FIAU

Guidance Note:

A Look Through the Obligation of Transaction Monitoring

Issued: April 2023

Introduction

Subject persons (SPs) have a number of obligations under the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR), including the obligation to carry out on-going monitoring. A main aspect of on-going monitoring is that of scrutinising unusual, anomalous and suspicious transactions detected through the systemic and continuous review of customers' transactions. When properly executed, transaction monitoring allows SPs to single out transactions that are to be reported to the Financial Intelligence Analysis Unit (FIAU), and enables them to gain deeper insights into their customers' activities, transactional patterns and behaviour. The ultimate goal remains that of minimising the risk of illicit funds entering the Maltese economy, thus safeguarding the integrity and stability of the financial system.

While all SPs have a critical role to play in the fight against financial crime, this guidance paper focuses on the transaction monitoring requirements pertaining to institutions which process payments and similar transactions for and behalf of customers, including but not limited to, banks and other depository institutions, electronic money (e-money) institutions, payment service providers (PSPs) and merchant acquiring companies. This document provides an overview of the statutory requirements that these institutions must fulfil from a transaction monitoring perspective, and describes the optimal transaction monitoring measures and systems that such institutions should strive towards implementing in order to meet their legal obligations. The FIAU recognises that in recent years, SPs have become more sensitive to their transaction monitoring obligations, and also acknowledges the considerable investments made by them to enhance their monitoring systems and controls. However, this document has been issued to offer more comprehensive and practical guidance, as well as address any misconceptions.

In an effort to enhance understanding and provide additional insight into the FIAU's expectations vis-à-vis transaction monitoring, this guidance paper also includes common transaction monitoring related findings and observations noted during the enforcement and follow-up processes, as well as any key takeaways that emerged therefrom. By analysing the root causes of these findings, identifying areas for improvement and suggesting best practices, this document should help institutions which process payments and similar transactions for and behalf of customers to enhance their AML/CFT compliance programmes, thereby improving their ability to prevent financial crime, as well as detect and report suspicious activity.

Characteristics of an Effective Transaction Monitoring Programme

Throughout this guidance paper, the key elements on which effective transaction monitoring is predicated are explored and discussed in detail. The following is a non-exhaustive list of the core characteristics of an effective transaction monitoring programme which feature within this document:

Key Takeaways
Knowing and understanding your customers – establishing the customers' business and risk profiles, as well as updating such profiles on a risk sensitive basis.
Adequately monitoring and scrutinising all transactions that appear to be unusual, suspicious or diverge from the customers' business and risk profiles, which includes requesting further supporting information and/or documentation to justify the rationale behind certain transactions.
Implementing appropriate and tailored transaction monitoring systems which take into consideration the products/services offered, transactions executed on a daily basis and the customer base.
Establishing a set of properly defined detection rules (risk scenarios, thresholds and parameters) which are tested and fine-tuned on a regular basis.
Having in place a robust process for the notification and handling of alerts that minimises the likelihood of false positives being generated.
Ensuring that if there are reasonable grounds to suspect ML/FT, the transaction/activity is reported to the FIAU without undue delay.
Ascertaining that the transaction monitoring programme has sufficient resources, which includes personnel, technology and infrastructure, to support effective transaction monitoring.

Legal Obligation for Transaction Monitoring

The obligation for SPs to scrutinise transactions arises from Regulation 7(2)(a) of the PMLFTR, which stipulates that as part of the on-going monitoring process, SPs must use the knowledge obtained on their customers to adequately scrutinise the transactions affected throughout the course of the business relationships to ensure that these are in line with what the SP knows about the particular customer. The end purpose remains that of identifying any unusual or suspicious transactions. Therefore, transaction monitoring is an indispensable measure that enables SPs to detect behaviour or transactions that are not in line with the customer's business or risk profile, or otherwise diverge from the expected or known transactional pattern. It is vital that SPs take the necessary measures to understand the background and purpose of these transactions, and ensure that a reasonable explanation for such transactions exists.

Scrutinising transactions can be seen as a 'bridging' obligation as it entails the effective use by SPs of the information and documentation collected when establishing a business relationship to mainly meet their reporting obligations. The business and risk profile of the customer sets the baseline against which any transactional activity is to be considered.

A transaction, or pattern of transactions, that falls outside the SP's expectations should serve as a red flag or trigger event for the SP to assess the situation and determine whether it needs to delve deeper into the customer and its activities through the collection and consideration of further information and/or documentation, including information in relation to the purpose and intended nature of the business relationship. For this purpose, the SP may need to collect (additional) information/documentation regarding the following: (a.) the customer's source of wealth (SOW) and the source of funds (SOF) of the specific transaction(s); (b.) any new operational activities; (c.) any significant relevant changes relating to the customer; and (d.) any other information that the SP deems reasonably necessary to be satisfied that the funds are derived from legitimate sources and/or that the purpose of the transaction is a legitimate one. The PMLFTR also set out particular transactions that should inevitably be the subject of scrutiny by SPs. Regulation 11(9) obliges SPs to examine the purpose and background of all transactions that are complex, unusually large, conducted in an unusual pattern, and have no apparent economic or lawful purpose. The reason for this is that these types of transactions are, by their very nature, unusual.

Where it transpires that these transactions are indeed legitimate, and any change in customer activity is justified, the SP may need to update the customer risk assessment (CRA) and adjust the customer due diligence (CDD) and on-going monitoring measures being applied to the particular client. On the other hand, where on the transaction scrutiny undertaken, the SP knows, suspects or has reasonable grounds to suspect that one or more transactions are suspicious and may be connected to money laundering or the funding of terrorism (ML/FT), or to the proceeds of criminal activity, a Suspicious Transaction Report (STR) will need to be promptly filed with the FIAU in terms of Regulation 15(3) of the PMLFTR.

