



Effective Transaction Monitoring Measures and Systems, Alerts Management and Training (incl. Case Studies)

Jeremy Mercieca Abela and Liza-Marie Cassar

Enforcement Section



Implementation of Effective Transaction Monitoring





Establishing the Customer's Business and Risk Profile

- Subject Persons need to obtain a comprehensive understanding of their customers' business and risk profiles. To this end, prior to entering into any business relationships or carrying out any occasional transactions, Subject Persons must conduct a CRA and subsequently perform the necessary CDD checks.
- Once such understanding is formulated, Subject Persons will be able to determine the degree and nature of transaction monitoring checks to be undertaken.
- It is important that Subject Persons tailor their transaction monitoring approach depending on the customer type, risk profile, and products/services offered.





Implementation of Effective Transaction Monitoring

Importance of Adequate Scrutiny of Transactions

- Inadequate transaction scrutiny may adversely impact the detection of unusual and suspicious activity, as well as well hamper the Subject Person's ability to maintain a comprehensive business and risk profile.
- This allows for risks to be unmanaged, and for transactions to be processed without the necessary controls in place.





Changes to the Customer's Profile and Risk Level

- Certain transactions can trigger a review, and require an update of, the customer's profile, especially if there are changes in the customer's activity.
- In view of the updated risk assessment or other considerations, Subject Persons will need to determine whether the business relationship still falls within their risk appetite. If it does, Subject Persons will then need to assess whether any adjustments to the level of CDD are required.





Supporting Information/Documentation

There are instances where the identification of certain transactions or behaviour requires Subject Persons to obtain supporting information and/or documentation. These instances include transactions or activities that:

- Are unusual or suspicious;
- Are anomalous, atypical or outliers;
- Are unexplainedly or illogically repetitive in nature;
- Are inconsistent with the customer's business and risk profile;
- Diverge from the customer's usual transactional pattern; and
- Significantly differ from what is normally carried out or requested by the customer.











Supporting Information/Documentation (cont.)

- Regulation 11(9) of the PMLFTR obligates Subject Persons 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.
- Subject Persons should collect adequate supporting information/documentation on a risk-sensitive basis to substantiate the transactions under scrutiny, understand their purpose, and ensure that their rationale is justified.
- Transactions executed by customer need to be legitimate, and make business sense.



Implementation of Effective Transaction Monitoring

Supporting Information/Documentation (cont.)

 <p>SOW/SOF</p>	 <p>Bank Statements</p>	 <p>Financial Statements</p>	 <p>Invoices & POs</p>
 <p>Shipping Docs</p>	 <p>Contracts & Agreements</p>	 <p>Transaction Records</p>	 <p>Valuations</p>



Supporting Information/Documentation (cont.)

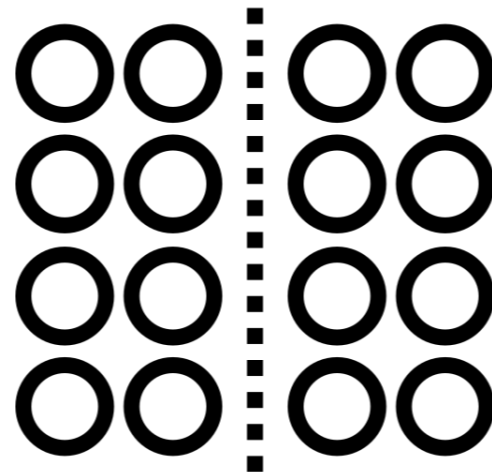
- Other relevant customer information that SPs should seek to acquire during the course of the business relationship:
 - Any new operational activities;
 - Any significant changes relating to the customer (e.g. change in ownership structure);
 - Details of any significant third-party relationships entered into;
 - Details of any legal or regulatory action against the customer; and
 - Any other relevant information to verify that the customer's funds are derived from legitimate sources.





Transactions of a Similar Nature

- If the customer's transactions are of a similar nature and have an analogous level of risk, Subject Persons may opt to focus on those transactions that are unusual, suspicious or deviate from the customer's expected level of activity (i.e. outliers) rather than reviewing all transactions.
- To justify the rationale behind transactions of a similar nature, the SP may also rely on the supporting information/documentation collected for previously executed transactions that are akin to the ones in question.





Reliance

- While a Subject Person may exercise reliance on the CDD measures carried out by another Subject Person or third party, the obligation to conduct ongoing monitoring always remains the former Subject **Person's** responsibility.
- Therefore, this means that the Subject Person cannot rely on another Subject Person or third party to scrutinise transactions.





Implementation of Effective Transaction Monitoring

Transaction Monitoring Red Flags

Transactions inconsistent with the customer's profile

Unusual customer activity

Inconsistencies in the customer's transactional pattern or behaviour

Significant changes in the customer's profile and account activity

Substantial changes in transaction values or volumes

Unusually large transactions

Carrying out of transactions in rapid succession



Transaction Monitoring Red Flags (cont.)

