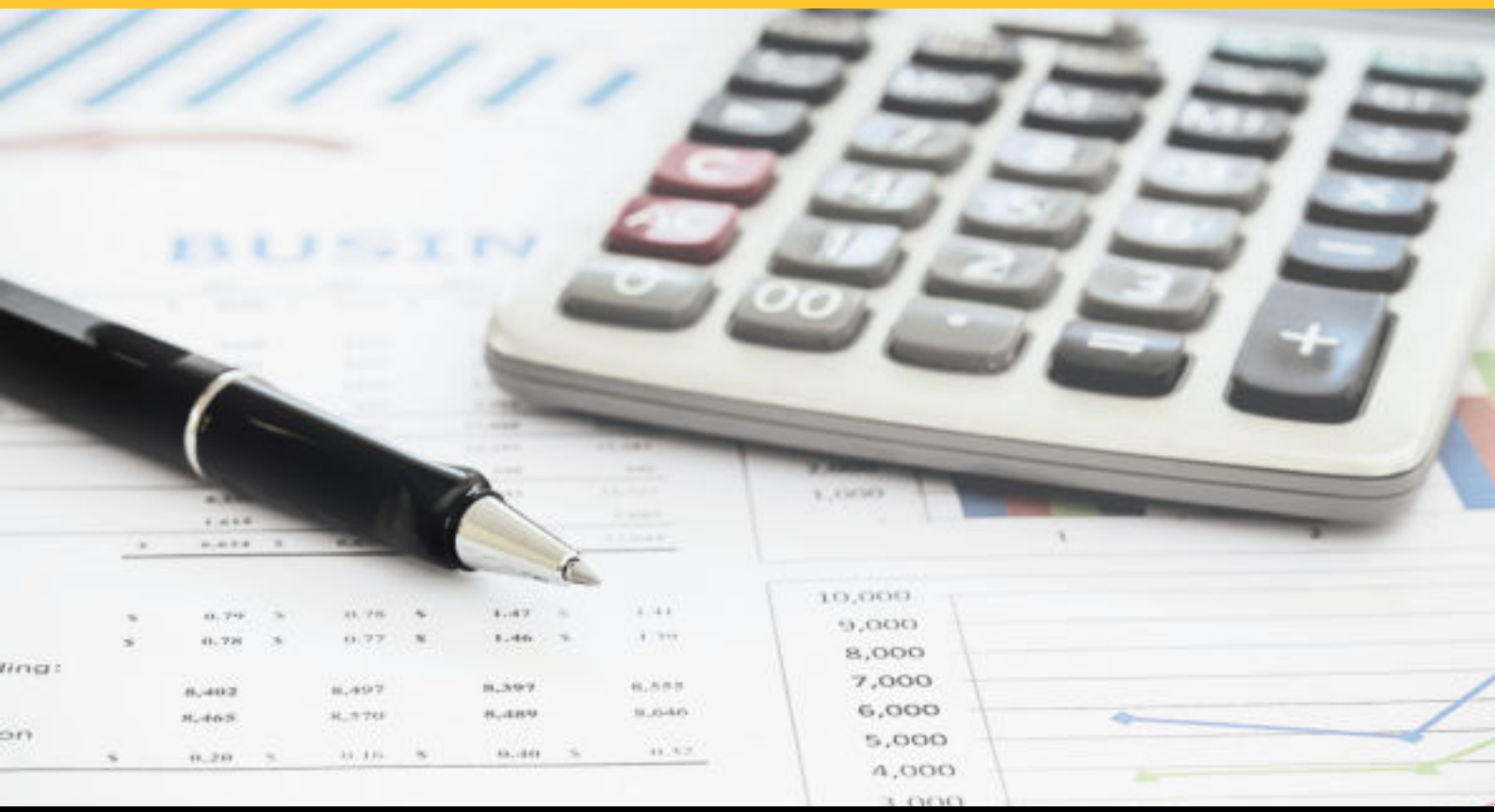
Transaction Monitoring Training and Outreach Event

Questions and Answers Document

Published July 2023



Disclaimer

This document contains a compilation of selected questions and corresponding answers that were raised during the Q&A sessions of the transaction monitoring training and outreach event organised by the FIAU, in collaboration with the MFSA, on 6th June 2023. It is important to emphasise that the queries covered in this document are specifically focused on transaction monitoring and related sub-topics that featured during the training session. Any additional enquiries on this document or the application of AML/CFT measures can be directed to queries@fiaumalta.org

Questions and Answers

1 **What constitutes an unusually large transaction? Is there a specific threshold in place, or is this determined based on comparison with previous transactions?**

There is no pre-defined monetary threshold or specific criteria in place to establish if a transaction is considered to be unusually large when compared to other transactions. This determination depends on several factors such as the industry, products and services offered, customer base, and available resources of the Subject Person. The context, customer segmentation, and understanding of the customers' transactional patterns play a crucial role in identifying transactions that are significantly larger than others and deviate from the norm. Ultimately, Subject Persons must apply the risk-based approach and carry out adequate transaction monitoring to ensure compliance with their obligations and mitigate potential risks.