Execution of Transaction Monitoring

How to Ensure Effective Monitoring of Transactions

For transaction monitoring to be effective, SPs need to have a comprehensive understanding of their customers' risk profiles and business activities. Therefore, before entering into business relationships or carrying out occasional transactions, SPs must carry out the necessary CDD checks and establish the level of ML/FT risk posed by their prospective customers by conducting a CRA. Once such understanding is formulated, the SP will be able to determine the degree and nature of transaction monitoring checks to be performed for customers with different levels of ML/FT risk. To this end, it is key that SPs adapt their transaction monitoring approach depending on the customer type and risk profile, as well as the products/services offered.

At times, SPs do detect the right transactions they should be asking questions about but then fail to sufficiently understand the rationale behind the same, leading to the improper scrutiny of transactions. Lack of adequate transaction scrutiny may adversely impact the detection of unusual and suspicious activity, as well as render SPs unable to keep a comprehensive business and risk profile on its customers. Moreover, if the SP's ability to carry out effective transaction monitoring is impaired, this allows for the risks of the customers to be unmanaged for a considerable period of time and for transactions to be processed without there being the necessary mitigating controls in place.

Some examples of when SPs failed to adequately scrutinise transactions in line with their AML/CFT obligations are being relayed below:

- *Example 1*: There were instances where SPs allowed unusual or suspicious transactions to be executed without properly scrutinising the same, not even as a part of a retrospective transaction monitoring exercise. In doing so, the SPs failed to ensure that the transactions undertaken were consistent with their knowledge of the customer and of his/her business and risk profile. During a compliance examination on an institution, it was observed that the customer held a corporate account to which a substantial number of sub-accounts were linked. The activity through such accounts, particularly, incoming transfers followed by immediate identical cash withdrawals from an ATM, was deemed to be suspicious, and not customary to what would have been expected from a company involved in marketing consultancy. In total, the customer received incoming payments amounting to circa €250,000, which funds were subsequently withdrawn almost in their entirety through a series of hundreds of ATM withdrawals, each amounting to less than €5,000. The SP neither queried the purpose for the receipt of the payments, nor the dubious ATM withdrawals that happened within the same period of time. The SP also failed to obtain an understanding as to why a marketing consultancy company was receiving funds and immediately withdrawing them.

- *Example 2*: SPs did not always take into consideration the customer's specific ML/FT risks, and other important factors such as the customer type, industry type, geographical area of exposure and account turnover. For some business relationships, discrepancies between the transactional activity and information held by SPs vis-à-vis the customers' profiles were also observed. The main cause for such discrepancies was the fact that the particular SPs' transaction monitoring systems only considered recent activity, and failed to monitor transactions based on the expected customer activity declared at onboarding. In the case of one specific customer that held an account with an SP, although the expected monthly turnover was approximately €15,000, the total amount credited to the customer's account during a particular month was more than ten times the expected monthly turnover, with over €100,000 being credited in just one day. However, given that the transaction monitoring thresholds in place were not violated, no alert had been generated for this transaction. The SP also submitted that as per revised KYC information obtained, the customer's projected annual turnover was substantially increased to circa €700,000. However, no documentary evidence was held on file to support the increase from €15,000 to €700,000. Should supporting documentation on the customer's change in expected activity have been obtained, the sudden deposit spikes may have been justified.

- *Example 3*: There were also some SPs that failed to thoroughly scrutinise transactions that were unusually large, anomalous, dubious or suspicious, allowing such transactions to pass through the customers' accounts undetected. In certain cases, the transactions affected were extremely large, with single payments at times even exceeding €5 million, while in other cases, the transactions diverged from their customers' business and risk profile. SPs neither questioned the voluminous amounts being transacted, nor attempted to obtain further supporting information and/or documentation to ensure that the payments made economic and lawful sense.

- *Example 4*: Other isolated cases where SPs executed their customers' transactions without duly scrutinising them include the following:
  - Internal transfers between own accounts or corporate customers owned by the same beneficial owners – In the case of one particular SP, all transactions carried out between two customers were cleared out as internal transfers, and the SP either did not obtain any explanations and/or supporting documentation, or else, when invoices were obtained, these at time did not match the value of money that was being transferred and were generic or lacking in detail. Over a period of one and a half years, close to €6 million were transferred from one customer to another without obtaining the relevant information and/or documentation to substantiate the rationale behind the payments. It was further observed that when the SP eventually started to request documentary evidence, the transactions between these customers drastically decreased, both in terms of value and volume, which is another red flag.
  - Payments from one party to another that were backed-up by questionable, suspicious or vague loan agreements and invoices.
    - In one case, it was noted that the customer received nine payments totalling nearly €2 million from another customer of the over a period of three years. A loan agreement between the SP's customers was obtained; however, such agreement was dated six months after two out of the nine payments had already been received. Hence, it was unclear on which basis these initial two payments were made. Moreover, the loan agreement provided lacked the necessary details to facilitate the understanding of the rationale behind the loan, simply stipulating that the purpose of the loan is to "supporting the company, its subsidiary and group companies with all costs, liabilities and investment advances", which was considered as being too vague and does not explain why such a high value loan was required.
    - In another unrelated case, it was observed that invoices pertaining to a customer operating within the textiles industry simply included a general description of the purpose for the payments request (e.g. "textiles" or "fabrics") and amount due, without detailing the type of textiles/fabrics involved and prices per type, which are typically expected to be delineated in an invoice for the sale of goods. This raised doubts regarding the reliability and authenticity of the invoices provided to support the payments made. To compound matters further, the sums transacted did not completely match the payments envisaged within such invoices.

