GLOBAL RADAR®

ASSURING INTEGRITY

WHITE PAPER:

Transaction Surveillance

INTRODUCTION

TRANSACTION SURVEILLANCE

As the overall landscape of the finance and trade world markets continue to evolve, the need for constant monitoring of individual activity has become increasingly necessary.

It has been said that information is the most valuable commodity for a business. This statement is extremely important for financial institutions. We can agree that, with very limited exceptions, all financial institutions create, receive and dispose of multiple information records on its customers: checks, contracts, invoices, correspondence (including emails), signature cards, and financial reports, account statements, etc. Each financial decision an individual or a business takes involves multiple elements of information that are valuable to different persons and for different purposes. Tracking all this data could be a daunting task.

$1-$2 trillion

According to PWC Global, "Global money laundering transactions are estimated at 2 to 5% of global GDP, or roughly U.S. $1-$2 trillion annually."

FinCEN may bring an enforcement action for violations of the reporting, recordkeeping, or other requirements of the BSA.

That is why knowing what types of information are needed to effectively monitor financial transactional activity is of extreme importance. As the overall landscape of the finance and trade world markets continue to evolve, the need for constant monitoring of individual activity has become increasingly necessary.

CHALLENGES FINANCIAL INSTITUTIONS FACE TODAY

Although the regulatory framework is in place for institutions to follow in regards to the reporting of suspicious financial activity, the monitoring of customer activity aspect is one of, if not the most, formidable challenges that an institution must take on, and this is due to the vast number of complications that can arise throughout the surveillance process.

Making matters all the more complicated are factors which are often directly related to the size of the organization at hand, such as manpower available, size of the budget allocated, increased regulatory obligations that must be met, and the growing costs of the AML/KYC/Surveillance software that is being purchased and eventually run by the company in general. It has been found that there is a direct correlation between the increased number of companies that have engaged in the financial securities business and the increased cost of AML software that is now evident, thus completely altering the market in regards to security software.

IMPLICATIONS OF ILLEGAL ACTIVITIES

According to PWC Global, "Global money laundering transactions are estimated at 2 to 5% of global GDP, or roughly U.S. $1-$2 trillion annually. Yet according to the United Nations Office on Drugs and Crime (UNODC), less than 1% of global illicit financial flows are currently seized by authorities" (PWC, 20161). These staggering statistics clearly illustrate why money laundering and terrorist financing are now gaining precedence in the eyes of national governments around the world. With the AML regulations in place, the need for transaction surveillance services is all the more important, not only to hinder the flow of financial crime worldwide, but also for respective corporations to avoid the assessment of immense fines (ranging from millions to billions of dollars, potentially) and strict sanctions, which can include travel bans, asset freezes, trade embargoes and other restrictions, not to mention the often devastating blow to the reputation of the company at hand.

In the matter of regulatory compliance, "under the Bank Secrecy Act (BSA), 31 (U.S.C. 5311 et seq.), and its implementing regulations at 31 C.F.R. Chapter X, FinCEN may bring an enforcement action for violations of the reporting, recordkeeping, or other requirements of the BSA. FinCEN's Office of Enforcementevaluates enforcement matters that may result in a variety of remedies, including the assessment of civil money penalties" (FinCEN, 2016).

For example, civil money penalties can be determined for violations in the keeping of records or for reporting violations, including failing to file a currency transaction report (CTR), a suspicious activity report, or a report of foreign bank and financial accounts (FBAR), and even for a failure to register with FinCEN in general. evaluates enforcement matters that may result in a variety of remedies, including the assessment of civil money penalties" (FinCEN, 2016). For example, civil money penalties can be determined for violations in the keeping of records or for reporting violations, including failing to file a currency transaction report (CTR), a suspicious activity report, or a report of foreign bank and financial accounts (FBAR), and even for a failure to register with FinCEN in general.

PURPOSES OF TRANSACTION SURVEILLANCE

An effective transaction monitoring system is an important component of any strong AML compliance program. The basic purpose of having an AML transaction monitoring system is to identify suspicious transactions and protect the institution from any that could be related to money laundering and/or terrorist financing, resulting in the institution filing relevant SARs. Most financial institutions rely on AML technology software to cull the transactions and pick out the potentially suspect transactions. Some smaller institutions use manually designed systems. Automated AML solutions include sanctions/black list screenings, customer profiling, and comprehensive transaction monitoring with reports/alerts.