2 **If a 76-year-old individual, who receives a direct credit of pension and has no other known source of income, makes with a €3,000 cash deposit, should this be considered unusual and warrant Enhanced Due Diligence (EDD)? Moreover, should an alert be raised for such a transaction?**

If this transaction is a one-time occurrence, there should be no immediate suspicion that would necessitate the application of EDD, and therefore, the implementation of CDD measures should suffice. However, Subject Persons should consider previous transactions and assess whether there were any previously executed deposits and withdrawals that are unusual, suspicious or not in alignment with the customer's risk profile. If such patterns are identified, EDD may be required for that specific transaction or customer. It is essential that Subject Persons remain vigilant and request additional explanations and/or supporting documentation from their customers when deemed necessary.

3 Should cases of fraud be reported to the FIAU?

The FIAU's remit is specifically on the proceeds of crime arising from fraud, and not on the handling of individual instances of fraud. Thus, if the Subject Person knows, suspects or has reasonable grounds that the funds involved in the transaction have been generated from fraud, this criminal activity is to be reported to the FIAU without undue delay. However, it should be noted that the mere occurrence of fraud itself does not merit reporting to the FIAU. The reporting obligation arises when the fraud is linked to proceeds of crime, as fraud is a predicate offence.

4 Questions related to non-reputable jurisdictions

a.) How is transaction monitoring to be carried if a customer is linked with a non-reputable jurisdiction (e.g. Gibraltar or South Africa)? Does the credit/financial institution need to scrutinise each individual transaction that passes through the customer's account?

Even if the customer is associated with a non-reputable jurisdiction, the Subject Person is not required to monitor every transaction involved, especially if the transactions make economic sense and are similar in nature. Hence, as long as the Subject Person can identify a consistent pattern in the customer's behaviour, it would not be necessary to scrutinise each individual transaction affected by the customer. However, this approach relies on the accuracy and reliability of the information provided.

b.) Should a payment be flagged as connected to a non-reputable jurisdiction if a remitter or beneficiary is registered in Gibraltar, but the associated bank account is in the United Kingdom?

This particular transaction should usually be flagged by the Subject Person's transaction monitoring system, as most solutions have detection rules configured to alert transactions from non-reputable jurisdictions such as Gibraltar. However, as explained previously, it is not necessary for the Subject Person to have evidence on file for each and every transaction linked with non-reputable jurisdictions.

5 Questions related to the level of transaction scrutiny required in different scenarios

a.) In relation to sale of property, would a copy of the sale/acquisition contract be sufficient to meet due diligence standards when no background information is provided on the buyers and their source of wealth (SOW)?

This assessment depends on the method of payment, i.e., whether it is through a loan or from the customer's own funds. If the transaction involves a loan, this does not usually present a heightened level of risk as long as there are appropriate checks in place to verify the borrower's ability to repay the loan using their own funds or other legitimate funds. However, if the transaction directly involves the customer's own funds, it carries a higher level of risk, especially if the amount is large. In such cases, the Subject Person would be expected to obtain documentary evidence to substantiate the customer's SOW and the source that would be funding the purchase of the property.

b.) In a scenario where the Subject Person has no direct relationship with the lender and the customer of the Subject Person is the borrower, to what extent should the Subject Person scrutinise the source of funds (SOF)/SOW of the lender?

The mitigating measures to be adopted by the Subject Person will depend very much on the rationale for the transaction in question and how it is taking place. To effectively address potential risks, Subject Persons needs to ascertain the intended use of the funds being lent, determine the specific terms and conditions under which the funds are being lent, identify the parties to the transaction, and understand the connection that exists between such parties, if any. The explanations provided, the amount involved, how the funds are being made available, and the associated jurisdictions will also contribute to the Subject Person's understanding of the transaction in terms of both its business rationale and the ML/TF risks it presents.

Where it results that the situation presents significant ML/TF risks due to the lender and/or the amounts being provided, the Subject Person should seek additional information on the lender and its activities from the borrower as well as from publicly available sources.