- *Example 5*: The customer deposited over €100,000 in cash on the same day by affecting a total of six distinct transactions through the same channel. Based on the information and documentation available to the credit/financial institution, these transactions were not reflective of the customer's profile. The customer's gross salary had started off as being slightly above €1,000 a month, and only gradually increased to approximately €3,000 a month after many years of working experience. It was also noted that the pattern and value of the transactions undertaken were significantly above the average value of other transactions passing through the customer's account. In fact, the anticipated level of annual deposits declared by the customer in a CDD form that was submitted was only circa €20,000. When asked about the amounts so deposited, the customer explained that the funds comprised of savings held at home, and provided supporting documentation such as the employment contract and payslips. However, the documentation provided did not sufficiently substantiate the cash transactions executed by the customer because they were not consistent with the customer's profile and expected transactional activity. Prior to this spike in cash deposits, the total value of both cash transactions executed by the customer on the same day only slightly exceeded the €10,000 figure. In this situation, given that the deposits made were not proportionate to the customer's employment income and anticipated level of annual deposits, the SP was expected to further question the deposit spike, and if necessary, request additional explanations and/or supporting documentation to justify the rationale behind these transactions.

- *Example 6*: At the onboarding stage, the corporate customer had declared that its main activity consisted in the buying and selling of vessels. However, it transpired that the customer was also involved in extending financing to a third party, which activity was not congruent with what the institution knew about the customer. In total, the customer lent the third party roughly $700,000 through five separate loan agreements. Although the SP obtained the loan agreements in question, these only covered the terms of the loans, and did not make any reference to the actual purpose behind such loans. As part of the transaction scrutiny process, the SP should have queried why the customer was providing such financing when it was not in line with the customer's known activities and why the loans had been structured in such a manner (five loans of a smaller value) rather than granting one single loan. The explanations provided would have allowed the SP to determine whether these transactions, which were completely outside of the customer's profile, were legitimate or otherwise, and what additional steps needed to be taken.

- *Example 7*: To mitigate the exposure from incoming payments, one of the controls implemented by a certain SP was requesting payment allocation details, as well as a bank credit advice statements bearing the name of the customer and specifying the payment amount. However, several shortcomings pertaining to such process were found. Notably, it was concluded that this control was inadequate to provide the required comfort to establish, on a risk sensitive basis, the SOF for incoming settlement payments that were made through the SP's interrelated company incorporated overseas. This is due to the fact that simply obtaining a credit advice is not sufficient to confirm that the incoming funds originated from non-illicit activities. Further to this, the SP was unable, in some instances, to furnish the credit advice statements that it claimed to have collected. This raises further concerns regarding the effectiveness and consistent application of the control.

As demonstrated above, if the SP detects any transactions that are unusual, inconsistent with the customer's profile or significantly differ what is usually carried out or requested by the customer, the SP must, on a risk sensitive basis, obtain adequate supporting information and/or documentation to substantiate such transactions and ensure that their rationale is justified. If a transaction is flagged for scrutiny, this does not necessarily mean that such transaction is indicative of possible ML/FT and needs to be reported. However, even legitimate transactions may trigger a review and possible update of the customer profile if there is a change in the customer's activity. In this case, the risks posed by the customer may need to re-assessed, with any changes in risk rating being reflected in the CRA.

SPs are required to obtain an understanding of the transactions executed by their customers in line with the risk these transactions present, including the rationale behind the purpose of such transactions. To this end, SPs are expected to collect the necessary supporting information and/or documentation to support the transactions in question, as well as ensure that these transactions were affected for legitimate purposes. In this respect, it is important to reiterate that if a SP exercises reliance on another SP, the obligation to carry out ongoing monitoring on the business relationships remains the former SP's responsibility, which includes obtaining sufficient information and/or documentation to justify the transactions that took place. Simply being satisfied with knowing

the flow of the funds is not sufficient; therefore, SPs must also acquire the necessary documentary evidence to understand the source of the incoming funds.

To determine whether an unusual transaction can be reasonably explained, SPs should obtain supporting information and/or documentation which provides evidence that there is a legitimate reason for the transaction. Examples of information and/or documentation that could be requested include: (a.) the SOF of the transactions involved; (b.) any new operational activities; and (c.) any significant changes relating to the customer.

The following are some examples of when SPs failed to obtain adequate supporting information and/or documentation to justify and substantiate the transactions affected by their customers:

- *Example 8*: Several transactions processed by various SPs were identified for which no or insufficient information/documentation was held on file, despite the presence of certain higher risk factors that should have warranted a review. These include the following:
    - Not scrutinising incoming transactions even though the transacting part had been named in several adverse media reports;
    - Not scrutinising transactions on the basis that the customer was itself a SP; and
    - Not adequately scrutinising a transaction involving a repayment of a shareholders' loan by failing to understand the purpose behind the loan and collect the relevant supporting documentation such as a copy of the loan agreement.

- *Example 9*: For a number of SPs, although supporting documentation was requested and duly collected, this was not satisfactory, and did not explain the transaction being reviewed. Cases were also noted where the supporting documentation obtained in relation to particular alerted transactions were not specifically related to such transactions. This means that these transactions were validated on the basis of inappropriate documentation.
    - In the case of one specific SP, the supporting information/documentation held was collected due to be required for the conduct of business, and not for transaction monitoring purposes. In fact, the documents submitted merely comprised of customers' instructions and invoices needed to process payments or offer services, and could not be used to confirm the purpose of the transactions.
    - Another SP operating as a merchant acquiring company was found to have failed to enquire regarding account-related activity that casted doubts on the viability of the merchants' operations. For certain merchants, the ratio of declined transactions exponentially exceeded the ratio of processed transactions, bringing into question the viability and legitimacy of the respective merchants' operations. The SP considered these ratios as being normal in relation to the services provided by the merchants but did not justify why this is the case.
    - In a third example, the SP failed to question and scrutinise certain generic statements made by its customers to determine the true purpose behind the funds being remitted. Instead, the SP placed reliance on the customers' explanations, such as remittance of funds to support "friends" and "family", without requesting further supporting information and/or documentation to corroborate these claims.

