFS Rule 504 'Regulated Institutions' means "all banks, trust companies, private bankers, savings banks, and savings and loan associations chartered pursuant to the New York Banking Law… and all branches and agencies of foreign banking corporations licensed… to conduct banking operations in New York."
[3] DFS Rule 504, §504.3.
[4] DFS Rule 504, §504.7.
[5] DFS Rule 504, §504.6.
[6] DFS Rule 504, §504.3.

Transaction Monitoring Program Attributes

1. Based on the institution's risk assessment (discussed below).
2. Reviewed and periodically updated with consideration to changes to applicable BSA/AML laws, regulations and regulatory warnings, and other relevant information.
3. Matching of BSA/AML risks to products, services, and customers/counterparties.
4. Design of BSA/AML detection scenarios to detect potential money laundering or other suspicious or illegal activities.
5. Comprehensive pre- and post-implementation testing.
6. Documentation of current detection scenarios and the underlying assumptions, parameters, and thresholds.
7. Listing and documentation of protocols and processes regarding the investigation of alerts, decision making process for filing of alerts and responsible functions and individuals.
8. Subject to an on-going analysis to assess the effectiveness of the detection scenarios, the underlying

Filtering Program Attributes

1. Based on the institution's risk assessment (discussed below).
2. Based on technology, processes, or tools for matching names and accounts.
3. Comprehensive pre- and post- implementation testing.
4. Subject to ongoing analysis to assess the logic and performance of the matching systems and the threshold settings.
5. Documentation regarding the intent and design of the Filtering Program tools, processes or technology.

Transaction Monitoring and Filtering Program Attributes

1. Identification of all data sources that contain relevant data.
2. Validation of the integrity, accuracy and quality of data to ensure completeness and accuracy of data flowing to the Transaction Monitoring and Filtering Program.
3. Data extraction and loading processes to ensure a complete and accurate transfer of data from its source to automated monitoring and filtering systems, if automated systems are used.
4. Governance and management oversight, including policies and procedures governing changes to the Transaction Monitoring and Filtering Program to ensure that changes are defined, managed, controlled, reported, and audited.
5. Vendor selection process if a third-party vendor is used to acquire, install, implement, or test the Transaction Monitoring and Filtering Program or any aspect of it.
6. Funding to design, implement and maintain a Transaction Monitoring and Filtering Program that complies with the DFS Rule 504 requirements.
7. Qualified personnel or outside consultant(s) responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the Transaction Monitoring and Filtering Program.
8. Periodic training of all stakeholders with respect to the Transaction Monitoring and Filtering Program.

Based on the above, the development of a successful transaction monitoring and filtering program that satisfies the requirements of DFS Rule 504 should focus on six key areas:

1. Development of processes surrounding the identification, extraction and validation of data.
2. Utilization of advanced methodologies to analyze data.
3. Development of risk assessment processes that align with the transaction monitoring and filtering program.
4. Testing of the transaction monitoring and filtering program.
5. Appropriate oversight and accountability for the transaction monitoring and filtering program.
6. Hiring and training of qualified personnel.

Processes Surrounding Identifying, Extracting, Validation and Integrating of Data

The ability of an intuitions' transaction monitoring and filtering program to successfully identify suspicious transactions is first and foremost dependent on the quality and accuracy of the data being fed into the program. Data fed into the program should not only be capable of being analyzed (i.e., in a format that makes analysis easy), but also relevant to the purpose for which it is being analyzed. To achieve this, institutions need to have processes around the identification, extraction and analysis of data.

When identifying the relevant population data for analysis, institutions should take care to integrate information from other functions, departments, business units and sources, such as customer onboarding documents and the entity risk assessment. Business units, departments and functions across the institution should be able to communicate and collaborate with each other to provide for a clear picture of all possible relevant data. Data identified for analysis purposes should be subject to formal extraction and loading processes with sufficient controls to ensure that the all relevant data is accurately transferred.

After all relevant data sources are identified and the data is extracted and gathered, the quality and accuracy of customer and transactional data should be validated as it flows from source systems into the monitoring and filtering program(s). This process may be subject to complications because platforms often have to extract and load data from multiple source systems and architectures within an institution, some of which may be legacy systems. Alternatively, institutions may not possess effective or efficient data sharing methods across the entity resulting in individual business units or functions owning potentially relevant information that remains siloed and unavailable for analysis. Thus, institutions will need to evaluate the data architecture and source systems supporting the transaction monitoring and filtering to start identifying potential data quality or data flow issues.