When there is no existing relationship between the Subject Person and the lender, the level of scrutiny should depend on factors such as the amount and the jurisdictions involved in the transaction. The Subject Person should not solely focus on the transaction itself, but also obtain relevant information pertaining to the lender, consider any additional risks in relation to the lender, and ascertain that the purpose of the transaction is well understood.

6 What supporting documentation/information should be obtained for intra-group transfers and/or loans?

When dealing with intra-group transfers and loans, it is vital for all parties involved to have a clear understanding behind the purpose of the transaction taking place. This understanding should be supported by appropriate documentation such as service agreements, loan agreements, and terms of reference. The documentation obtained should provide insight into the relationship between the companies involved, which should go beyond the mere fact that they form part of the same group. Generic statements such as “the transfer/loan was provided to sustain the business operations of another company” are insufficient and should be avoided. Rather, such documentation should include details regarding the nature of the business operations that the transfer or loan is intended to support. Furthermore, it is of utmost importance to assess whether these operations make sense in light of the customer profile and available information.

7 If a customer receives a dividend, is the Subject Person required to scrutinise the financial statements of the company from which the dividend was distributed?

The scrutiny of dividends should be based on the amount being transferred to third parties and the associated level of risk. If the dividend amount is large, it is at the Subject Person's discretion to determine whether the risk related to such dividend distribution warrants additional scrutiny. This may include cross-checking the information contained within the dividend warrant with the declared dividend in the financial statements. However, for smaller amounts, the dividend warrant may be deemed sufficient, without the need to acquire further supporting documentation.

8 How should a credit institution treat the use of bank cards at ATMs/point of sales in high risk jurisdictions? Should a customer be contacted and asked to provide a reason for such usage?

In situations where a credit institution notes that a customer is utilising bank cards in high risk jurisdictions, the decision for the credit institution to contact the customer should depend on the circumstances at hand. If the amounts being withdrawn are substantially high, the Subject Person would be expected to enquire further about the purpose of the transactions. Additionally, it could also be the case that such withdrawals become frequent and habitual, potentially due to a change in residency. In this instance, the Subject Person would need to perform a re-assessment of the customer's profile and update the Customer Risk Assessment (CRA) to reflect the change in risk, as well as obtain additional information/documentation as necessary to update the customer profile.

9 In the case of home loans, where customers are expected to finance a percentage of the property price from their own funds, should the credit/financial institution scrutinise the SOF of the front finance amount?

The value of the front finance amount should be assessed in light of the information and supporting documentation obtained. In cases where the 10% upfront deposit is of a significant amount, in addition to collecting information on the customer's employment and income streams, Subject Persons should seek further supporting documentation to substantiate the transaction. For example, while it is relatively common for a customer to pay a 10% upfront deposit of €20,000, which can be supported by merely obtaining information on employment, higher amounts should be accompanied by additional evidence such as payslips or other SOW/SOF documentation.

10 If the Subject Person is in the process of changing its transaction monitoring solution, is it expected for there to be a period of time during which both the existing and new systems are running simultaneously, to ensure there are no gaps in monitoring coverage?

When transitioning from one transaction monitoring solution to another, it is not mandatory for Subject Persons to have both systems operating at the same time. However, it is considered prudent to run both systems in parallel, as this ensures that there is a backup system in place in case any issues arise during the implementation of the new system. The crucial factor is ascertaining that proper records are maintained during the transfer of data between the two systems.

11 When it comes to transaction monitoring for short-term loan and microloan customers, how should Subject Persons approach transaction monitoring, particularly if the loan is repaid by third parties?

With regard to short-term loan and microloan customers, the Subject Person should prioritise gaining a comprehensive understanding of the customer and clearly identifying the purpose of the loan. Short term loans, in particular, warrant additional scrutiny due to their potential association with terrorism financing. Additionally, it is important for the Subject Person to monitor any third parties involved in paying off the loan. In such instances, it is vital to gather information about the third parties involved to ensure a holistic assessment of the transaction.

12 What are the FIAU's views in relation to the role of Artificial Intelligence (AI) and Machine Learning in transaction monitoring?

The FIAU acknowledges the potential benefits of incorporating AI and machine learning technologies in transaction monitoring systems, recognising that they can enhance operational efficiency and optimise resource allocation. However, Subject Persons are advised to exercise caution due to the evolving nature of these technologies. Moreover, it is important that Subject Persons do not place sole reliance on transaction monitoring systems merely because they encompass elements of AI and machine learning. Rather, these systems should be tested, fine-tuned and validated on a regular basis to ensure that the right types of transactions that indeed warrant further scrutiny are being captured and flagged for review.