As envisaged under Regulation 11(9) of the PMLFTR, the presence of any unusually large transactions is a trigger for further scrutiny and review. The following is an example of when an SP failed to sufficiently monitor large value transactions that were repetitive in nature:

- *Example 10*: The FIAU identified shortcomings in relation to a total of 19 transactions processed by the institution ranging between approximately €50,000 and €1 million. For 15 out of the 19 transactions, the institution emphasised that these comprised of inter-company transfers between companies within the same group, and that such transfers are not normally flagged since they frequently relate to liquidity management purposes. The explanation provided was not deemed satisfactory because the SP was expected to obtain an understanding of the purpose behind the repetitive transactions being affected. Simply clearing off these repetitive and high value transactions as internal transfers between companies forming part of the same group is not sufficient, even if they frequently relate to the treasury transactions for liquidity management, this since the rationale and legitimacy of these transfers also need to be ascertained. For the remaining four

transactions, the SP provided an extract detailing the transaction data. While such documentation explained the flow of the funds, the source and rationale of the same was not indicated.

In situations where the transactions affected by the customer are of a similar nature and thus have analogous risks, the SP may decide, depending on the ML/FT risk level posed by such customer, not to monitor every single transaction involved, but rather, analyse those transactions that appear to be unusual, suspicious or otherwise not in alignment with the customer's expected level of transactional activity. Consequently, if on a day-to-day basis, the customer affects similar and possibly related transactions, some of which are subsequently alerted by the transaction monitoring system, the SP may opt to focus on those transactions that appear to be atypical or outliers, without reviewing all transactions involved. In order to obtain an understanding of, and justify the rationale behind, transactions of a similar nature, the SP may also rely on supporting information/documentation collected for previously executed transactions which are akin to the ones in question.

Transaction Monitoring Systems

Transaction scrutiny is unlikely to be effective unless the SP has some form of process in place through which it is to detect unusual or suspicious transactions, seek to understand their rationale and determine what is the correct measures to take. It is for this reason that SPs are expected to have the necessary system in place to effectively monitor transactions and identify any unusual or suspicious activity for further processing. On this point, it is important to note that when referring to monitoring measures, reference is made to the totality of the processes in place used to detect, understand, and, where necessary, escalate and report transactions.

When determining the type of transaction monitoring systems to be implemented, the SP needs to first consider the nature of the products and services it offers, and whether it establishes business relationships with its customers, carries out occasional transactions, or a combination of both.

It is important to note that it is not a legal requirement for transaction monitoring to be automated. In fact, the degree to which monitoring is to be carried out manually or through automated processes depends on a variety of factors, which include the following:

- The size of the SP's set-up;
- The complexity of the SP's business model;
- The risk appetite of the SP; and
- The number of transactions executed on a daily basis.

Thus, if the SP has a significant customer base and processes a substantial number of transactions on a daily basis, there is the expectation that significant elements of the monitoring measures be automated so as to manage the increased volume and velocity of transactions. Automation would especially be expected with regard to the detection of unusual transactions as the SP cannot solely rely on manual transaction monitoring. Doing so creates inefficiencies in the process and may result in certain unusual, anomalous or suspicious transactions going by undetected, exposing the SP to a higher level of ML/FT risk. While smaller SPs may opt for transaction monitoring measures that are less automated, the decision for employing a manual measure needs to be duly substantiated. Furthermore, if the SP decides to implement a wholly manual transaction monitoring system, it is crucial that such system is properly administered to ensure that the risks arising from daily transactional activities are addressed.

- *Example*: During a compliance examination on an institution, it was noted that it was carrying out transaction monitoring entirely on a manual basis. The SP's transaction monitoring process involved analysing transactions one by one, and flagging any unusual or suspicious transactions to the MLRO for further analysis. When taking into consideration the SP's number of customers, transactions processed on a daily basis (approximately 30 a day), and the compliance staff complement involved in scrutinising the transactions, it was concluded that the monitoring system was sufficient for the SP to adequately satisfy its transaction monitoring obligations. Nonetheless, if the SP continued to grow and delve into other markets

and industries, it would become humanly impossible for the SP to keep performing manual transaction monitoring. As a result, the SP would then need to enhance its transaction monitoring systems, and introduce an element of automation to its operations.

How to Best Implement Detection Rules

The transaction monitoring system adopted by the SP should be based on a set of risk-based detection rules established according to the SP's business model, customer base, transaction channels and historic transaction activity. In practical terms, detection rules comprise of applied risk scenarios, thresholds and other parameters against which the customers' transactions are analysed. SPs should be mindful of the fact that there exists no one-size-fits-all approach to configuring detection rules, and that such rules should be calibrated based on the specific ML/FT risks associated with their customers.

- *Example*: There was one specific instance where the transaction monitoring rules employed by the SP's transaction monitoring system did not generate alerts matching the activity undertaken by individual customer segments, but rather, alerts were generated on a one-size-fits-all basis without considering the specific nature and characteristics of the SP's customers, as well as prevalent ML/FT typologies. The transaction monitoring rules in place only triggered alerts on the basis of certain flags with invariable and static thresholds/parameters, some of which include the following: (a.) product specific daily thresholds; (b.) frequency of transactions; (c.) risky merchants; and (d.) risky countries. While these rules were deemed to be adequate, additional rules were required in order to allow the SP to better detect transactions or behaviour that diverged from the customers' usual transactional patterns, as well as minimise the number of alerts that were false positives. The very nature of a one-size-fits-all model defeats the purpose of establishing a comprehensive customer profile because such profile is not taken into consideration while monitoring customer activity and transactions.