Spikes in deposits or withdrawals

Payments to/from unknown or unrelated third parties

Structuring of transactions to evade suspicion

Suspicious cash activity

Suspicious ATM activity and activity involving the use of bank cards

Transactions involving PEPs

Transactions involving high risk or non-reputable jurisdictions



Transaction Monitoring Red Flags (cont.)

Transactions involving individuals or entities subject to sanctions or named in adverse media

Transactions involving high risk products or services

Unexplained changes in transaction geography or parties involved

Incomplete, inadequate or inconsistent supporting information and/or documentation

Lack of rationale behind transactions in agreements or contracts

Generic explanations or statements for transactions that are not in line with the customer's profile



Case Studies – Credit Institutions

Based on real-life scenarios involving transaction monitoring breaches observed in credit institutions





Customer Background

Nationality: British

Residence: Malta

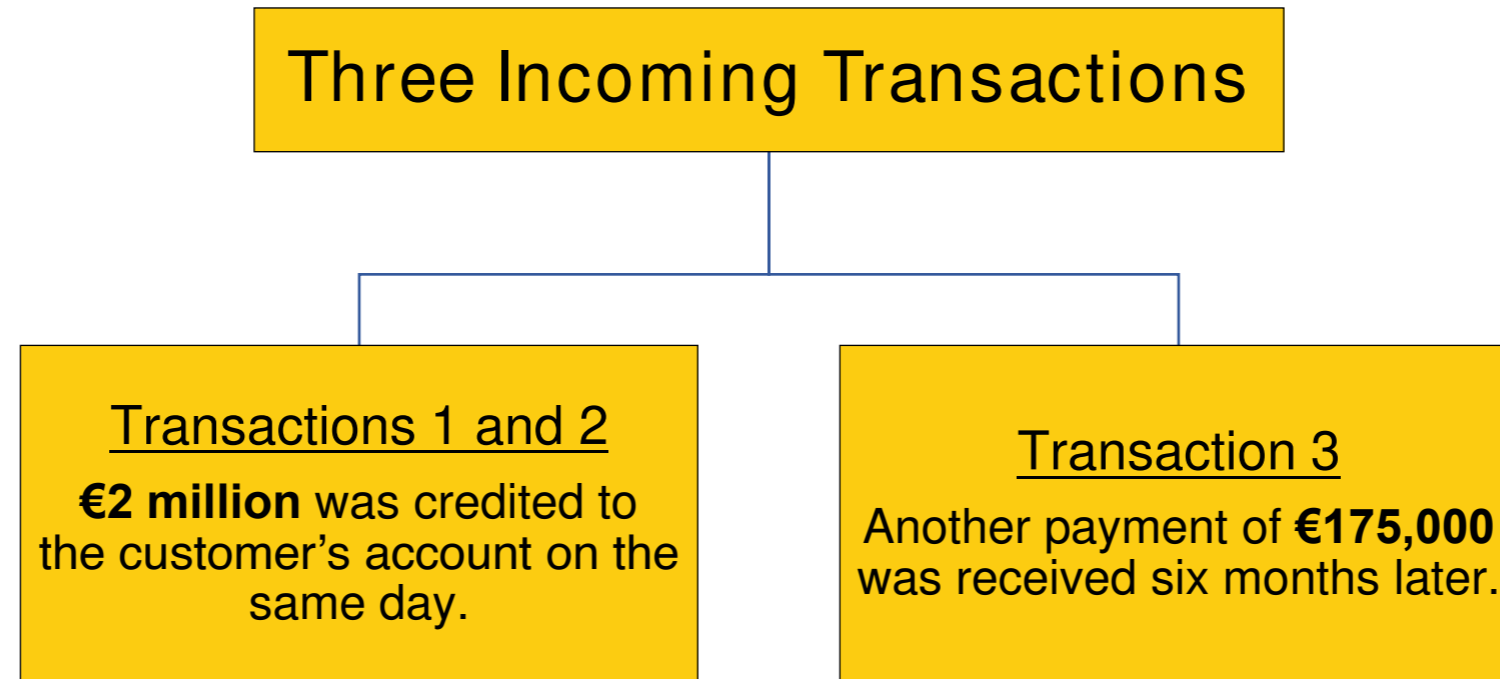
Occupation: Engineer

Declared Annual Income: < €75,000

Products: Term and deposit accounts



Incoming Payments:
Total of €2.2 million





Case Studies – Example 1a

Incoming Transactions 1 and 2 (€2 million)

Bank officials expressed concerns regarding these transactions and attempted to schedule a meeting with the customer for clarifications.

However, no further updates were provided to confirm whether the meeting took place, and if any additional supporting documents were eventually collected.



Incoming Transaction 3 (€175,000)

The Bank only obtained the basic payment details of the sender and beneficiary, which is inadequate for proper verification and scrutiny.





