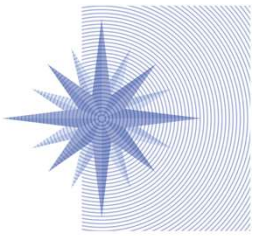

Banco Santander
Bank of America
Barclays
Citigroup
Deutsche Bank
Goldman Sachs
HSBC
JPMorgan Chase
MUFG Bank
Société Générale
Standard Chartered Bank
UBS

the Wolfsberg Group

The Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity

Introduction

The Wolfsberg Group (the Group) published a Statement on Effectiveness in 2019[1] which outlined three clear elements, the Wolfsberg Factors, that a financial institution (FI) should pursue and be measured/examined against:

1. Comply with Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) laws and regulations.
2. Provide highly useful information to relevant government agencies in defined priority areas.
3. Establish a reasonable and risk-based set of controls to mitigate the risks of an FI being used to facilitate illicit activity.

In subsequent publications, the Group described how FIs can develop and demonstrate effectiveness in their AML/CTF programmes.[2] This body of work built on the recognition by the Financial Action Task Force (FATF), in its 2013 revision of the Mutual Evaluation Methodology, that jurisdictions should not focus solely on technical compliance with laws and regulations but evolve actively towards measuring effectiveness and outcomes.

Each FI should develop its own financial crime risk management (FCRM) programme in line with its own business model as determined by its size, scale, footprint, customers, and risk appetite. There is no 'one size fits all' FCRM programme that applies to all FIs and each FI should be supervised accordingly.

This paper seeks to describe how consideration of the Wolfsberg Factors can be translated into a more effective approach to Monitoring for Suspicious Activity (MSA). We have deliberately chosen to characterise this as MSA to cast a wider net than just Transaction Monitoring because customer behaviour and customer attributes, when combined with the consideration of transactions, can provide a broader insight into potentially suspicious activity. Transaction Monitoring is therefore a sub-set of MSA, which might also include concepts such as ongoing Customer Due Diligence (CDD).

[1] The Wolfsberg Group - Statement on Effectiveness (2019)
[2] Ibid – Developing an Effective AML/CTF Programme (2020) and Statement on Demonstrating Effectiveness (2021)

MSA specific terminology has been added in a Glossary at the end of this document. MSA is not limited to customer activity and behaviour attributes but could also encompass employee, vendor, or counterparty activity, albeit this paper focusses on the customer.

As part of their FCRM programmes, FIs monitor for suspicious activity by collecting and analysing information from customers and their transactions to identify what may be suspicious and require reporting to competent authorities. These processes were introduced well over two decades ago and have grown to become one of the more mature and expansive risk and control frameworks producing an ever-increasing number of Suspicious Activity Reports/Suspicious Transaction Reports (SARs/STRs).

The Group does not believe that the value being derived from the (constantly increasing) volume of SARs/STRs is contributing proportionately to effective outcomes in the fight against financial crime. While the concept of effectiveness has been discussed for many years by lawmakers, regulators, supervisors, standard setters as well as the private sector, the Group believes it has yet to be fully integrated into the overall FCRM framework which will require acceptance and alignment across public and private sectors.

To make effectiveness in MSA a more tangible concept, this paper recommends that the industry pivot towards a true risk-based approach (RBA), resulting in both a move away from prescriptive rules-based risk management routines and towards higher-value, quality outputs, thereby enhancing the fight against financial crime.

The Group considers that focusing on the measurement of effectiveness, targeting outputs, harnessing new technology and embracing innovation are the key attributes that are necessary to making a step change in how FIs approach MSA regimes. These aspects, along with several enabling factors, will contribute to greater success in the identification of financial crime.

Targeting and measuring effectiveness and outputs

Managing an MSA programme that has a primary focus on the usefulness of the information it generates, is a significant but necessary paradigm shift which would allow FIs to maximise the production of high-value outputs, which would be highly useful to relevant authorities in clearly defined priority areas.