One of the considerations that SPs will need to take into account when configuring their detection rules is whether they have customers with multiple accounts. If this is the case, SPs must ensure that the transaction monitoring systems and controls implemented are capable of holistically monitoring the customers' activities across their various accounts by adopting an aggregated view. A further consideration is the distinction between Single Euro Payments Area (SEPA) payments and Society for Worldwide Interbank Financial Telecommunications (SWIFT) payments[1]. Making use of SEPA brings with it several advantages, such as payments usually taking less than one business day to be processed, and transfers only requiring the customer's International Bank Account Number (IBAN) and not the Bank Identifier Code (BIC) to be executed. Furthermore, given that SWIFT enables international payments, this means that certain SWIFT transfers may present a heightened level of risk, especially if there are higher risk countries involved. Notwithstanding, SPs should still remain alert in the case of SEPA payments, ascertaining that such transactions are duly monitored and validated if necessary. The use of SWIFT or SEPA can therefore be an indication of geographical risk though it would need to be considered in more detail. Further information regarding additional factors that may be considered when implementing detection rules are illustrated in the table found on page 13 of this document.

In addition to the configuration of detection rules, the SP may need to develop customer segments and monitor their transactional activity through the analysis of transactions undertaken by each respective segment. A customer segment should comprise a cluster of customer profiles that are similar in nature in terms of characteristics, risk rating and transactional activity, and the clustering of which makes economic sense. It is recommended that the customer segmentation methodology applied by the SP distinguishes between personal customers and corporate customers, and is then further broken down into other related segmented target groups, which may include the ones delineated below:

[1] SEPA is a payment type used to transfer euro currency across Europe in countries within the SEPA region, while SWIFT is an international payment type used for cross-border payments in different currencies.

Personal Customers	Corporate Customers
Employed individuals - Full-time, part-time and seasonal employees - Professionals, public sector employees and blue collar workers	Size of business and operations - Small-sized enterprises - Medium-sized enterprises - Large-sized enterprises
Self-employed individuals - Small business owners, e.g. retail shops, restaurants and hawkers - Designated Non-Financial Businesses and Professions (DNFBPs)	Business structure - Private and public companies - Other legal arrangements such as trusts, foundations, associations and charities - Governmental entities
Low/no income individuals - Unemployed - Pensioners - Students	Economic sector - Primary - Secondary - Tertiary - Quaternary
Higher risk customers - Politically exposed persons (PEPs) - High Net Worth (HNW) individuals - Non-resident customers	Industry and product risk - Cash intensive businesses - High risk products - Foreign financial institutions - Correspondent banking relationships
	Transactional activity - Average transaction value and volume (e.g. distinction between customers that have an average monthly transaction amount of €10,000 vs €1 million)

Through risk-based customer segmentation, SPs are able to calibrate suitable thresholds and parameters for each customer segment. These thresholds and parameters can include a limit on transaction amounts in a particular currency, a cap on the number of transactions, or a combination of both. It is equally important that consideration be given to the implementation of rules that can help the SP detect situations where instead of a single transaction the customer meets a given threshold through two or more transactions. By appropriately configuring and implementing thresholds and parameters, SPs will be able to flag unusual or suspicious transactions, or patterns of transactions, that have potential ML/FT elements with a reasonable degree of certainty. It is important that the monetary values and/or volumes of the thresholds and parameters established for specific customer segments are realistic. Setting thresholds and parameters that are too high may hinder the SP's ability to effectively monitor transactions when taking into account the transaction amounts and ML/FT risks involved. As a consequence, this may result in certain large and anomalous transactions, as well as sudden deposit spikes, not being detected and properly scrutinised.

- *Example*: While reviewing the transactional activity of a number of customer files pertaining to a credit/financial institution, the FIAU noted deficiencies related to the thresholds applied for a particular detection scenario that the SP had in place to monitor high value transactions that exceed a specified threshold for a 14 day aggregate amount. In the case of two customer files, various large transactions ranging from approximately €300,000 to €1,100,000 affected during a specific year were not alerted by the SP's transaction monitoring system, despite the materiality of the values involved. The SP explained that such transactions were not flagged because the threshold for the segment related to the first customer was around €6 million for a 14 day aggregate amount, while the threshold for the segment related to the second customer was circa €4.5 million for a 14 day aggregate amount. These monetary thresholds were deemed to be too wide to allow the SP to effectively monitor large transactions and adequately mitigate the underlying risks associated with such transactions.

SPs need to be aware of what type of transactions or behaviour are to be expected during the course of the business relationship. By defining a set of parameters or factors within which transactions are considered normal for a particular customer or customer segment, this will allow the SP to determine whether the customer's transactions or behaviour are consistent with its knowledge of the same, and if necessary, question any discrepancies noted.

Thresholds and parameters can be grouped and integrated into specific risk scenarios that enable the identification of transaction patterns and behaviours associated with certain higher risk areas and known ML/FT typologies. The use of risk scenarios should not be limited to SPs with fully automated systems because smaller SPs with more manual measures can apply similar detection logic to assist with capturing the more complex risks. Applying oversimplified risk scenarios to broad ranges of customers or behaviours may impinge on the SPs' ability to monitor the actual transactional activity of certain customer segments. However, having too many risk scenarios in place makes it more difficult for SPs to maintain context among, and distinguish between, the scenarios. For this reason, SPs should strive to establish scenarios that are sufficiently detailed, but at the same, are still manageable and efficient.

The table overleaf contains a non-exhaustive list of the factors that SPs may consider when developing their detection rules, as well as some practical examples of risk scenarios that can be applied:

Detection Rules Category	Factors to consider when configuring Detection Rules	Risk Scenarios that can be applied
Customer	The type of customer (i.e. personal or corporate customer). The customer segment. The customer's size and set-up. The customer's industry. The customer's risk profile and rating. How long a customer has had a relationship with the SP – stricter monitoring may be required for new customers. Comparisons with the customer's age group.	Customer operating within a high risk industry/sector. Adverse media found on customer. Change in customer risk classification. Customer behaviour: • Monitoring the customer's monthly/quarterly/yearly activity and comparing it to the same customer's activity in the previous period. • Significant activity by new customer. • Significant deviations from past customer activity. Manual submission of a payment order. Periodic customer profile monitoring – generates an alert if the review period has expired.
Product/Service and Client Interface	The specific products or services being offered by the SP such as banking, trade finance, wealth management, payment services and foreign exchange. Products/services that are more susceptible to being exploited for ML/FT purposes and/or fraud. The distribution channels (i.e. face-to-face or non-face-to-face).	Change in customer activity by product. Cash withdrawn from unusual product. Anomalous activities involving the use of bank cards (e.g. ATMs, credit cards or debit cards). Multiple deposits made by the same customer in different bank branches. Over-pricing/under-pricing of products offered by customers. Seasonal products being traded out of season or products sold outside their usual geographical market. Payments by third parties unrelated to the customer for certain products that are not customary to receive payments from third parties, e.g. fixed deposit accounts, loan accounts and brokerage accounts.