In order to assess the effectiveness of the model, institutions should also perform detailed model validation and document the key assumptions underlying that validation. Finally, procedures around loading processes should also be developed to achieve accurate transfers and track and

document the origins and then implement processes to identify and evaluate changes to systems and data structures.

Recommended Practice

- Develop policies and procedures around the identification, extraction and validation of data from all of the institution's relevant sources systems, business units and functions.

Data Analysis Methods

In order to assess transaction data, it is imperative that Transaction Monitoring and Filtering Programs be sufficiently technologically advanced to identify and prevent fraudulent transactions. This can be made possible via dynamic cloud network supported by highly reliable behavioral analytics, advanced algorithms and dynamic rule management designed to meet the highest security standards.

As financial crime methods have evolved over time and become more sophisticated, particularly with the introduction of new product and service offerings and cross border banking services, monitoring and detection programs must utilize technologies that are more advanced than traditional manual reviews or machine based reviews that use pre-determined rules to identify fraudulent activity. Instead, institutions must look to automated, risk-based big data platforms that utilize advance technologies such as machine learning and analytics-based anomalous behavior detection that can analyze massive amounts of structured and unstructured data, detect outliers and suspicious behavior patterns even when they do not breach any pre-determined BSA/AML or other illegal scenarios. These platforms should also be capable of handling an extensive documentation of scenarios, thresholds and parameters to detect suspicious behavior.

Platforms should not take a "vacuum" approach to analyses but must be able to analyze transactions by incorporating all relevant and available information. This will allow institutions to "connect the dots" to identify customer patterns and behaviors and also identify relationships that might not otherwise be obvious from a review of transactions in isolation.

Further, to minimize losses and save resources expended in chasing fraudulent transactions, platforms must be able to generate suspicious alerts in real time, before, or at the time the transaction is consummated. The real-time insights into risk management programs offered through powerful analytics will ensure propelling business growth by reduction of fraud loss.

Similarly, filtering programs should also allow institutions to conduct meaningful due diligence on customers and other third parties. Most institutions have traditionally used manual reviews when performing customer due diligence and third-party screening against watch lists, negative news and adverse media. Filtering programs should use technologies such as graph databases and network analyses to allow for the identification of common relationships between customers

and entities as well as identifying beneficial ownership. This will help the institution in achieving a holistic view of its relationships with potentially high risk third parties.

Finally, institutions should make sure there is a documented process that outlines (i) the process for clearing of alerts and investigations in both the transaction and filtering programs and (ii) the roles and responsibilities of individuals in the suspicious activity decision making and reporting process. Transactions requiring investigation should be appropriately segregated into case management to determine if a regulatory filing (e.g., SAR or CTR) is required. A documented workflow that outlines roles and responsibilities in the review, escalation and investigation process serves to eliminate confusion about each functions' and individual's responsibilities when problematic situations arise. Finally, all workflows should be subject to an audit trail identifying that records who in the institution had involvement in the each stage of the alert and investigation process.

Recommended Practice

- Consider the use of advanced technologies such as machine learning, predictive analytics, network analyses and graph databases in your institution's transaction monitoring and filtering program.
- Review, escalation and investigation workflows should be documented with roles and responsibilities clearly assigned to specific individuals and functions.

Risk Assessment

DFS Rule 504, consistent with other BSA/AML regulations that came before it, requires the use of an enterprise-wide comprehensive risk assessment that is customized based on among other things, the institution's size, staffing, operations, services, products, geography of operations, customer type and activity as well as any audit or other findings of program weaknesses. Results of the risk assessment and any updates or changes should be incorporated into the parameters of the transaction monitoring and filtering program. Once established, the risk assessment and the programs must be reviewed, analyzed, tested and updated periodically.

The requirement to perform risk assessments is not a new concept for financial institutions. It is clear that there is an expectation by regulators for BSA/AML and OFAC Risk assessments to provide a deeper review of ALL areas of the organization. Current best practices dictate that risk assessments minimally consider and include the following:

- The risk assessment should properly reflect the current BSA/AML risk profile across the *entire organization*.
- The risk assessment should clearly identify (i) all areas within the organization with direct BSA/AML responsibilities and (ii) each BSA/AML responsibility specific to each function or business unit.
- A detailed, in-depth evaluation of the risks present in each business unit such as every existing, new or significantly expanded or modified added customers, geographies,

products, services and systems used or offered by each BU within the organization with direct BSA/AML responsibilities (i.e., inherent risk).