Subject Persons should be able to prove that the transaction monitoring system in place is effective and calibrated on the basis of their specific customer base, their customers' respective risk profiles, and the products/services offered. It is also pertinent that Subject Persons are actively involved in the system implementation, have a comprehensive understanding of the underlying considerations and parameters adopted, and maintain an audit trial of any changes made to the detection rules.

While AI and machine learning systems can provide a high level of efficiency in detecting unusual and suspicious transactions, human intervention and oversight will always remain an essential component of the transaction monitoring process, particularly with respect to interpreting and addressing the alerts generated. Such human intervention is necessary to contextualise the alerts, consider additional factors, and make informed judgements as part of the decision-making process.

13 In the context of a gift or donation, how are Subject Persons supposed to obtain relevant SOW/SOF information and/or documentation pertaining to the donor if such individual or entity is a third party and not a customer of the company?

It is acknowledged that obtaining relevant SOW/SOF information and/or documentation on the donor in certain situations can be challenging. However, Subject Persons should still strive to carry out the necessary transaction monitoring checks on a risk sensitive basis, even when collecting documentary evidence may present difficulties.

At the onset, the Subject Person should assess the risk associated with the transaction, taking into consideration factors such as the nature and size of the gift or donation, as well as the customer's specific risk profile and the relationship between the donor and the donee. In cases where there is a legitimate relationship between the donor and donee that justifies the gift or donation (e.g. parent – child relationship), and the amount of the gift or donation is within the expected means of the donor, then there would be no need for any additional measures to be taken.

If the gift or donation is of a substantial value or raises concerns, the Subject Person may need to obtain further information on the donor through the donee to verify the legitimacy of the funds received. As part of the transaction scrutiny process, the Subject Person may request the customer to provide certain information regarding the donor, which will vary depending on whether the donor is a natural or legal person. If the donor is a natural person, the requested information may include the individual's name, address, occupation and other wealth generating activities. Conversely, if the customer is a legal person, the Subject Person could consider requesting information/documentation such as the entity's legal name, registered address, ownership structure, business activity, and industry. The Subject Person may also take advantage of publicly available information found online or in databases to validate the information provided by the donor. In some cases, the Subject Person may opt to request the necessary SOW/SOF information and/or documentation directly from the donor.

14 Will the imminent introduction of instant payment regulations have an impact on Subject Persons' obligations vis-à-vis transaction monitoring?

The European Union (EU) Commission acknowledges the need for pre-transaction monitoring, even in the context of instant payments. In fact, the Commission emphasises that when providing instant payments, Subject Persons must ensure that they have in place real time fraud, money laundering, and terrorist financing prevention tools, in full conformity with existing EU legislation. Therefore, it is clear that the introduction of instant payments does not exempt Subject Persons from carrying out real time transaction monitoring and is without prejudice to any risk-based measures implemented in terms of AML/CFT.

In view of the above considerations, it should be re-highlighted that the instantaneity of these payments, within less than 10 seconds, will not affect the obligation of Subject Persons to perform their required AML/CFT checks and, if necessary, file suspicious transaction reports (STRs) with the competent authorities. There may be circumstances where these checks have to be conducted in real time as opposed to post-transaction; however, this determination should be made on a risk sensitive basis, as it is not expected that all transactions are screened ai priori.

The advent of instant payments reinforces the importance for Subject Persons to adopt technologies and systems that enable the timely identification of unusual and suspicious transactions, as well as the effective management of ML/FT risks in real time. By implementing robust pre-transaction monitoring controls, Subject Persons are able to proactively detect and prevent potentially illicit activities, thereby safeguarding the integrity of financial systems and protecting their customers from financial crimes. Notwithstanding, it should be re-emphasised that effective monitoring post-transaction tools are also indispensable, and Subject Persons must ensure that such measures are implemented in a timely manner and are not unnecessary delayed.

15 Is it necessary to carry out periodic reviews for low risk customers?

Periodic reviews should be conducted for all customers, irrespective of their assigned risk rating, and even in the absence of a trigger event that may point to a change in the business relationship. This ensures that the information, documents, and data held on the customers are kept up-to-date. Since this process needs to be risk-based, the frequency and scope of the periodic reviews should vary depending on the risks associated with the customers involved. As a result, customers considered to present a high risk of ML/FT should be subject to more frequent and extensive reviews than those deemed to be low risk. In terms of frequency of ongoing monitoring, there are no mandatory timeframes prescribed by law for each customer category. However, it is important that Subject Persons establish reasonable timeframes based on the customer's risk rating, the type of information to be updated, as well as the potential risks that could be mitigated through updating.