Detection Rules Category	Factors to consider when configuring Detection Rules	Risk Scenarios that can be applied
Jurisdiction	The jurisdiction(s) where the customer or its beneficial owner(s) are based, have their main place of business or where the activity generating their wealth is carried out.	Domestic vs international transfers. Transaction activities with nexus to higher risk geographies. Transactions to/from sanctioned or blacklisted countries. Transactions to/from high risk jurisdictions with which the customer did not have any business dealings before.
	The jurisdiction(s) with which the customer has strong trading or financial connections.	
	The jurisdiction(s) with which the customer or its beneficial owner(s) have relevant personal links, e.g. the individual's residence in a given jurisdiction.	
	The anticipated or actual jurisdictional connections.	
	Whether the customer has any links to high risk, sanctioned or blacklisted countries.	
	The transactions' country of origin or destination.	

Detection Rules Category	Factors to consider when configuring Detection Rules	Risk Scenarios that can be applied
Transaction	The nature (i.e. cash or non-cash) and frequency of the transactions.	Aggregated cash/non-cash transactions. SEPA vs SWIFT transfers. Unusual patterns of cash deposits or withdrawals which may be indicative of potential structuring/smurfing[2], including aggregated frequent and small transactions. Transactions that exceed a specified threshold that varies depending on the particular segment the customer falls in. Rapid movement of funds in and out of a customer account. Anticipated level and volume of transactions declared at onboarding not in line with actual activity. Actual customer turnover exceeds the declared turnover in terms of transaction value or volume. High activity after period of low activity. High activity without any previous activity. Aggregated amounts just below the threshold. Credit followed by a debit (e.g. pass-through transactions) – compares a customer's incoming and outgoing payment activity to flag any unusual pass-through behaviour. Transactions to/from legal arrangements such as estate management trusts and private foundations. Transactions to/from high-risk industries/sectors. Transactions to/from higher risk customers such as PEPs.
	The anticipated level and volume of transactions as determined through the customer's business and risk profile.	
	The expected level and volume of transactions when taking into account the specific customer's background, occupation, claimed SOF and past transactional history.	
	When a dormant account suddenly becomes active.	

[2] A money laundering technique which involves breaking up large transactions into smaller ones to avoid detection.

		Transactions in round amounts. Inter-company/group transactions – transactions between companies with a shared relationship/economic connection. Circular payment flows between originator and beneficiary – multiple transfers to/from the same counterparty. Customer account being used for different purposes, e.g. an account created to collect condominium payments being used for personal use. Hidden and significant commercial relationships between customers evident through funds flows. Activities or behaviours consistent with certain predicate offences such as fraud, possible tax evasion or avoidance, corruption nexus, or funding of terrorism. Multiple reversals linked to particular customers. Idle account with sudden activity. Premature repayment of a loan. Sudden emptying of customer account. Substantial percentage of the available balance of the customer's account used within a day. Early closure of customer account. Customer with frozen accounts affecting transactions through other non-frozen accounts. Violations linked with the Fund Transfer Regulation.

Testing of Detection Rules

Detection rules need to be periodically tested and reviewed from both a technical aspect and effectiveness standpoint. The need for such regular fine-tuning is to allow for more granular analysis while minimising the likelihood of false positives being generated. False positives not only increase the cost of compliance, but may also result in analysts focusing their attention on transactions that are incorrectly flagged as being unusual or suspicious. Maintaining a tolerable low false positive rate is paramount for SPs to ensure that:

- Internal resources are not wasted;
- Customer experience is not adversely impacted; and
- Unusual or suspicious transactions are more accurately identified and timely investigated.

SPs must clearly document how detection rules are defined, maintained and tested. One way through which SPs can test their detection rules is back-testing, whereby the effectiveness of the rules applied is tested retrospectively, and if required, adjustments are made. Aside from back-testing, SPs can also make use of certain statistical tools and methods such as above-the-line (ATL) and below-the-line (BTL) testing. These approaches involve increasing and decreasing the transaction monitoring thresholds and parameters to arrive at the most optimal calibrations, which reduces the volume of false positives or negatives generated.

Alerts Management

When the underlying criteria behind a pre-determined detection rule/s is/are met, a transaction monitoring alert should be generated for further assessment. SPs should have an adequate process for the notification, handling and recording of alerts, as well as the actions taken. When a particular transaction is flagged, transaction monitoring analysts should exercise due diligence, ascertaining that the transaction in question is duly reviewed, and if required, obtaining the necessary supporting documentation/explanations, as well as clearly documenting the rationale for closing or escalating the alert. Where appropriate, analysts may need to adopt a more holistic approach and not only consider the alerted transaction in question, but also the customers' transactional history and past alerts. It is essential that alerts are analysed and cleared within a reasonable timeframe, and that internal timelines are established for the monitoring of alerts. If the elements resulting in the alert provide reasonable grounds to suspect ML/FT, the SP must report this suspicious transaction to the FIAU without undue delay so as to ensure that it is satisfying its obligations in terms of Regulation 15(3) of the PMLFTR.