- An evaluation of the potential and impact of each identified risk.
- An evaluation of the design and operating effectiveness of systems and internal controls utilized by each business unit and the possibility that those controls will fail to capture the identified risks (i.e., control risk).
- The determination of the risk remaining risk after consideration of existing polices procedures and controls of each product, service and system used or offered through each business unit (i.e., residual risk).
- Incorporation of risk assessments conducted by other functions (internal audit, compliance, business units etc.) in the organization.
- Major events or changes (e.g., mergers, acquisitions, expansions, expansion into new markets, new or changes to products or services, prior controls deficiencies and weaknesses that have not been corrected, the exceeding of determined thresholds regarding assets under management, deposits, or outstanding credit etc.) that may have an impact on the entity.
- Findings should be supported by appropriate qualitative and quantitative data.
- Documented processes for periodic review and updating of the risk assessment, insuring that all changes to business units with any BSA/AML responsibilities are represented appropriately.
- Sharing and communication with all business units across the organization, including management and appropriate staff.
- Reporting of results to the appropriate supervisory committee(s) and/or to the Board of Directors.

There is not one recommended methodology or format specified or method required when completing a risk assessment. As long as the risk assessment can be understood by the appropriate parties who will review its contents, the format should be acceptable to federal regulators. Quatrro & SurveilLens will ensure effective risk assessment & monitoring by integrating concepts of internal control and strategic planning with evolved machine learning capabilities, thus enhancing customer experience.

Institutions should review their current AML and OFAC assessments to determine if they include the above attributes, are otherwise sufficient in scope, depth and frequency and if they adequately capture all risk. Further, identified risks should be factored into the parameters of the Transaction Monitoring and Filtering Program to ensure that objectives of that program are aligned with the risk assessment.

Practice Tip

- The risk assessment process should be at the entity level and include the identification of operational and compliance risks, owners of the identified risks, controls in place to mitigate and reduce risks, and an assessment of the risk potential and impact.

Testing of the Transaction Monitoring and Filtering Program

While DFS Rule 504 mandates comprehensive pre- and post-implementation testing of the Transaction Monitoring and Watch List Filtering programs "to assess the effectiveness of currently used detection scenarios, threshold values, parameters and assumptions", it is silent with respect to details of the nature, amount and form of testing required.

Accordingly, questions and issues for institutions to consider when designing testing programs should be include:

- What level and frequency of testing is required for compliance? The answer to this question should incorporate other factors such as the results of the risk assessment, the number of transactions being marked as suspicious by the monitoring program, the amount of the human and capital resources the institution is able to dedicate to the testing function. Consideration should be given to outsourcing this function to qualified personnel particularly if the monitoring program produces many flagged transactions.
- What role, if any, should other functions such as business, compliance and internal audit play in the testing process?
- What is the appropriate type and level of documentation necessary for the testing process?
- What is the process for remediating weaknesses identified during the testing process?

Program Oversight and Accountability

DFS Rule 504 requires an annual certification by members of senior management and/or the Board of Directors that they have: (1) reviewed the documents, (2) taken steps to confirm that the transaction monitoring and filtering programs comply with the final regulation and (3) affirmed that, to the best of their knowledge, the programs are compliant.

The DFS Rule 504 certification process is not unlike the certifications required of management under Sections 302, 404 and 906 of the Sarbanes Oxley Act. Institutions should develop a formal process to ensure that relevant information is escalated to the appropriate members of management so that they can comfortably meet certification requirements.

While in most institutions, the certification will fall on the shoulders of the Compliance Officer, the institution's Board should still be familiar with issues raised during the monitoring and testing processes. Accordingly, there should be a formalized and documented escalation process to ensure that management and/or the Board is receiving the level of information that they will require to sign the certification with confidence. Both senior officers and board members who will be expected to certify should be fully briefed and trained on the underlying detail of the programs being used as the basis of the certifications.

Senior Compliance and Risks Officers, CEOs and the Board should set the tone early on and make clear their expectations regarding the importance of compliance with the requirements to the ongoing success of the Regulated Institution. Additionally, senior management must also walk the talk by taking affirmative steps in showing the importance they place on the requirements. Such steps would include:

- Ensuring that all processes are clearly documented and disseminated to all employees
- Swiftly punishing deviations from policy and performing root cause analyses to understand why such deviations occurred and what can be done to prevent future deviations
- Providing adequate resources (financial and human capital) for the compliance and monitoring function and underlying programs
- Providing training to stakeholders with respect to these programs.
- Requiring that changes to the monitoring and filtering program, including the scenarios and testing parameters, are approved before hand as those may affect the nature of the information being reviewed by management.