DEVELOPMENT OF A TRANSACTION SURVEILLANCE COMPLIANCE PROGRAM

The development of a transaction surveillance program requires planning and careful implementation for it to be successful. The following principles should be applied when assessing the design or acquisition of a transaction surveillance system:

GOVERNANCE

Governance refers to how the institution manages and controls its business. Governance provides the structure through which an institution sets and pursues objectives while taking into account the regulatory and market environment and culture of the institution. The governance structure specifies the responsibilities for the board of directors, managers, auditors, and other stakeholders and specifies the level of authority and accountability for decision making. Governance also includes mechanisms for monitoring actions and decisions enterprise-wide. The development or acquisition of an AML transaction monitoring system (TMS) should follow the minimum governance requirements:

(a) Board of Directors approval and oversight; (b) designation of an officer responsible for managing all aspects of the TMS; (c) internal and external compliance monitoring; and (d) on-going training.

RISK ASSESSMENT

The same risk management principles that the institution uses in traditional operational areas should be applied to assessing and managing the risks associated with the TMS. This information should be in agreement with the overall institution's risk assessment and, at the same time, should be part the "large picture". By understanding and incorporating the risk profile of the institution in the TMS implementation process, the whole compliance program focuses on mitigating the associated risks.

The risk assessment process enables management to better identify and mitigate gaps in the internal controls. Although not required by regulation, a best practice approach is to reduce this analysis in written form as part of the due diligence conducted by the institution.

The development of the risk assessment generally involves two steps: first, identify the specific risk categories (i.e., products, services, customers, entities, transactions, and geographic locations) unique to the institution; and second, prepare a more detailed analysis of the risk factors identified and how they interact with the TMS. The development or acquisition and maintenance process of the TMS includes numerous risks. These risks include the possibility of loss resulting from inadequate processes, personnel, or systems. Losses can result from errors; fraud; or an inability to deliver products or services, maintain a competitive position, or manage information. The analysis should also consider the institution's current and proposed IT systems; interaction with affiliates and customers; internal lines of business; third parties (e.g., third-party providers) and the public. A detailed analysis of these risks and their respective controls should be part of the analysis and will certainly be required by the examiners.

As with any other function, the TMS risk assessment should be reviewed and periodically updated at risk-based intervals to take into account and reflect changes to applicable BSA/AML laws, regulations and regulatory warnings, as well as any other information determined by the institution to be relevant from the institution's related programs and initiatives.

DESIGNATION OF A COMPLIANCE OFFICER

The Board may delegate the design, implementation, and monitoring of specific TMS activities to management or a committee. The steering committee generally comprises senior management and staff from the IT and other appropriate business units. In smaller or less complex institutions that may not have steering committees these functions could be performed by management, IT department personnel, the board, or a board committee.

Committee members do not have to be department heads, but members should understand BSA/AML policies, standards, and procedures. Each member should have the authority to make and be held accountable for decisions within their respective business units. If the institution has a formal risk management function, risk management staff should participate in an advisory capacity.

Any designation should consider that the BSA Compliance Officer has one of the most relevant roles in this structure. The BSA Compliance Officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance and is also charged with managing all aspects of the BSA/AML compliance program. As such, the BSA Compliance Officer should have the decisive authority in any matters involving the TMS.

The BSA Compliance Officer is responsible and should be held accountable for the development and implementation of the processes taken to support the institution's business strategy in line with its risk appetite. The BSA Compliance Officer typically oversees the TMS budget and maintains responsibility for performance management, acquisition oversight, professional development, and training. In addition, the BSA Compliance Officer is responsible for implementing the designated systems and participating in planning activities. The management reporting structure should enable this position to accomplish these activities and ensure accountability for security, business resilience, risk reporting, and alignment with business needs.

TAILORED INTERNAL POLICIES, PROCEDURES AND CONTROLS

The institution's internal policies and procedures reflecting the implementation of the TMS should be described in writing and reviewed and updated as the institution's business and regulatory environment changes. The established policies should include goals and objectives and appropriate procedures for meeting those goals and objectives. Generally, the degree of detail or specificity of procedures will vary in accordance with the complexity of the issue or transactions addressed.

The institution's policies and procedures should provide personnel with all the information needed to appropriate use the TMS. This may include applicable regulation cites and definitions, sample forms with instructions, institution policy, and, where appropriate, directions for routing, reviewing, retaining, escalating and disposing of transaction reports. For example, TMS procedures should be established so that personnel consistently complete certain tasks within established regulatory timeframes. These procedures should incorporate and clearly convey to staff the regulatory requirements and the institution's BSA/AML policy, including procedures for aggregating cash transactions, preparing required reports and escalation of possible suspicious activity.

The BSA Compliance Officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance and is also charged with managing all aspects of the BSA/AML compliance program.

The procedures should be as detailed as possible and should be developed and updated as necessary to ensure clarity and completeness as examiners will be using them to evaluate the institution's compliance function.

