INSIGHT

FEBRUARY 2019

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

PART 504 OBSERVATIONS AND RECOMMENDATIONS

Since the implementation, in January 2017, of the New York State Department of Financial Services ("DFS") Part 504 Banking Division Transaction Monitoring and Filtering Program Requirements and Certification ("Part 504"), Sia Partners has observed how banks have been working to comply with it. In this article, we focus on some of the most challenging parts of Part 504, the strategies banks have been implementing to address them and the shortcomings they still have to solve. These shortcomings pertain to the banks' risk assessment, inefficiencies in screening system, independent testing, data validation and governance processes. Below we discuss these and other deficiencies and provide associated recommendations to improve the soundness of bank's Bank Secrecy Act ("BSA") and Anti-Money Laundering ("AML") framework to support their efforts to comply with Part 504.

Transaction Monitoring and Filtering Programs

Risk Assessment

Part 504 requires the Board of Directors Resolution or Senior Officers Compliance Finding that each Bank maintains a Transaction Monitoring and Filtering Program in compliance with Section 504.3.

Part 504 specifies the Transaction Monitoring and Filtering Program be based on a comprehensive risk assessment including "an enterprise wide risk assessment, that takes into account the institution's size, businesses, services, products, operations, customers/counterparties and their locations, as well as the geographies of its operations and business relations which lay the foundation for the requirement" [1]. The financial institution's risk assessment can be independent of the sanctions risk assessment or it can be included as an enterprise wide risk assessment.

Observation: Since the implementation of the Part 504, Sia Partners has found deficiencies in banks' risk assessments. Specifically, banks have not incorporated all customer types into the overall risk assessment. Also, in some instances, banks lack an enterprise wide risk assessment. This results in risk to the financial institution as it creates an incomplete overall risk profile.

The recent fine incurred by Capital One Bank (USA) N.A in the amount of $100 million was a consequence of deficiencies identified in the Bank's BSA/AML program, included among other things, the absence of an enterprise wide risk assessment[2] and systemic deficiencies in its transaction monitoring systems. This underscores the importance of a strong risk assessment framework as the foundation of the transaction monitoring and sanctions filtering programs

Recommendation: Banks should have a clearly defined risk assessment methodology. This methodology must include both quantitative and qualitative factors to determine the inherent risks of the institution, allow for the implementation of corresponding control mitigants, and ultimately determine the bank's level of money laundering and sanctions related risk exposure. The risk assessment methodology should be updated at least annually, by a designated BSA/AML and or Sanctions Officer or independent senior official. The risk assessment methodology should be communicated to all pertinent parties within the organization to establish a sound foundation of risk awareness and ensure customer risk ratings are reviewed and updated periodically. This will help ensure the appropriate level of due diligence and monitoring is consistently applied to the customer base.

Risk-Based Transaction Monitoring

Part 504 requires monitoring of all transactions to identify potential BSA/AML violations and facilitate filing of Suspicious Activity Reports ("SARs")[3]. All Transaction Monitoring and Filtering Programs are to be risk based, which means that the monitoring applied to a customer depends on its risk profile. For instance, high risk customers should be subject more stringent monitoring criteria than lower risk customers. Additionally, monitoring rules should also be based on customers profile and activity. This can be achieved through on-going calibration of the transaction monitoring system with third-party vendor solutions.

[1] See Part 504.2 (f)

[2] US Department of the Treasury Comptroller of the Currency News Release - October 2018

[3] See Part 504 504.3(a)

Inefficiencies in Screening Systems

According to Part 504, banks are tasked with ensuring names of individuals and entities are effectively screened against Office of Foreign Assets Control (« OFAC ») Specially Designated Nationals And Blocked Persons List (« SDN List ») and those lists issued by the United Nations, European Union and other national and supra-national entities.