Key Takeaways

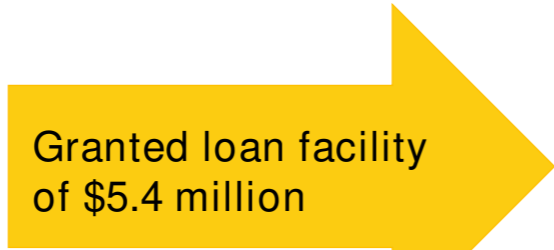
- The three incoming transactions were clearly inconsistent with the customer's business and risk profile, and greatly exceeded his declared anticipated annual income of approximately €75,000.
- Merely attempting to reach out to the customer is not sufficient if the Subject Person has concerns about one or more specific transactions. Thus, persistent follow-up is necessary to establish the rationale behind the transactions and obtain relevant documentary evidence.
- Subject Persons must collect adequate supporting documentation to justify transactions that appear to be unusual or suspicious, ascertaining that they understand their purpose and verify their legitimacy.
- Timely and appropriate action should be taken in cases involving unusual or suspicious transactions.



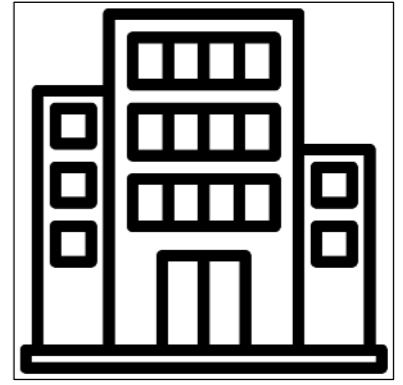
Case Studies – Example 1b



Subject Person



Holding Company



Unrelated Third Party



Property



Case Studies – Example 1b



At the time of the loan request, the customer maintained a balance of \$9.8 million with the Bank, while the total loan account, including interest payable, amounted to \$5.68 million. This means that the interest payable on the loan was equal to almost \$300,000.

The Bank proceeded to grant this loan on the basis that it was 100% cash collateralised without understanding the purpose of the loan and questioning the customer's need to borrow such a significant amount instead of utilising its own available funds.



Loan was fully repaid within seven months



Key Takeaways

- The short repayment timeframe, coupled with the fact that the customer had sufficient funds to cover the alleged property acquisition, raises strong suspicion that the loan was used to obscure the actual source and origin of the funds. Moreover, the loan being 100% cash collateralised is another red flag that should have prompted immediate action from the Bank.
- Prior to granting a loan facility, Subject Persons must establish the rationale of the transaction and obtain adequate supporting documentation, such as a loan agreement, to ascertain the legitimacy of the transaction.
- When the purpose of the transaction diverges from the anticipated business profile of the customer, this should trigger heightened scrutiny from the Subject Person. In this instance, the transaction's purpose was evidently not aligned with the customer's expected business activities and operations, which involved holding shares in several other companies.