At present, and largely in response to supervisory expectations, FIs design and implement their MSA programmes with a view to ensuring technical compliance, even when this entails continuing ineffective activities such as:

- Demonstrating expanding red flag and typology coverage across the entire customer and product range, even when an FI's data shows that these result in little to no escalations when performed via systemic monitoring.[3]
- Ensuring that no historical SAR/STR is "left behind," which results in ineffective and over-alerting monitoring programmes.
- Reporting potentially suspicious activity in all cases where red flags and typologies potentially indicative of financial crime have alerted and in which the legitimacy of the underlying transactions could not be fully verified. This has resulted in FIs gradually reducing the threshold for filing a SAR/STR. A 'defensive' SAR/STR filing may eliminate the regulatory risk

[3] The effectiveness of this approach may be further reduced by the fact that illicit actors are able to access red flags and typology papers which are available in the public domain and can adapt their schemes accordingly to go undetected.

for an FI as a result of not filing a SAR/STR but is unlikely to provide useful information to law enforcement.

In line with these expectations, FIs currently measure the effectiveness of their Transaction Monitoring programmes using metrics such as the coverage of potentially relevant red flags and typologies, alert and case volumes, alert productivity, or alert-to-SAR/STR ratios. These metrics are limited in their ability to measure actual effectiveness due to their focus on the quantity, as opposed to the usefulness, of the information provided. Overall, the current approach has resulted in substantial increases in the volumes of SAR/STR filings by FIs globally. Yet, no reliable evidence shows a proportionate increase in highly useful information for relevant government agencies[4] or a material reduction in money laundering and terrorism financing activities.[5]

The Group therefore believes it is necessary to re-define how the effectiveness of an FI's MSA programme is determined and measured. Embracing this material shift would allow FIs to prioritise their MSA efforts better by:

1. Risk-based monitoring of their customers, products, and transactions focused on material typologies and observed risks. FIs should leverage their available data regarding the productivity of certain suspicious activity monitoring routines as well as the demonstrated value of SARs/STRs filed when deciding whether to continue or stop certain suspicious activity monitoring routines.[6] This allows FIs to allocate resources toward mitigating crystallised risk rather than processing and documenting coverage against theoretical risk that has not been observed.
2. Developing and enhancing analytical capabilities to complement risk-based monitoring with targeted, timely data analysis and investigations in line with the operational priorities outlined by the relevant government authorities.
3. Pro-actively conducting holistic risk identification exercises on their business (across all customers, products, channels, and transactions) to identify potential exposure to idiosyncratic risks,[7] as well as trends and emerging threats across the FI's enterprise.

In order to establish a risk-based MSA programme focused on providing highly useful information in line with the three focus areas outlined above, FIs need to understand and align to national priorities (however communicated) with regard to combatting financial crime. While some jurisdictions publish specifically defined national or supra-national priorities, others may rely on more general communications[8] from which priorities can be discerned.

Furthermore, as a true measure of effectiveness, FIs need to understand the value (or otherwise) of the SARs/STRs which they have reported. As previously outlined by the Group,[9] the best indicator of

[4] For example, the German Financial Intelligence Unit (FIU) reported in 2022 that from 337,186 STRs (page 14) only 15.3% (51,700) were forwarded to law enforcement agencies (page 19). Feedback received showed that 95% of cases resulting from the STRs forwarded were closed without prosecution (page 21).

[5] The FATF Report on the State of Effectiveness and Compliance with the FATF Standards notes that only a small fraction of all proceeds of crime is recovered and convictions for money laundering are often not in line with the major risks identified within each country. In 2016, Europol noted that 2.2% of estimated proceeds of crime were provisionally seized or frozen and 1.1% of criminal profits were confiscated at the EU level.

[6] FIs should conduct regular testing against de-scoped MSA routines to confirm the absence of material risk.

[7] Such risks would include undetected, large-scale risks (e.g. laundromats, mirror trading schemes, money mule networks). Using lessons learned from such risks detected in the past and the economic and geo-political factors which have led to these, as well as the results from its annual financial crime risk assessments, FIs would need to develop and execute "stress tests" to identify potential anomalies not identifiable through the ongoing monitoring of individual customer relationships.

[8] Such as advisories or National Risk Assessments.

[9] The Wolfsberg Group (2021) Statement on Demonstrating Effectiveness

the quality and usefulness of SARs/STRs is direct feedback from government authorities.[10] Where such feedback is limited or unavailable, FIs should consider factors like the complexity of the investigation, the identification of network activity, or reporting in identified priority areas, as indicators of quality and, subsequently, the value of their SARs/STRs.