Practice Tip

- Consider having individual functions and business units issue sub-certifications that roll up to an overall entity certification. This would require these units and functions to have their "skin in the game".

Qualified Personnel

The success of any program is ultimately dependent on the qualifications and experience of the individuals charged with its implementation, design and oversight. For instance, what, if any, additional action is required when alerts or hits are triggered.

While the requirements of the transaction monitoring and filtering program provisions will require the integration of business functionalities, such as the internal audit and compliance departments, it will also undoubtedly generate a need for a greater number of internal or externally trained and experienced AML compliance-dedicated personnel and resources. In order to demonstrate adequate governance and oversight, regulators will expect that the personnel involved are trained, skilled, experienced and appropriately supervised.

Conclusion

DFS Rule 504 has the potential to launch similar legislation by Federal, state and local agencies in and out of NYS, especially those that also audit DFS regulated institutions. Regulators in other foreign jurisdictions may also adopt the DFS approach of requiring transaction monitoring and filtering systems, and mandating senior officer/board liability as a means of increasing the requirements of their own AML filtering laws. Thus, banks and financial institutions, whether they

are currently subject to DFS Rule 504 or not, should proactively review their current compliance frameworks and strengthen systems and processes as necessary.

Quatrro and SurveilLens developed their solution and services around Big Data and next generation analytics to create anti-fraud compliance programs and futuristic solutions to reduce frontline risks, maximize revenue and attain competitive advantage.

The SurveilLens Platform

surveilLens™ is a single technology platform that goes beyond traditional monitoring systems to integrate into one solution, the elements of an anti-fraud compliance program with machine learning and the features of Big Data platform described in this document.

surveilLens utilizes the latest big data methods and artificial learning (AI) capabilities to monitor all of an institution's data including:

- ✓ *Processing of 10,000,000 + transactions a day (easily scalable beyond that)*
- ✓ *Up to 10,000 customizable rules*
- ✓ *100 percent data coverage and analysis*
- ✓ *Real time updates*
- ✓ *Capable of integrating data from multiple systems*
- ✓ *Dynamic rules based engine*
- ✓ *Database searching and matching*
- ✓ *Real time updates*
- ✓ *Anomaly detection*
- ✓ *Text mining*
- ✓ *Predictive modelling*
- ✓ *Advanced statistical analysis including machine learning*
- ✓ *Network analytics*

The surveilLens™ solution consists of several modules including: transaction monitoring, anomaly detection, case management, third-party due diligence policies and procedures, training and certifications, risk assessments, and internal controls. These modules work in isolation or with each other to create integrated workflows.

The various workflows can be customized and designed to give maximum flexibility and efficiency. The solution addresses organization, entity, industry, and region-specific requirements. It is a simple to use, plug-and-play model. Clients can pick as many modules as they need to develop or integrate into their existing compliance programs.

surveilLens™ is dynamic with self-learning capabilities. Designed to be implemented within a network or in the cloud, the surveilLens™ solution meets the highest security standards including but not limited to, global data privacy requirements. Thus, clients and compliance professionals can rest assured that their data is secure.

About surveilLens

surveilLens™ is a compliance solutions company that provides advanced technology-enabled governance, compliance and risk (GRC) solutions. Our software, is designed to identify, mitigate and remediate organizational risks while bringing convenience, effectiveness and efficiencies to an organization's overall compliance program. Founded by professionals with decades of experience in compliance, technology, data science and auditing, we offer our clients customized and scalable compliance solutions. Our goal is to transform the traditional approach to GRC from a manual process to an automated one, where all of a company's data sources are harnessed to provide meaningful insights.

About Quatrro Processing Inc.

Quatrro Processing Services (QPS) is a leading provider of services to Financial Institutions, Prepaid Issuers, Wallet Companies, Merchants and Payment Gateways worldwide. Quatrro's service offerings for financial institutions help fulfill the ever changing customer needs while mitigating the threats, balancing false positives with urgency and timeliness that the marketplace demands without any significant upfront investments in technology and infrastructure.

For more information:

SurveilLens
Visit: www.surveil-lens.com
inquiries@surveil-lens.com
or call (212) 804-5734

Quatrro Processing Inc.
Visit: http://www.quatrroprocessing.com