The bank must ensure that all third party vendor solutions used for sanctions screening operate accurately. We have observed filtering systems that do not always recognize name variations such as concatenated/separated names, names with multiple or extra letters, phonetic variations and truncated names. In October 2018, JP Morgan Chase was fined $5 million as a result of a third-party vendor filtering system failure to identify customer names with hyphens, initials, middle and last name, and names similar to potential or identical names on the SDN List. [4]

It is imperative for banks to have a transaction filtering process that accurately screens entities and individuals, which pose sanctions risks.

Filtering not Conducted with the Most Up-to-Date Sanctions Lists

In order to ensure compliance with OFAC regulations and to identify individuals and entities on all relevant sanctions lists, there must be an ongoing monitoring of the filtering system by banks. The SDN and other sanctions lists are frequently updated. There is no predetermined timetable, but rather names are added or removed as necessary and appropriate. Risks exist when there are gaps between the time the sanctions lists are updated and when that information is fed into the bank's filtering system.

All lists used in the filtering system need to be kept up to date reflect, on a timely basis, all changes to the SDN and other sanctions Lists. Transactions with sanctions nexus should not be processed through the filter without detection.

We recommend that banks ensure that filtering systems always contain the most recent sanctions lists

High Volumes of False Positives - the Risk of Failing to Identify Suspicious Transactions and Sanctions Matches

Banks are often burdened with managing high volumes of alerts, which may contain a high volume of false positives. High volumes of false positives mean the compliance staff has to spend time reviewing and dispositioning each false positive which may lead to a higher risk of missing true suspicious activities.

Recommendation: Banks can utilize Artificial Intelligence ("AI") for transaction monitoring and sanctions filtering to reduce the volume of false positives. The use of AI for Compliance and AML purposes has recently been emphasized in a speech by Federal Reserve Governor Lael Brainard[5].

Machine learning algorithms can also be used, either to:

- Automate repetitive tasks requiring a little investigation, for instance, the clearing of alerts that one observed to be generated by identified messages with words similar to those on the sanctions lists; or,
- Identify suspicious transaction patterns difficult to identify otherwise.

Machine learning algorithms are already used by intelligence agencies and police departments. The use of AI for transaction monitoring and sanctions screening can enable a bank to screen higher volumes of transactions more efficiently to help increase operational efficiencies and reduce cost.

Independent Testing

Part 504 rule requires the independent testing of the Transaction Monitoring and Filtering Programs. Independent testing can help identify errors in transaction monitoring and sanctions screening and reduce the chance of processing suspicious transactions as well as transactions to prohibited entities and individuals. Failure to conduct adequate independent testing poses risks to financial institutions that can result in penalties imposed by regulators.

[4] See the Enforcement Information For October 5, 2018

[5] See Federal Reserve Governor Speech "What Are We Learning about Artificial Intelligence in Financial Services?"

The following examples highlight the importance of ensuring that Transaction Monitoring and Filtering Programs operate effectively:

- In July 2016, Compass Bank (aka BBVA Compass) was issued an OFAC Finding of Violation due to failure to identify and block inactive accounts owned by two individuals identified as OFAC SDNs. This occurred as a result of a misconfiguration in the bank's sanctions screening software[6] ;
- The National Bank of Pakistan processed multiple transactions to a sanctioned entity. The bank's filtering system failed, on multiple occasions, to detect the sanctioned party transactions, and as a result, the bank was fined[7].

Recommendation: Independent testing should be conducted on a periodic basis to determine the efficient operation of the bank's transaction monitoring and filtering systems. This can be conducted at different intervals based on the risk profile of the institution or as defined within its compliance procedures.

Independent testing should be conducted by an independent party, using an objective approach taking into account whether the program operates consistently with the bank's policies and procedures. This serves to assess the operational effectiveness of the systems to ensure compliance with regulatory requirements. Further the independent testing should be reviewed by a bank's internal audit department for adequacy of the risk assessment and controls to mitigate risk.

Lack of Documentation of Change Management Policy and Change Tracking

Regulators expect banks to periodically fine-tune rules of the Transaction Monitoring and Filtering Programs. We have observed that some financial institutions lack a detailed change management program.