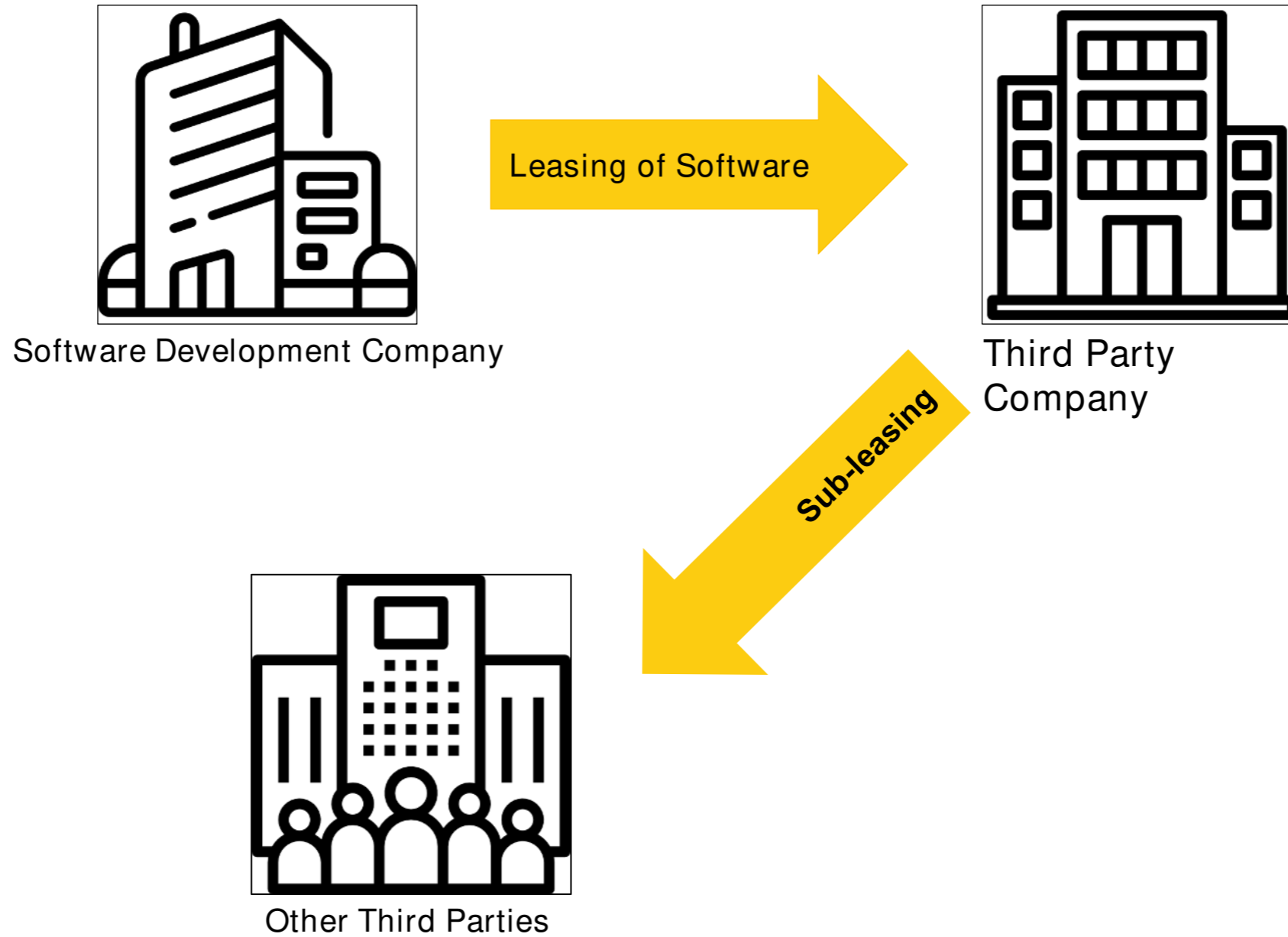
Case Studies – Financial Institutions


Based on real-life scenarios involving transaction monitoring breaches observed in financial institutions





Case Studies – Example 2a





Transactions

Over a period of 8 months, the customer received 9 payments totalling €3.7 million from the third party company.



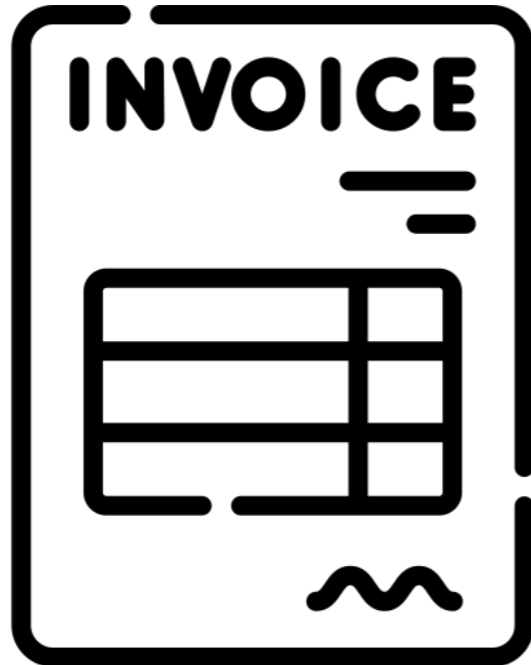
€50,000



€475,000

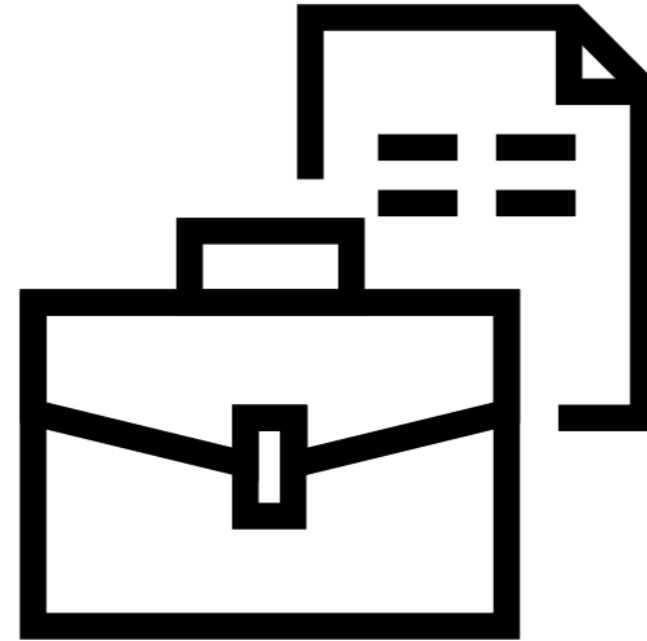


Case Studies – Example 2a



Invoices obtained for 3 out of the 9 transactions in question.

However, these lacked detail and did not contain information about the software being leased.



Licensing agreement collected did not include any details about the terms and conditions of payment.



Key Takeaways

- While SPs are not expected to obtain supporting documents for every transaction involved, they must have a comprehensive understanding of the customer's overall transactional activity and ensure that the transactions being executed are in line with the customer's business and risk profile.
- Any invoices collected should explicitly pertain to the transactions in question and provide sufficient detail about them.
- A contractual arrangement between the customer and another third party needs to be substantiated through a formalised agreement that outlines the terms and conditions of payment, including specific amounts due.
- Subject persons are required to question higher value transactions and obtain additional documentary evidence to confirm that they are legitimate and make economic sense.