Once FIs can understand the value of the SARs/STRs they have filed and have adjusted their automated monitoring scenarios accordingly, they should adopt additional metrics to understand better, and enhance, the effectiveness of their programmes, subject to local/more prescriptive regulatory requirements. Qualitative and quantitative metrics may include:

- Assessment of false negatives (based on the analysis of SARs/STRs which have resulted from other sources, such as internal referrals from front-line staff), with the aim of potentially covering these through automated MSA.
- Completeness of SAR/STR information (the value of a SAR/STR may increase with additional contextual information).

The Group also encourages FIs to leverage the evaluation of the quality of their SARs/STRs and their understanding of the underlying customers, products, and transactional flows to strengthen their overall FCRM programmes. For example, fully harnessing and understanding the specific risks underlying high value outputs could allow FIs to make certain detective controls preventative thereby preventing the illicit financial flows from occurring.[11]

Innovation

Traditional MSA platforms have reached a point where new technology can significantly improve effectiveness, operational efficiency, as well as compliance with regulatory expectations. Legacy tools have challenges with adapting to the risk of today's financial services sector, which is rapidly expanding cross border transactions, increasing volumes, and executing faster payments.

When changing an AML platform, concerns may arise related to a combination of factors, including increasing technology complexity, using 'black-box' solutions with low explainability, regulatory upskilling and understanding, slow end-user adoption, and weighing the opportunity costs of investment versus effectiveness.

Modern detection frameworks require sophisticated applications and the talent to engineer, develop and maintain them. To support innovation in MSA programmes, FIs, regulators and law enforcement need to understand that innovation is a journey which can take multiple years before benefits can be realised. Investments tend to focus primarily on the analytics used in detection, but other areas are ripe for improvement, such as optimising case management systems, leveraging external data sources, improving control oversight mechanisms, and creating tools to support exploratory analytics.

Focusing Detection on Crystallised Risk

Risk indicators published in guidance materials are based on either theoretical patterns of risk or are generalised statements that may not be translated easily into actionable items. Further to the

[10] National FIUs could, for example, provide FIs feedback on whether SARs were forwarded to law enforcement agencies. The current practice of some national FIUs, which provide overarching feedback across the whole industry is helpful, however, this feedback generally does not provide the specific, structured feedback which FIs require to focus their specific SAR/STR filing patterns on those areas considered to be of high(er) value.

[11] For example, FIs may find that their automated MSA results in high-value outputs when detecting and reporting transactions involving shell companies registered in specific jurisdictions. In such cases, the FI could establish a preventative control to block such transactions from being executed, until reviewed and considered legitimate.

statement above on effectiveness, to make financial crime detection better, FIs should prioritise optimising and refining their systems for observed or crystallised risk, while coverage of theoretical risk can be handled using an RBA inclusive of exploratory analytics.

Unlike traditional rule-based models which can be mapped to red flags and typologies, the use of Machine Learning (ML) models is more challenging as these systems are designed to make predictions across large data sets covering a wide variety of risks. FIs will need to document clearly and analyse ML models against the crystallised outcomes of detection to demonstrate how these solutions can continue to mitigate financial crime risk.

FIs should also consider incorporating information from case investigations and SAR/STR filings or other useful data, back into MSA platforms e.g. leveraging technology to extract information from case narratives to identify emerging risk patterns. The information can then be used to inform detection of future suspicious patterns, elevate the risk score of suspicious entities and identify previously unknown relationships.

It is important to define and choose the right success criteria when deploying new systems. FIs should look for opportunities to define and prioritise high value outcomes that go beyond just SARs/STRs, as the risk threshold to file will vary depending on a number of factors. For example, there may be instances where a risk is identified, but local regulations or FIU procedures do not require filing a SAR/STR unless materially new evidence is discovered.

Approach to Data

A successful evolution towards a more effective MSA programme involves the adoption of open-source applications that enable FIs to pick the underlying technologies that best suit their business model and risk appetite. Like Lego blocks, these components enable each FI to build a programme that is responsive to their needs. The use of Cloud technology, while not essential, is an accelerator towards higher-performing application execution and scalable, cost-efficient data storage, enabling faster responses to business and regulatory needs.

Input data for MSA platforms should incorporate not only transactional data, customer static data and internal reference lists, but also other dynamic behavioural customer information where proportionate to the risk (e.g. device ID, IP addresses). Using an RBA, input data may also include data from reputable external, publicly available sources, including information on company structures, Ultimate Beneficial Owners (UBO), and watch lists, as well as complementary sources such as market data and verified customer social media accounts. Finally, FIs should establish robust data governance and quality control frameworks.