ON-GOING, RELEVANT TRAINING FOR USERS

The financial institution must ensure that appropriate personnel are trained in the applicable aspects of the TMS. Training should include regulatory requirements and how these are applied through the institution's internal policies, procedures, and processes involving the TMS.

Training should be ongoing and incorporate current developments and changes to the TMS and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems regarding the TMS operation should also be covered during training. The training program should reinforce the importance that the board and senior management place on the institution's compliance with the BSA and ensure that all employees understand their role in maintaining an effective BSA/AML compliance program, including the use of the TMS.

The training programs should be documented by the institution. Training and testing materials, the dates of training sessions, and attendance records should be maintained and be available for examiner review.

INTERNAL MONITORING

Monitoring should be a proactive approach by the institution to identify procedural or training weaknesses in an effort to preclude regulatory violations. Institutions that include a compliance officer in the planning, development, and implementation of TMS increase the likelihood of success of its compliance monitoring function.

An effective internal monitoring system includes regularly scheduled reviews of (a) document filing and retention procedures; (b) identification of all data sources that contain relevant data; (c) validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows; (d) data extraction and loading processes to ensure a complete and accurate transfer of data from its source to the TMS; (e) quality of output reports; and (f) compliance with regulatory timeframes.

Changes to regulations or changes in business operations, products, or services should trigger a review of established TMS processes. Modifications that are necessary should be made expeditiously to minimize compliance risk, and applicable personnel in all affected operating units should be advised of the changes.

Monitoring also includes reviews at the transaction level during the normal, daily activities of employees in applicable operating units of the institution. This might include, for example, verification of the proper identification of a transaction type or the proper aggregation within a customer/account. This review should be conducted before the transaction is completed. Monitoring at this level helps establish management and staff accountability and identifies potential problems in a timely manner.

Internal monitoring should also include the review of employees' performance to ensure that the established internal policies and procedures are being followed. The frequency and volume of employee turnover at an institution should be factored into the review. Such reviews are especially critical after problems have been noted during past audits or examinations, regulation changes, new products are introduced, mergers occur, or when additional branch locations are opened.

INDEPENDENT TESTING

An independent testing or compliance audit is an independent review of an institution's compliance with BSA/AML laws and regulations and adherence to internal policies and procedures. The audit helps management ensure ongoing compliance and identify compliance risk conditions. It complements the institution's internal monitoring system. The Board of the institution should determine the scope of an audit, and the frequency with which audits are conducted.

The scope and frequency of an audit should consider such factors as expertise and experience of various institution personnel; organization and staffing of the compliance function; volume of transactions; complexity of products offered; number and type of branches or business locations; acquisition or opening of additional branches or locations; size of the institution; organizational structure

of the institution; degree to which policies and procedures are defined and detailed in writing; and magnitude/frequency of changes to any of the previous.

Independent testing (audit) could be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, a sound practice is for the institution to conduct independent testing generally every 12 to 18 months, commensurate with its BSA/AML risk profile. A review of the TMS should be part of the institution's overall BSA/AML audit. The persons conducting the independent testing should report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.

The audit should include specific testing for (a) BSA/AML detection scenarios with threshold values and amounts designed to detect potential money laundering or other suspicious or illegal activities; (b) end-to-end, pre-and post-implementation testing of the TMS, including, as relevant, a review of governance, data mapping, transaction coding, detection scenario logic, model validation, data input and program output; (c) documentation that describes the institution's current detection scenarios and the underlying assumptions, parameters, and thresholds; (d) protocols setting forth how alerts generated by the TMS will be investigated, the process for deciding which alerts will result in a filing or other action, the operating areas and individuals responsible for making such a decision, and how the investigative and decision-making process will be documented; and (e) an assessment of the continued relevancy of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.

FUTURE OF TRANSACTION SURVEILLANCE SYSTEMS

The financial environment is constantly changing and progressing. Financial institutions themselves also change over time and as they grow and mature, the information needs will change. At the same time the information systems implemented to support regulatory compliance will also need to change. It is essential, therefore, to review the institution's information needs on a frequent basis to continually to align business operations with changing regulatory needs, particularly in a business environment where everyone faces the impacts of globalization and cyber activities.

GLOBAL RADAR SURVEILLANCE TECHNOLOGY

A CUT ABOVE THE REST

Having potent AML technology software is of the upmost importance for all financial institutions today. Organizations are at a greater risk than ever of a potential breach in their security via the constant, and ever-increasing, threat of financial crime. Is there a simple way that an organization manage to protect their company from these potential risk while trying to manage the countless other operations on a daily basis? Is there also a way that that these processes could run smoothly and in a cost-effective manner?