Customer Background

Nationality: Indian

Residence: Malta

Occupation: Pensioner

Previous employment income:
\$50,000

Declared SOW/SOF: Savings and
pension



Over \$540,000 remitted over 3
years
No supporting documentation
obtained



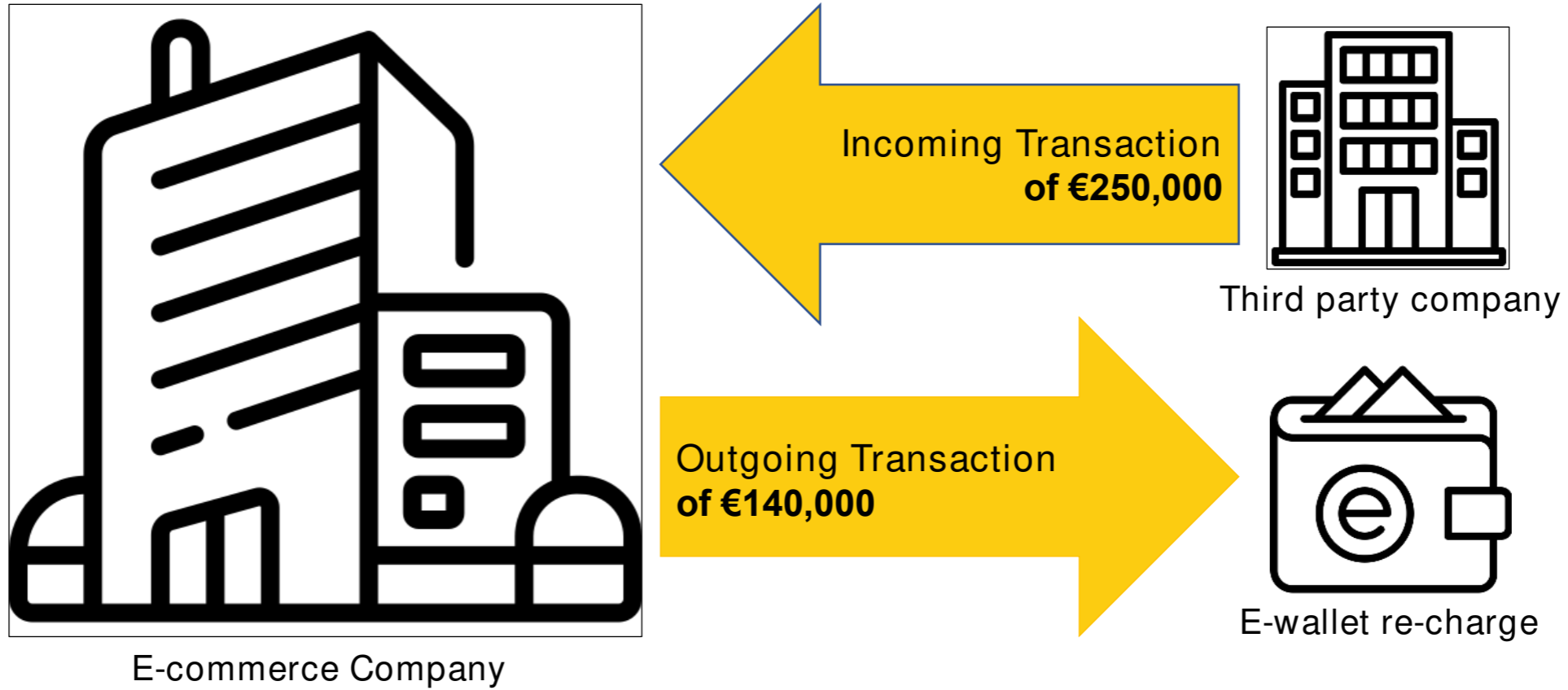


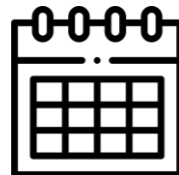
Key Takeaways

- In this case, the Subject Person was required to question the purpose of the remitted funds, particularly when considering the higher risks associated with the jurisdictions involved, and the significant cumulative value of the transactions.
- The large remittance amount involved and the lack of documentary evidence collected raises concerns regarding the credibility and legitimacy of the customer's financial claims, necessitating further investigation.
- While the customer's activities may potentially have had legitimate justifications, relying solely on the **customer's** statements is insufficient, especially in light of the higher risk factors present.