The recording of the alert and the actions taken as a result thereof are essential steps within the wider consideration of the transaction scrutiny process. Apart from ensuring a proper internal audit trail that can address any supervisory queries, the records can provide useful material to assess the adequacy of the transaction monitoring rules as referred to in precedence and the overall efficacy of the monitoring system, including its human elements. These same alerts and the results thereof can also provide interesting insights when reviewing a customer's risk understanding. In addition, in the event of possible queries from an intelligence or even a law enforcement perspective, the records will allow the SP to justify the course of action undertaken.

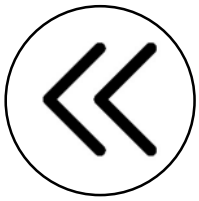
Adequate Resources and Training

SPs must have sufficient capacity and resources (both human and technological) available to perform risk-based transaction monitoring. Staff should be equipped to timely perform their transaction monitoring related duties, especially those related to the alert handling process. To this effect, SPs are required to not only allocate sufficient resources to this particular task but also provide adequate training and guidance to all relevant staff members on a regular basis to strengthen their knowledge and expertise in the area of financial crime, as well as make them more aware of existing ML/FT risks and typologies. Particular emphasis should also be given on training staff to identify unusual or suspicious transactions, and flag them for further assessment either prior or following their execution or reporting.

The importance of having in place formalised and detailed transaction monitoring policies and procedures that provide adequate guidance on how transactions are to be effectively scrutinised cannot be overstated. However, the FIAU noted that the policies and procedures drafted by SPs were at times lacking, and did not provide sufficient information in relation to transaction monitoring, as illustrated below:

- *Example*: For one SP, the transaction monitoring procedures in place failed to define the detection rules used to flag suspicious transaction activity and did not include any parameters that guided the basis for unusual or suspicious transactions to be discounted or otherwise.

Pre-transaction (a priori) Monitoring



AML/CFT obligations are intended to result in the implementation of measures that not only allow for the detection of possible ML/FT but also for the prevention of the same. This is especially visible when it comes to Regulation 15(4) of the PMLFTR, which envisages situations where SPs are able to detect and report suspicious transactions even before their execution, thus allowing the competent authorities to take the necessary measures with respect to the funds involved while the same are still with the SP. This in itself implies that there has to be a level of a priori or real time monitoring taking place.

Pre-transaction monitoring is carried out in real time prior to the transactions being affected, thereby introducing an additional layer of safeguards that facilitates the identification of unusual or suspicious transactions prior to their execution. Therefore, a priori monitoring minimises the potential ML/FT risks that could have materialised should the transactions have been undertaken without first undergoing adequate scrutiny.

Traditionally, pre-transaction monitoring is applied in situations where there is face-to-face contact, such as when a customer goes to a bank to make a cash deposit. Pre-transaction monitoring checks are also carried out in instances when transactions are not carried out instantaneously, but allow for its subsequent execution at a pre-determined future point in time, such as in the case of trade finance. A further example of pre-transaction monitoring is when as part of the credit application process, checks are completed on relevant parties before the loan is approved.

However, other than the scenarios outlined above, pre-transaction monitoring checks should also be undertaken prior to the processing of transactions assessed to pose higher risks or involving higher risk customers. While SPs are not expected to review all of their customers' transactions in real time, in line with the Risk Factor Guidelines issued by the European Banking Authority, they should identify those risk factors which, within the context of their particular business model, will highlight higher risk transactions and implement the necessary measures to be able to flag these transactions and scrutinise the same before being affected[3]. Such transaction monitoring measures are to be determined based on particular detection rules determined in line with the SPs' business models and customer bases. SPs should identify those scenarios that constitute unusual or suspicious activity and appropriately scrutinise the transactions involved before these are allowed to pass. At a minimum, SPs are expected to carry out pre-transaction monitoring in the case of the high risk scenarios set out hereunder:

- Transactions linked to sanctioned individuals, entities or countries;
- Transactions or behaviour indicative of certain predicate offences such as fraud;
- Transactions executed by individuals or entities for which repeated and reliable adverse media has been found;
- Transactions to/from high risk jurisdictions or non-reputable jurisdictions;
- Transactions or behaviours that inconsistent with the customer's business and risk profile and/or significant diverge from the expected or known transactional activity; and
- Unusually high value and anomalous transactions within the context of the SP's business model.

[3] Para 4.74 of the *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines')* under Articles 17 and 18(4) of Directive (EU) 2015/849 (EBA/GL/2021/01) dated 1 March 2021 and issued by the European Banking Authority.

When carrying out pre-transaction monitoring checks, SPs should determine the appropriate type and extent of checks to be applied for different customer types. Some examples of checks that can be conducted include the following:

- Obtaining an understanding of the background and purpose of transactions that exceed the pre-defined thresholds and parameters to ensure that these tally with the customers' profiles;
- Engaging customers and requesting further information and/or documentation to support the transactions in question; and
- Acquiring approval from management before processing higher risk transactions.

Over the years, there have been instances where the transaction monitoring system adopted by SPs were predominately based on post-transaction monitoring, meaning that transactions were not, when necessary, adequately scrutinised prior to their execution. At times, the pre-transaction monitoring measures applied were limited to sanction screening, which simply included screening new and existing customers against applicable sanction lists, PEP lists, and other watchlists. As a result, the screening conducted did not extend to cover the amount involved in the transaction. This resulted in SPs having very limited control over whether unusually large or anomalous transactions may be processed.

In terms of detection rules, SPs can configure their transaction monitoring systems to flag transactions on the basis of a variety of different scenarios, thresholds and parameters. By way of example, transactions can be alerted if an incoming or outgoing payment exceeds certain thresholds and parameters which may differ depending on the customer segment involved. Alerts can also be generated if the transaction details or payment field contain specific words that are of a more suspicious nature such as "drugs", "fuel", "chemical" and "weapon". Apart from establishing thresholds and parameters for individual customer segments, SPs can also decide to implement daily, weekly and/or monthly limits for specific customers or smaller customer groups, whereby an alert is raised, and related transactions halted, if in aggregate, the value or volume of transactions affected in any one day, week and/or month exceeds a certain pre-established threshold.