At Global RADAR we understand the challenges that can emerge from attempting to manage and survey countless transactions, and we also recognize that you as a consumer need quality information and analytical tools in order to support and facilitate the implementation of a high-caliber transaction surveillance system.

Our innovative AML Surveillance module delivers the power to address all of the AML and BSA regulations simply and efficiently, reducing the manpower necessary for these tasks to be completed, all while reducing company compliance costs as a whole. Our module, which can integrate with multiple core and third-party software providers, entails easily customizable software to address the unique requirements of your institution quickly, while sparing no expense in regards to the quality of the program. Once installed, our software allows the user to configure specific alert tolerances based on the transaction(s) being completed, and gives an automatic analysis of the transaction patterns that arise, as well as analysis of individual and group accounts, client portfolios, and all financial relationships that are found within the database of each respective institution.

Aside from these benefits is our distinctive “behavioral profiling” of the transaction activity being analyzed. This incorporates both rules and statistical based methodologies that can be used to detect irregular trends and behavioral patterns within the client profiles, a service that is offered exclusively through Global RADAR. Additionally, this module has the ability to generate an extensive library of reports based on the information being analyzed for management and board reporting requirements, making it less challenging to meet the requirements of the Bank Secrecy Act in a timely fashion. Overall, this comprehensive case management solution allows for the proper documentation of events to facilitate special investigations and the filing of suspicious transaction reports, and is a must have for all financial institutions that want to enhance the efficiency of their compliance department. The results of our analysis will not only expedite the means by which the regulations are met, but also ensure that your company is secure from financial criminals and high risk individuals.

In addition to our AML Surveillance module, Global RADAR offers Trade Surveillance capabilities. Once installed, an institution can track transactions across trading, fraud, anti-money laundering, and business management risk units to streamline investigations, which is accomplished by leveraging sophisticated analytics to ensure investment suitability using both rules and statistical based methodologies, as seen in our AML Surveillance module as well.

Additional benefits of this module include the ability to accelerate account openings and office compliance account reviews, with the information obtained being utilized for cross-selling products and services in real time. Perhaps the most beneficial aspect of this module, and one that sets Global RADAR apart from the competitors, is the simplicity of the program in regards to allowing organizations to better understand their clients’ relationships and increase their organization beyond the traditional system’s capabilities, which has a lasting effect on the coherence of the institution as a whole.

The ability to test the application settings in a staging area before deployment to production is another serviceable aspect of our software, which can reduce error once the program is enabled, effectively saving a business a fair amount of time and money.

This module too has the integration abilities necessary to function with existing core systems independent of their limitations, also limiting the costs and need for potential additional software, and the ability to personalize digital is an added enhancement to a process that was previously paper-based, which still is evident in the product provided by competitors. Moreover, the user-friendly nature of this software allows for it to be accessible to users outside of strictly the compliance/ AML departments, increasing the possibilities for the company to unify and ultimately expand the responsibilities of its workforce wherever they are required, and the comprehensive reporting and dashboard functionality allows managers from virtually any department in the organization to quickly assess the overall effectiveness of brokerage compliance policies and procedures so proactive steps can be taken to quickly identify and resolve issues.

Yet another area by which Global RADAR rises above the competition is in its revolutionary approach to surveillance and management of not only outside individuals, but also employees of each respective financial institution. It is a well-known fact that the most common sources of financial criminal activity come from companies' own employees. We also have you covered in this respect. Through our Employee Surveillance and Management module, Global RADAR provides a high degree of transaction control to help your institution monitor and ensure personal trading compliance. This module includes, but is not limited to, employee onboarding (the mechanism by which new employees acquire the necessary skills and behaviors to become effective organizational members), pre-hire performance review to increasing interviewing accuracy, certifications review, signing of employee attestations for greater overall protection of the enterprise against significant risk, and case management (the ability to manage workloads and digital information) through both reactive tasks and proactive activities involved directly with each case.

Our software also allows for organizations to monitor employee trades for violations, and closely analyzes them to confirm pre-clearance approval is being obtained, which is an essential practice to maintain security in regards to "in-house" activity. This module also helps to quickly identify violations so they can be easily reviewed and escalated, with a comprehensive library of activity reports being maintained in the process in order to facilitate the employee surveillance process. These activity reports can also be recalled from the database readily for review when necessary. As an added bonus, Global RADAR also provides standard certifications to distribute mandatory attestations such as the following:

- "Outside" business activities
- Gifts and entertainment
- Political contributions
- New Employee Forms

STAY IN TOUCH

60 Cannon Street London
England EC4N 6NP
United Kingdom

UK +44 20 8618 2216
US +01 1877 265 7475

email: info@globalradar.com
www.globalradar.com

GLOBAL RADAR®
ASSURING INTEGRITY