Case Studies – Example 2c

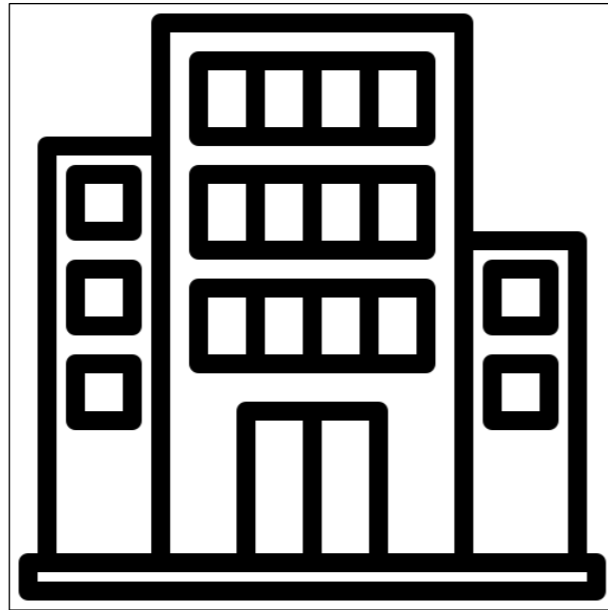


 Both transactions occurred on the same day



Case Studies – Example 2c

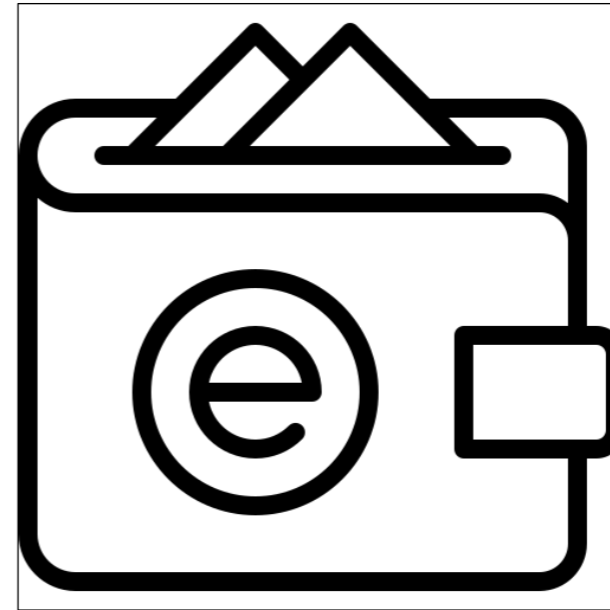
Incoming Transaction



Payment received from a third party company that was also a client of the Company.

No supporting documentation obtained despite the presence of adverse media.

Outgoing Transaction



Limited information available for this transaction, with only a brief description indicating that it was a e-wallet re-charge.

The Company claimed that the amount represents payment for services rendered (marketing).



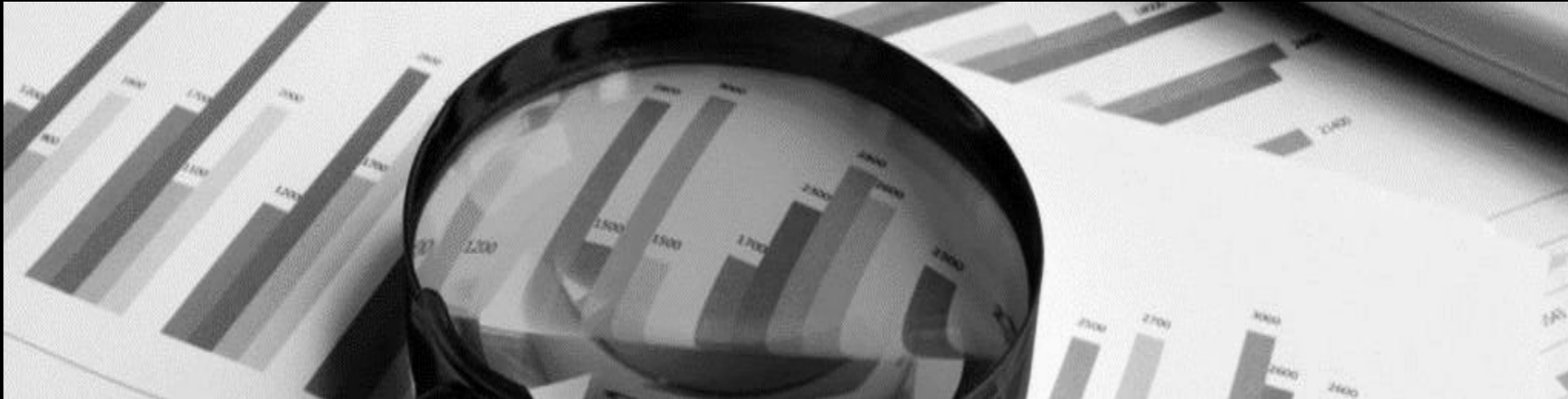
Key Takeaways

- If any party to a transaction is named in adverse media reports, the Subject Person must investigate and seek clarifications before processing further transactions.
- In cases where the transacting party is also the client of the Subject Person, the Subject Person is expected, at a minimum, to establish the nature of the relationship between its two customers, and ascertain the purpose of the transaction.
- The payment description should accurately reflect the nature of the transaction based on the Subject Person's understanding. Any discrepancies or inconsistencies between such understanding or the explanations provided and the actual nature of the transaction could raise concerns.