Recommendation: An effective change-management program documents the full scope and impact of all changes relating to policies, procedures, processes, technology and staffing resources any such changes. Documentation of system changes must be clear and up-to-date, and include governance aspects such as those authorized to make changes to the models, the approvers of system changes, and a record of the changes made.

Data

Validation of the Integrity of the Data

According to the Part 504, the data that flows through the Transaction Monitoring and Filtering Programs needs to be assessed for its quality, accuracy and completeness[8].

The data for Transaction Monitoring Systems is usually generated from internal records. With respect to the Filtering Systems, data can be sourced from both internal and external data sources (i.e. OFAC, United Nations, European Union and other national and supra-national sanctions and law enforcement lists).

We have observed a leading practice of using of a clearly documented data flow chart to provide an overview of all of the sources of data. This includes the various transaction types that flow into the two systems, which helps ensure all sources of data are known, captured, monitored, analyzed and tested periodically.

Banks should also have a vetting process in place to determine whether a third-party vendor should be used to manage the data.

The **F**RB and OCC's *Supervisory Guidance on Model Risk Management* (« MRM ») states:

- The structure and schedule of the data feeds need to be defined;
- How duplication/consolidation of data is managed needs to be determined; and,

[6] U.S Department of Treasury, Enforcement Information for July 2016.
[7] U.S Department of Treasury, Enforcement Information for June 2015.

[8] See Part 504 504.3(c)(2)

- The impact of amendments to the systems and auditing of adjustments should be established[9].

Data Analyses and Validation

Data validation is the process of testing the data within the compliance systems to:

- Confirm that information from the core systems flows accurately through the monitoring and filtering systems;
- Confirm data fields have been translated as intended;
- Validate the mapping of data to capture all transactions;
- Determine which transaction types should be included: and,
- Relevant fields and changes in the core systems.

For the Filtering System, the data validation process is designed to analyze the way in which names of individuals and entities are scanned each time the sanctions list is updated. The accuracy and quality of the data is important to ensure that restricted individuals and entities are identified through the filtering program at onboarding and during the customer relationship with the bank.

As part of the data validation process, periodic independent validations have to be conducted in order to capture changes in data, products, services, institutions processes and to identify gaps that pose regulatory risks to the financial institution.

Recommendation: We recommend that the validation process be conducted by independent and qualified personnel who are able to attest to the conceptual soundness of the model and to its alignment with the risk profile of the financial institution. Statistical methodologies are good ways for validating the Transaction Monitoring system while mock-up name lists can be used to validate the Filtering system.

Furthermore, according to the MRM, validation of the models has to be an ongoing process to identify limitations or deficiencies and provide the ability to implement controls to manage identified deficiencies[10]. Ongoing assessment of the model helps to capture changes in products, services, transaction types and other factors as they arise.

We also recommend tests of the « Above-and-Below-the-Line » type. This consists of applying a small incremental change to the threshold, and determining, if the change in the system output is caused exactly by this small change in the threshold. Running this type of binary test indicates whether the threshold function is working or not. Such methods can also be adapted to the optimization and fine-tuning of thresholds for Transaction Monitoring systems.

Data Governance and Management Oversight

One of the key findings of the NYDFS is the lack of proper governance and management oversight in financial institutions, which lead to the implementation of Part 504.

Part 504 specifies a robust governance program which includes policies and procedures that govern the processes of the Transaction Monitoring and Filtering Programs[11]. A strong governance program includes documented policies and supporting procedures, which provide a roadmap of:

- How the transaction monitoring and Transaction and Filtering Programs are designed to function;
- Roles and responsibilities of the persons tasked with the execution of the various functions; and,
- Documentation of regular and ongoing training of staff to ensure quality outcomes and funding of the programs.

Further, Part 504 requires adequate reporting and appropriate auditing of any changes to the programs. Where gaps and/or issues have been identified, the governance program has to define the action steps required to control or remediate these identified issues.