By performing reviews on a periodic basis, Subject Persons will be in a better position to capture changes in their customer's circumstances or risk profile, and ascertain that the risk rating allocated accurately reflects the ML/FT risk posed by the business relationship. Moreover, carrying out periodic reviews helps Subject Persons to identify potential red flags and suspicious activities that may merit further scrutiny.

Certain products or services offered to customers may indeed present an inherently low level of risk that is expected to remain unchanged during the course of the business relationship. Some examples of these low risk scenarios include term deposit accounts, fixed term insurance policies, and other similar financial instruments. Likewise, certain customer types such as students and pensioners do not customarily present a high risk. However, even in such scenarios, the carrying out of periodic reviews is still crucial to ensure that any relevant red flags or trigger events are detected and duly actioned upon, if necessary. As previously mentioned, while the frequency and scope of these reviews will be less than those required for higher risk customers, they still play an integral role in the ongoing monitoring process. For instance, while for higher risk situations, the information and documentation requested during a customer relationship review may be more intensive, in lower risk situations, simply obtaining a declaration may suffice.

16 What is the optimal approach for Subject Persons to implement detection rules? Is there a way for Subject Persons to prevent customers from circumventing the thresholds set?

Where the transaction monitoring systems adopted by Subject Persons are based on a set of risk-based detection rules, it is indispensable to ensure that the rules are established according to the Subject Person's own business model, customer base, products and services offered, transaction channels, and historic transactional activity. In practical terms, detection rules comprise of applied risk scenarios, thresholds, and other parameters against which the customers' transactions are analysed.

Prior to implementing their detection rules, Subject Persons should develop customer segments, each comprising of a cluster of customer profiles that are similar in nature in terms of characteristics, risk rating, and transactional activity. It is generally recommended that the customer segments differentiate between personal and corporate customers, as their risk profiles and transaction patterns usually differ significantly. Personal customers typically include individuals, sole traders, or small business owners, while corporate customers encompass entities such as companies or other organisations. Ideally, customer segments are to be further broken down into related target sub-groups to reflect the specific risks and characteristics associated with different subsets of the Subject Person's customer base. Through customer segmentation, Subject Persons will be able to calibrate suitable detection rules to align with the specific profiles and behaviours related to each segment.

Customers belonging to a particular customer segment are subject to the risk scenarios, thresholds, and parameters defined for that segment. Any transactions that exceed the pre-defined limits in place or display unusual patterns will be subsequently alerted by the system for further review and investigation. Although the circumstances surrounding each respective customer are unique, a transaction monitoring system with appropriate detection rules in place can effectively identify transactions or behaviour that deviate from the norm within a specific customer segment. By automating the initial detection and alerting process, Subject Persons can enhance their ability to identify potentially unusual or suspicious transactions.

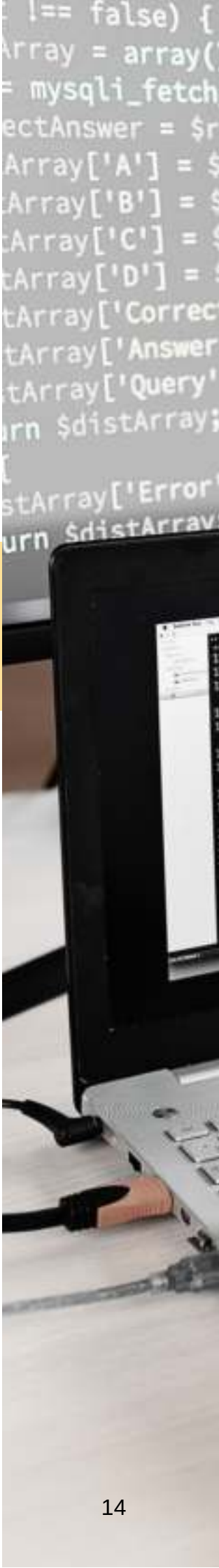
It is critical that detection rules are tested and fine-tuned on a periodic basis from both a technical aspect and effectiveness standpoint. The need for such regular tuning is to allow for more granular analysis while minimising the likelihood of false positives being generated. Furthermore, this minimises the risk of customers attempting to exploit or circumvent the thresholds and parameters set by manipulating their transactions to evade detection. Thus, periodic fine-tuning of the detection rules enhances the monitoring system's ability to identify unusual and suspicious transactions more accurately, even in cases where customers may have gained knowledge of the thresholds set.