Transaction Monitoring Systems, Alerts Management, Adequate Resources and Training





Automated transaction monitoring

- ✓ Specialized software or systems to analyze transactional data and detect suspicious patterns or anomalies

Manual transaction monitoring

- ✓ Human analysts reviewing individual transactions and conducting investigations to identify any suspicious activity



Transaction Monitoring Systems



Transaction monitoring using AI and machine learning tools may allow regulated entities to carry out traditional functions with greater speed, accuracy and efficiency (provided the machine is adequately and accurately trained). The use of new technologies for monitoring purposes should, for the most part, continue to be integrated with the broader monitoring systems which include an element of human analysis for specific alerts or areas of higher risk. These systems must also improve their degree of explainability and auditability in order to fully comply with supervisory requirements.

Opportunities and Challenges of New Technologies for AML/CFT – FATF, July 2021



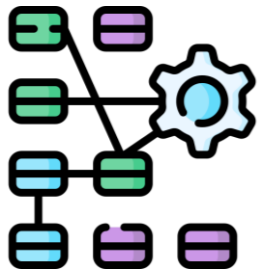
Transaction Monitoring Systems

- It is not a legal requirement to have an automated system in place
- HOWEVER, subject persons which are processing hundreds of transactions regularly are expected to demonstrate that they can scrutinise transactions effectively and efficiently
- There can be instances where the subject persons may demonstrate that even though it is processing a certain amount of transactions, it is still able to conduct transaction monitoring manually.



Transaction Monitoring Systems

There are various factors which should aid a subject person in determining whether to implement an automated transaction monitoring system including –



The complexity of the SP's business model



Whether the system is able to cater for new ML/FT trends



The number of transactions executed on a daily basis



Whether the system is able to generate reports



Transaction Monitoring Systems – Case Study A

Volume of
retail and
non-retail
deposits

- Retail deposits exceeding 150,000
- Non-retail deposits exceeding 500,000

Value of
retail and
non-retail
deposits

- Retail deposits exceeding €500mIn
- Non-retail deposits exceeding €990mIn



Transaction Monitoring Systems – Case Study A (Cont'd)

- Credit institution processing transactions of a high volume and value.
- The transaction monitoring system of the Bank was implemented in 2021 and the compliance examination was performed in 2020.
- Whilst the Bank was commended for implementing a TM system, the fact that the Bank had not adopted this system beforehand meant that it was not monitoring transactions in an efficient manner at the time of the compliance review.





Transaction Monitoring Systems – Case Study B

Volume of
retail and
non-retail
deposits

- Retail deposits exceeding 450,000
- Non-retail deposits exceeding 200,000

Value of
retail and
non-retail
deposits

- Retail deposits exceeding €500mln
- Non-retail deposits exceeding €990mln



Transaction Monitoring Systems – Case Study B (Cont'd)

- The Bank relied on the manual scrutiny performed by cashiers and post-transaction monitoring through weekly generated reports.
- Therefore, the transaction monitoring performed by the Bank was inadequate and the Bank was found in breach of its obligations.





Transaction Monitoring Systems – Case Study C

The Bank was performing transaction monitoring manually rather than through an automated system. The Compliance Team was analysing each transaction one by one, and any suspicious transactions were flagged to the MLRO.



The Bank's officials were reviewing approximately 30 transactions per day at the time of the examination.





Transaction Monitoring Systems

Issues which may arise with TM systems

False positives

Large number of cases which do not warrant review

May create a backlog and lead to legitimate cases not being reviewed





Transaction Monitoring Systems

Issues which may arise with TM systems



One size fits all approach

Applying the same transaction monitoring rules to different customers

May also give rise to false positive alerts over time



Transaction Monitoring Systems

Issues which may arise with TM systems

Limited scenarios

Scenarios do not cover a wide range of suspicious activities

Certain ML/FT red flags may go undetected





Alerts Management



When an alert is generated by a transaction monitoring system, it is expected that SPs have the adequate processes for the notification, handling and recording of alerts, as well as the actions taken in relation to such alerts.



Alerts Management

Why is alert management essential?



Detection of Suspicious Activities:

- AML systems generate alerts based on predefined rules and algorithms that flag potentially suspicious transactions or patterns.
- Effective alert management ensures that these alerts are promptly reviewed and investigated, helping to detect and prevent illicit activities.



Compliance with Regulatory Requirements:

- Subject persons are expected to demonstrate robust alert management processes to promptly identify and report suspicious transactions.



Alerts Management

Why is alert management essential?



Risk Mitigation:

- Money laundering and terrorist financing pose significant risks to the integrity of the financial system.
- Effective alert management helps mitigate these risks by identifying and preventing illicit activities.



Operational Efficiency:

- Efficient alert management processes enable financial institutions to handle large volumes of alerts effectively.
- By employing automated technologies, data analytics, and risk-based approaches, institutions can streamline their alert management workflows.



Alerts Management

Why is alert management essential?



Enhanced Due Diligence:

- The investigation of alerts on a particular customer enables the subject person to gain a deeper understanding of the customer.
- Such information can contribute to an increase in customer due diligence, including the carrying out of enhanced due diligence.