[9] US Department of the Treasury Comptroller of the Currency, Supervisory Guidance on Model Risk Management

[10] US Department of the Treasury Comptroller of the Currency, Supervisory Guidance on Model Risk Management

Conclusion

Compliance with Part 504 has proven challenging for financial institutions, required to address many different aspects of Sanctions Filtering and Transaction Monitoring functions. First comes the risk-assessment of financial institutions and the design of their programs. Then, a third-party vendor solution is usually chosen and implemented. This solution has to be independently tested. Governance aspects are also key, from the governance of the program to data governance.

How Sia Partners Can Help You

Sia Partners has experts globally and locally in the US who can address Part 504 challenges. This includes strengthening the Risk Assessment, fine-tuning the Transaction Monitoring and System Filtering systems and methodologies, performing the independent testing and data validation and establishing an appropriate data governance and management oversight.

YOUR CONTACTS

DANIEL H CONNOR

CEO US
+ 1 (862) 596 - 0649
daniel.connor@sia-partners.com

LAUREN L. PICKETT

Director of Anti-Money Laundering, U.S. Sanctions, and FATCA
+ 1 (917) 439 - 3328
lauren.pickett@sia-partners.com

FIONA LAYNE-GERMAIN

Senior Consultant
+ 1 (516) 296 - 0563
fiona.germain@sia-partners.com

DAVID H COHEN

Senior Consultant
+ 1 (917) 445 - 1162
david.cohen@sia-partners.com

ABOUT SIA PARTNERS

Sia Partners is a next generation consulting firm focused on delivering superior value and tangible results to its clients as they navigate the digital revolution. With over 1,200 consultants in 15 countries, we will generate an annual turnover of USD 230 million for the current fiscal year. Our global footprint and our expertise in more than 30 sectors and services allow us to accompany our clients worldwide. We guide their projects and initiatives in strategy, business transformation, IT & digital strategy, and Data Science. As the pioneer of Consulting 4.0, we develop consulting bots and we integrate the disruption of AI in our solutions.

Abu Dhabi
PO Box 54605
Al Gaith Tower #857
Abu Dhabi – UAE

Amsterdam
Barbara Strozzilaan 101
1083 HN Amsterdam -
Netherlands

Brussels
Av Henri Jasparlaan, 128
1060 Brussels - Belgium

Casablanca
46, Boulevard Adbellatif
Ben Kaddour, Racine –
Casablanca 20000 -
Morocco

Charlotte
101 S. Tryon Street, 27th
Floor, Charlotte, NC 28280,
USA

Doha
Al Fardan Office Tower #825
PO Box 31316
West Bay Doha - Qatar

Dubai
Shatha Tower office #2115
PO Box 502665
Dubai Media City
Dubai - UAE

Hong Kong
23/F, The Southland
Building, 48 Connaught
Road Central
Central - Hong Kong

Houston
800 Town and Country
Boulevard, Suite 300
77024 Houston, TX

London
36-38 Hatton Garden
EC1N 8EB London - United
Kingdom

Luxembourg
7 rue Robert Stumper
L-2557 Luxembourg

Lyon
3 rue du Président Carnot
69002 Lyon - France

Milan
Via Vincenzo Gioberti 8
20123 Milano - Italy

Montreal
304 - 19 Rue le Royer Ouest
Montreal, Quebec,
Canada, H2Y 1W4

New York
40 Rector Street, Suite 1111
New York, NY 10006 – USA

Paris
12 rue Magellan
75008 Paris - France

Riyadh
PO Box 91229
Office 8200 - 12, Izdihar city
Riyadh 11633 - KSA

Rome
Via Quattro Fontane 116
00184 Roma - Italy

Singapore
137 Street Market, 10-02
Grace Global Raffles
048943 Singapore

Tokyo
Level 20 Marunouchi
Trust Tower-Main
1-8-3 Marunouchi,
Chiyoda-ku
Tokyo 100-0005 Japan

For more information, visit: **www.sia-partners.com**

Follow us on **LinkedIn** and **Twitter @SiaPartners**

siapartners