Entity resolution and graph networks have increasingly become an important part of MSA platforms i.e. linking internal customer, account, transaction and external data to provide a network-based contextual view of a customer. FIs should consider building risk profiles for key entities (e.g. customers, underlying customers, UBOs, and other entities) leveraging both internal data and external data from reputable third-party providers beyond customers and/or focal entities being monitored. The MSA platform may be enhanced to enable context and comprehensive customer behaviour analysis which could expedite risk management decisions. Better technology will enable FIs to accelerate towards more effective and risk-based identification of financial crime risk.

FIs can consider advanced and dynamic segmentation to identify patterns in behaviour in lower-level segments, improving the performance and accuracy of detection models and reducing false positives. Traditional segments typically include static factors such as customer type, industry, type of business,

and inherent customer risk. Drawbacks to this approach are that these segments do not capture common transaction activity among the segmented entities consistently and rely mainly on outdated information or the static information gathered during customer on-boarding and refreshed during periodic, event-driven, or perpetual review processes.

Better solutions should monitor and analyse transactions, patterns of activities and create new, more accurate and meaningful segments on an ongoing basis. A combination of known attributes and a dynamic statistical clustering could lead to more meaningful segmentation that can account for changes in customer activity and keep segments up to date.[12] [13]

Data visualisation, advanced analytics, and research

FIs should employ robust resilience controls when collating data and once sourced it may be made available to all key stakeholders via a unified self-service framework incorporating visual dashboards with collaborative workflows. Consideration should be given to the use of visual data discovery tools to highlight connections, patterns of money transfers, and the entities involved. Availability of such self-service tools will allow a more robust and faster response to data-related audit and regulatory enquiries, and reduced technology efforts related to the provisioning of data.

FIs should consider building data environments to research and test new risk patterns and 'what-if' scenarios, conduct complex investigations, and evaluate new rules/scenarios to cover for emerging risks (e.g. evolving geo-political issues, pandemic loan/loan guarantees, cyber-enabled fraud).

FCRM programmes should actively research and test for new typologies and patterns. Below-the-line reviews are one method to allow for the testing of entirely new challenger models that are still in experimentation phase to gather feedback and improve detection. Today, for false negative testing, only minor adjustments to current model parameters are made in the controls by incrementally dropping the existing model's detection thresholds (e.g. 10% below the current value). Minor modifications to existing parameters are unlikely to produce meaningful results that will materially increase overall the effectiveness of detection.

Machine Learning

A recent industry trend in FCRM is the use of Machine Learning (ML) capabilities to reduce inefficiencies as well as improve effectiveness. This technology can be developed within the FI or run as a service. Traditional ML techniques, such as supervised or unsupervised algorithms, are well established and used across a variety of industries. While there is a growing interest in other advanced areas of Artificial Intelligence (AI), such as Generative AI (GenAI) and Large Language Models (LLMs) in FCRM, these technologies are in their infancy and their application will require more research and validation and will need to align to an FI's AI conduct principles such that bias and explainability are managed through governance[14].

ML algorithms may be used as booster models to augment a rules-based system, or, in some cases, be used as the primary detection tool itself. Beyond detection use cases, ML capabilities can be applied in other areas of MSA, such as providing secondary name screening to reduce false positives or auto-

[12] For example, applying k-means or Jenks.
[13] Further efficiency could be gained by enabling data exchange between the periodic/perpetual CDD review and the MSA control, i.e. detailed investigation of a client from a MSA alert could be the reason to postpone a periodic CDD or a recent CDD review might be used as an alert de-prioritisation consideration.
[14] The Wolfsberg Group, Principles for Using Artificial Intelligence and Machine Learning in Financial Crime Compliance

populate case management systems with additional information to expedite and streamline investigations.

Some ML methods, e.g. supervised ML, depend on the identification of historical outcomes, or targets, to train the model during development. In MSA, this may include historic SARs/STRs resulting from automated monitoring processes; however, ML systems will benefit from being trained on a variety of crystallised risks from multiple sources, including manually generated cases and law enforcement production orders, as these may help the model predict new risks that were not considered or identified in prior legacy systems. If SAR/STR data is included, ML based MSA systems need to strike a balance: catch as many known risks (recall) while being accurate (precision). Sacrificing some past cases may help predict higher value outputs in the future. Aiming for 100% recall, or 'No SAR/STR left behind', is likely to lead to an ineffective system.