Alerts Management – Case Study

- Credit institution processing transactions of a high volume and value
- Despite this, no alerts were generated by the Bank's systems
- Since the compliance review, a fine tuning exercise had been performed by the Bank nonetheless, this did not justify the Bank's failure to scrutinise the transaction – the fact that an alert would have now been generated does not excuse the Bank



Alerts Management – Case Study

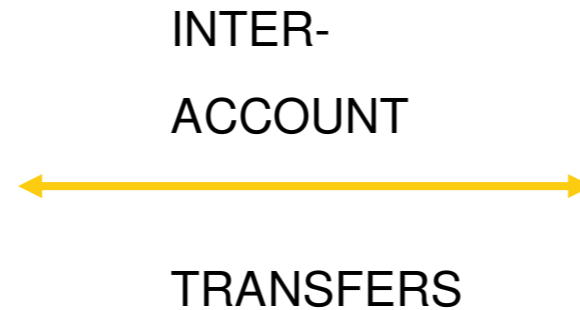


Transaction of over
€4mIn

- ⊗ No information or documentation collected
- ⊗ Turnover of €1 million
- ⊗ Beneficial owner was similar to that of another customer which was linked to adverse media
- ⊗ Involvement of high-risk jurisdictions
- ⊗ Customer was also linked to a money laundering racket and subject to an administrative penalty by a regulator



Alerts Management – Case Study



- Over 300,000 transactions
- Period of two and a half years
- Transactions ranging up to €1million



No alerts raised
No supporting documentation collected
No blocked transactions
No suspicious reports submitted to FIAU



Alerts Management

Pointers to keep in mind when managing alerts –



Alerts are to be cleared in a reasonable timeframe

Timely Detection and Prevention of ML/FT: If there are reasonable grounds to suspect that ML/FT has occurred or is occurring or may occur, then the subject person is expected to submit the relative suspicious report to the FIAU's Intelligence Section.

If alerts are not cleared immediately, they could result in ML/FT being undetected or prevented



Alerts Management

Pointers to keep in mind when managing alerts –



Necessary information and documentation, where required, is to be requested

Effective alert management systems would enable the SP to focus on a patterns of activity and carry out the necessary due diligence on that particular customer as required.

It is essential that when obtaining documentation and information from the customer, this is analysed in a thorough manner and not simply collected for the sake of obtaining additional information.



Alerts Management

Pointers to keep in mind when managing alerts –



An audit trail of alerts raised by the system is to be maintained at all times, as per Section 4.5.2.3 of the Implementing Procedures

An audit trail provides a detailed record of all transactions, activities, and decisions made within the system.

It enables investigators to trace the flow of funds, identify suspicious patterns, and determine the individuals or entities involved.



Alerts Management – Case Study



A financial institution failed to retain a record of the rationale behind discounted alerts. The Committee found this matter to be concerning. It noted that in the event of similar instances in the future, the Company's officials would not be able to understand the rationale behind its' discounting.



Alerts Management – Case Study

The Company did not provide evidence of investigations performed to ensure that the alerted transactions were not suspicious.

→ Outward transactions over €100,000 which were alerted were not investigated by the financial institution



OUTWARD
PAYMENT → € 100,000

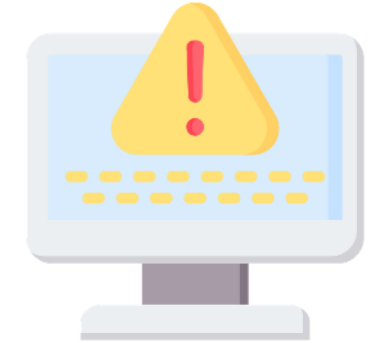
- User accumulates EUR 250,000 in 7 days
- User with 3 previous rejected deposits rules
- User with a high-risk scoring

→ The Company stated that supporting documentation had been provided however this was not found on file during the compliance examination



Alerts Management – Case Study

→ Outward transaction around €410,000 which was alerted was not adequately investigated by the financial institution



OUTWARD
PAYMENT → € 410,000

- Pay out larger than EUR75,000
- Account age is less than 180 days
- User accumulates EUR 250,000 in 7 days
- High risk score

→ The Company stated that supporting documentation had been provided however this was not found on file during the compliance examination



Adequate Resources and Training

- Subject persons should have sufficient resources, including an adequate and efficient IT infrastructure to perform transaction monitoring in a timely manner

- The necessary guidance to staff members is to be provided on –
 - ✓ Transaction monitoring itself
 - ✓ How the system works
 - ✓ How escalations to the MLRO are to be made
 - ✓ Updates to AML/CFT legislation
 - ✓ Current/upcoming ML/FT risks and typologies





Adequate Resources and Training – Case Study (1)



Identify suspicious transaction(s) through live monitoring, post-transaction monitoring and periodic reviews



Evaluate whether to investigate in extensive detail the suspicious transaction(s)



Escalate to the MLRO either to re-evaluate the risk rating, to monitor the relationship, or to close the relationship completely