17 What considerations should Subject Persons take in relation to Single Euro Payments Area (SEPA) payments and Society Worldwide Interbank Financial Telecommunications (SWIFT) payments[1] when configuring their detection rules?

SEPA payments are limited to the 28 EU member states and the four members of the European Free Trade Association (EFTA), and are subject to harmonised standards and regulations within the SEPA framework. In contrast, SWIFT enables international payments beyond the SEPA region, involving a wider range of countries and institutions worldwide. This global reach of SWIFT transfers may present additional complexities and a heightened level of risk, especially if there are high risk or non-reputable countries involved. Nevertheless, Subject Persons should apply appropriate AML/CFT measures for both types of payments, including SEPA payments, even though these are generally considered to be lower risk.

When establishing their detection rules, specifically those related to transactions, Subject Persons may choose to make a distinction between SEPA and SWIFT payments, which includes tailoring their transaction monitoring systems to address the potentially higher geographical risks associated with SWIFT transfers. This can be achieved by incorporating stricter thresholds and parameters for incoming and outgoing SWIFT payments, which may vary depending on the customer segments involved.

[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.



18 Is the cash element limited to transactions directly settled in physical cash, or does it also include incoming wire transfers from other credit/financial institutions that have been settled in cash?

If a customer receives a wire transfer from an individual/entity serviced by another credit/financial institution that previously involved the use of physical cash (for example, cash is deposited at financial institution A and then wired to financial institution B), this transaction should not be considered to have a cash element to it by the receiving credit/financial institution. Indeed, although the receiving credit/financial institution is still required to scrutinise the transaction in question as part of the normal transaction monitoring process, the previous cash element associated with such transaction is not a factor that the receiving credit/financial institution is expected to be aware of and take into account. This is especially true when considering the inherent difficulty for the receiving credit/financial institution to ascertain whether the transaction had a cash element in its prior stages. Moreover, if there was the involvement of several credit/financial institutions in the transaction chain, it becomes even more challenging for the receiving credit/financial institution to be aware of the previous use of cash.

19 Are Subject Persons expected to review transactions linked to adverse media?

While Subject Persons are not expected to review all of their customers' transactions in real time, at a minimum, they are expected to carry out pre-transaction monitoring in the case of certain high-risk scenarios, one of them being transactions executed by individuals or entities for which repeated and reliable adverse media has been found.

Adverse media alone does not provide sufficient justification for filing an STR with the FIAU; however, it is an element that should always be closely monitored by the Subject Person. When a party to a transaction is named in adverse media reports, the Subject Person must assess the adverse information found, the extent of its veracity and reliability, as well as consider the context of such adverse media in relation to the customer profile and transactions being processed. A correlation between such considerations should prompt the Subject Person to seek further clarifications on the customer and the transactions taking place before processing further transactions.

It is essential for Subject Persons to evaluate the reliability of the adverse media reports by considering factors such as the quality and independence of the source/s, as well as the persistence of these reports. The absence of an arraignment or a conviction should not be automatically lead to the dismissal of adverse media reports. Furthermore, while acquittals should also be factored in, Subject Persons should consider the reasons that led to the acquittal and whether such reasons dispel any concerns about the individual/entity involved.

20 Can Subject Persons rely on statistical data to create the profile of an average customer?

Subject Persons may use statistical data to develop behavioural models against which to eventually gauge a customer's activity in low/medium risk situations. In adopting this approach, Subject Persons can rely on data collected: (a.) from official economic indicators, such as average national income or average disposable income, issued by national public bodies or reputable financial institutions; or (b.) over a period of time by the Subject Person itself. However, it is important to note that the latter is only possible when the Subject Person has a sufficiently wide customer base to allow the creation of an average profile. It is crucial to ascertain that statistical models are monitored and updated as necessary, regardless of the approach selected.

21 For pre-transaction monitoring, what supporting documentation can be obtained from the customer to scrutinise transactions in investment funds made in kind or in specie?

Subject Persons are required to obtain an understanding of the transactions affected by their customers in line with the risk these transactions present and their underlying rationale. When a transaction is made in kind, it is important to ensure that the value of the assets is appropriate and aligns with market estimates. For high value investments, obtaining verified valuation reports and independent assessments may be necessary. Lower value investments can be evaluated on the basis of market trends.