Risk typologies can be distilled into a set of individual statistical features that can be shared across existing or new typologies. Such feature sets are enhanced using feedback during testing, applying feature engineering techniques, as well as involving subject matter experts. An opportunity for Public-Private Partnerships (PPPs) could be defining and sharing a standard baseline feature set for those features that prove influential in detecting financial crime, without sharing any sensitive information.

Enabling Factors

Systemic evolution of the AML/CTF regime cannot occur until all parties foster an environment that encourages innovation. While FIs should continue to enhance effectiveness, there are certain enabling factors which are incumbent on other parties in the financial crime prevention ecosystem that will enhance an RBA. In addition, laws and regulations have the most potential to enable FIs to focus on an RBA and implement the Wolfsberg Factors. All parties need to prioritise feedback between themselves and continually push for enhancements in information sharing between national FIUs, law enforcement and FIs. This would also allow for innovation and targeted, risk-based MSA.

Legal and regulatory change

In order to remove unnecessary barriers to innovation, the industry should adopt regulatory statements on innovation in their risk-based approach, while streamlining overhead requirements or expectations, such as model risk management or no SAR/STR left behind. While some jurisdictions have endeavoured to provide targeted AML guidance for model risk,[15] the pace at which FIs adjust their model governance and oversight approach to be nimbler remains slow out of concern of running afoul of the current regulatory environment.

While risk appetite for missed SARs/STRs has also increased in recent years when FIs are designing and developing innovative solutions, regulators should promote collaboration, embrace concepts like sandbox development, reject the concept of parallel processing in the transition of monitoring capabilities, and emphasise information sharing.

Until this occurs, FIs will be hampered in how they deploy resources and identify suspicious activities, too often focussing on avoiding regulatory infractions as opposed to identifying and mitigating financial crime risk; this is not simply an issue for FIs as ever higher volumes of SARs/STRs can exceed the capacity for FIUs and law enforcement to analyse and process them.

Crystallised Risk from feedback and information sharing

[15] For example, the U.S. published an "Interagency Statement on Model Risk Management" in 2021.

Receiving intelligence or feedback from national FIUs, directly from law enforcement, or through PPPs can significantly impact the FI's ability to understand if their monitoring programmes are effective. Forward-thinking data sharing regulations can facilitate this knowledge transfer in a way that protects both individuals and enterprises e.g. using anonymisation technologies. Proactive sharing of intelligence by law enforcement can provide FIs with clarity on what typologies are most used by criminals, what networks FIUs or law enforcement are tracking, ultimately allowing FIs to align resources better with national priorities.

Feedback on completed investigations, such as confirmed activities, or additional clarity on typologies, would provide FIs with the ability to refine monitoring programmes. Such feedback can create a virtuous circle of better outputs from FIs leading to more actionable intelligence for FIUs and law enforcement and more successful legal action against illicit actors which, in turn, should reduce the amount of financial crime in society. Initiating more progressive public-private and cross-jurisdictional information sharing noted above, even in the form of pilot programmes, would significantly enhance the industry's ability to evolve the MSA approach.

Conclusion

After many years of focusing on technical compliance, managing false negative cases and a steadily growing number of SARs/STRs that do not always appear to add value to the fight against financial crime, the Group encourages all parties across the MSA lifecycle to be proactive in the development of innovative techniques and supporting technologies. Such approaches can strengthen FCRM programmes by delivering effective end-to end risk detection capabilities that maximise the utility of critical risk management resources.

Existing MSA methods are inefficient and ineffective at producing timely outcomes that are useful to law enforcement. As a result, the time has come for government agencies to partner more closely with FIs as part of the SAR/STR filing process. The need for a new approach is further necessitated by the fast-changing threat landscape across new communication and transaction channels.

An enhanced approach combined with the use of emerging technologies presents an opportunity for FIs to work in partnership with law enforcement and supervisors to improve detection capabilities, reduce adverse customer impact, provide more highly useful information to relevant government agencies about crime, and for those agencies to increase their ability to act against the criminals. Increasing the proportion of SARs/STRs that are viewed by relevant government agencies as highly useful offers the benefit of making a greater impact on criminals and their illicit activity and reducing much of the inefficiency and customer friction represented by low value reporting that may rarely or never be used by those agencies and yet which may need to be analysed by them.