SPs can also set tailored limits for certain relationships between their customers and other third parties, or even whitelist these relationships by applying thresholds and parameters that are higher than normal. In these relationships, the customer may either be regularly receiving funds from a third party, regularly remitting funds to a third party, or a combination of both. Prior to such limits being implemented, the SP would need to obtain an understanding of the purpose of the relationship between the customer and the other third party involved, as well as confirm that the transactions executed make economic sense. Likewise, the SP can blacklist payments to/from certain individuals or corporate entities that fall outside of the SP's risk appetite. More stringent detection rules should also be in place in cases where there is a cash element to the transactions in question, such as a bank deposit or subscription made in cash.

Post-transaction (a posteriori) Monitoring

Contrary to pre-transaction monitoring, which is carried out before the transactions are processed, post-transaction monitoring takes place after the transactions have already been affected, i.e. after the event. Thus, while pre-transaction monitoring focuses more on detecting unusual or suspicious transactions that are more obvious outliers, post-transaction monitoring facilitates the holistic review of customers' transactions over a period of time, thereby enabling SPs to also build and continuously update its customers' profiles on the basis of their historic transactional activity.

A posteriori monitoring empowers SPs to identify patterns of transactions that are unusual, raise suspicion and/or are not in line with the customer's profile but which may not be immediately apparent as they take place over a period of time. The implementation of effective post-transaction monitoring controls also enables the identification of deposit spikes or deviations from the information available on the customer and its transaction history, which should include information on the customer's expected level and nature of activity. When spikes in customer deposits are identified, the SP should establish the purpose of the transactions and source of the incoming funds, as well as ensure that there exists a justifiable explanation for these transactions. Following the necessary review, should the transactions give rise to suspicion of ML/FT, it is critical that such transactions are reported to the FIAU in a timely manner. Further to this, if a red flag or trigger event is detected, the SP is required to analyse the matter and take the appropriate action in a timely manner, and not wait for such issue to be addressed during the performance of routine periodic reviews.

As is also the case for pre-transaction monitoring, detection rules as explained above can be integrated into a post-transaction monitoring system, on the basis of which transactions are alerted for further investigation once they have already been executed. However, as part of the post-transaction monitoring process, SPs can also opt to issue post-transaction reports based on a pre-determined frequency. Each individual report will contain transactions of a similar nature which are grouped and examined together depending on the nature of the transactions and customer segments involved. Some examples of post-transaction monitoring reports that can be generated include those analysing:

- Cash deposits (aggregated over a period of time or totalling more than a certain amount);
- Aggregated frequent and small transactions to a related or unrelated party;
- Structured large transactions;
- Wire transfers with filters using amounts and geographical factors;
- Monetary instruments usage;
- Account turnover;
- Peer group activity; and
- New account activity.

Having access to a wide variety of post-transaction reports which cover several different transaction types and customer segments allows subject persons to have a more holistic view of its customers' transactional patterns and facilitates the detection of unusual and suspicious transactions.

To establish expected customer behaviour, SPs may divide its customer portfolio into homogenous peer groups which comprise of groups of customers with the same characteristics and risk rating. Through data analysis, the SP will then be able to compare the actual transactions or behaviours of individual customers to the expected transaction patterns of the peer groups. Any statistically significant deviations or outliers are automatically captured by the transaction monitoring system, triggering an alert for further assessment.

The transaction monitoring systems adopted by SPs should incorporate a combination of elements of both pre-transaction monitoring, as well as post-transaction monitoring. Insights derived from carrying out post-transaction monitoring such as the most common customer transactional patterns, behaviour and trends can be used to continuously refine the set of initially configured detection rules that are applied as part of the pre-transaction monitoring process. This enables SPs to conduct more targeted pre-transaction monitoring that focuses on the highest risk areas. Correspondingly, having a robust pre-transaction monitoring system in place means that the majority of unusual or suspicious transactions are identified and reviewed before they are executed, which in turn helps to reduce the degree of monitoring required at the post-transaction monitoring stage.

Conclusion

This guidance paper sets out the FIAU's expectations with regard to the measures and practices to be adopted for the effective application of transaction scrutiny, with a particular emphasis on institutions processing payments and similar transaction for and on behalf of customers. With the increasing complexity of financial systems and evolving tactics applied by criminals to carry out ML/FT, transaction monitoring has become more crucial than ever. SPs that fail to implement robust transaction monitoring controls not only run the risk of facilitating potential ML/FT, but may also face reputational damage and administrative action. Therefore, it is pertinent that SPs invest in sophisticated transaction monitoring tools that incorporate both pre-transaction monitoring and post-transaction monitoring, as well as continuously enhance their monitoring processes to safeguard their businesses, customers and the local financial system as a whole.

The evolution of technology is increasing the demand for an ever more positive customer experience as they expect transactions to be executed within seconds of having given their instructions. Indeed, the time within which transactions have to be legally executed is ever decreasing, posing questions as to how AML/CFT obligations can still be met. And the answer is to be found in the adoption and deployment of ever more advanced technological solutions that can analyse transactions in ever shorter timeframes. Indeed, machine learning and AI-based solutions are to become ever more important in the context of transaction scrutiny as they will allow SPs to meet what can appear to be contrasting sets of obligations and even enhance the scrutiny carried out through detecting transactional patterns that are not easily identifiable through other means.

65C, Tower Street,
Birkirkara BKR 4012,
Malta

Questions on this document or on the application of AML/CFT measures may be sent to **queries@fiaumalta.org**

Financial Intelligence Analysis Unit
65C, Tower Street,
Birkirkara BKR 4012,
Malta

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org