Considering the increasing use of Machine Learning or other technological enhancements, regulators and law enforcement should provide appropriate guidance on the implementation and validation of these technologies. Furthermore, there is an opportunity for PPPs to define a standard baseline feature set that have historically proven influential in detecting financial crime, without sharing any sensitive information.

However, the Group believes strongly that the explicit focus on the provision of more highly useful information to relevant government agencies, and feedback from them on the information provided, will yield dividends in the form of more effective measures being taken against criminals and their illicit activity.

Glossary

Above the Line Testing (ATL): Involves evaluating the parameters by raising them above the baseline. This helps identify the threshold at which false positives might increase, potentially overwhelming investigators with non-suspicious alerts.

Accuracy: Overall proportion of correct predictions across all classes.

Artificial Intelligence (AI): The ability of a computer or computer-controlled robot to perform tasks commonly associated with intelligent beings, such as reasoning, discovering meaning, generalising, or learning from past experience.

Below-the-line Testing (BTL): Involves conducting tests by lowering the thresholds or criteria below the baseline. This helps identify the point at which the system may generate false negatives, potentially missing potentially suspicious activity.

Bias: Unintentional prejudice in data or algorithms, leading to unfair outcomes.

Champion-Challenger: Allows different approaches to be tested by deploying multiple models simultaneously. The current deployed model, known as the Champion, competes with other models, called Challengers, which may be retrained versions of the Champion or entirely new ones.

Classification: Predicting discrete categories (e.g. fraudulent/legitimate transaction).

Crystallised Risk: Realised risk events, i.e. risk events that have occurred rather than those that are theoretical.

Customer Due Diligence: As set out by FATF in Recommendation 10 (see FATF Recommendations)

Entity Resolution: Entity resolution in compliance links data fragments (people, companies, transactions) that refer to the same real-world entity, boosting accuracy, uncovering hidden risks, and saving time in reporting and investigations.

Explainability and Explainable AI (XAI): The ability to understand how a model arrived at its predictions. XAI refers to the development and use of machine learning models that are understandable and transparent to humans. Many AI systems, particularly those using complex algorithms like deep neural networks, can be seen as "black boxes" where the internal workings and reasoning behind their outputs are unclear.

False Negative: An instance incorrectly classified as negative.

False Positive: An instance incorrectly classified as positive.

Feature Engineering: Transforming raw data into features suitable for machine learning models.

Generative AI: Algorithms that create new content based on existing data.

Graph Scripting: Programming paradigm where scripts interact with graph-based data structures. These scripts enable manipulating, analysing, and visualising the relationships and interconnectedness within the graph data.

Jenks Optimisation: Also known as the Jenks natural breaks classification method, a data clustering technique that aims to determine the best arrangement of values into different classes.

Large Language Model: An advanced computer program capable of understanding and generating human-like text by learning from vast amounts of written language data.

K-Means Clustering: Unsupervised machine learning technique that partitions data points into distinct clusters based on their similarity, aiming to minimise the variance within each cluster while maximising the dissimilarity between clusters.

Machine Learning: A subfield of artificial intelligence (AI) that uses algorithms trained on data sets to create self-learning models capable of predicting outcomes and classifying information without human intervention.

Model: A representation of information learned from data that can be used to make predictions.

Monitoring for Suspicious Activity: Various control elements that identify the risk of a customer behaviour.

Natural Language Processing (NLP): Techniques for computers to understand and process human language.

Overfitting: When a model memorises training data too well and performs poorly on new data.

Parallel Run: Running both the existing and new systems simultaneously during transition.

Precision: Proportion of positive predictions that are actually positive (True Positive).

Recall: Proportion of actual positive (True Positive) cases correctly identified by the model.

Regression: Predicting continuous values (e.g. credit score).

Sensitivity Testing: Assessing how robust a model's conclusions are to variations in its inputs and assumptions, ensuring confidence in the results and accounting for potential limitations. Sensitivity analysis helps assess the appropriateness of a specific model specification.

Supervised Learning: Uses labelled data to train algorithms to make predictions or classifications.

Transaction Monitoring: The automated or manual process of monitoring transactions after their execution in order to identify unusual transactions, including monitoring single transactions as well as transaction flows, for subsequent review and, where appropriate, reporting to the authorities.

True Negative: An instance correctly classified as negative.

True Positive: An instance correctly classified as positive.

Unsupervised Learning: Learning from unlabelled data where the model identifies patterns on its own.