Post-event transaction monitoring process for banks

Guidance

DeNederlandscheBank

EUROSYSTEEM

30 August 2017

PO Box 98, 1000 AB Amsterdam
+31 20 524 91 11 – info@dnb.nl
www.dnb.nl

Contents

1 Introduction

1.1 What is the purpose of this guidance document?

Financial and economic crime is a major problem in our contemporary society. Headlines in the media show how society has unwittingly fallen victim to this form of crime. Take for example, the Panama Papers and the terrorist attacks in Western Europe. Financial institutions, including banks, play a key role in preventing money laundering and terrorist financing. Their actions in this respect include conducting customer due diligences (CDD) and monitoring customer transactions to identify unusual transactions. This guidance focuses on the latter, transaction monitoring.

2A bank can only intervene in good time when a potentially unusual transaction is made or a notifiable transaction pattern occurs, if it adequately monitors transactions. The bank should investigate these cases further and report them if necessary. Failure to ensure adequate monitoring may result in a bank inadvertently cooperating in terrorist financing or in money laundering.

As gatekeepers for the Dutch financial system, banks are expected to adequately and continuously monitor transactions, and to stay alert. There are statutory requirements which banks must meet in this regard, and it is our task to supervise compliance with these rules and regulations. All banks are therefore obliged to conduct transaction monitoring, although this obligation and its supervision is principle-based. This means that the practical interpretation of this requirements is not prescribed in detail by laws and regulations, or by the supervisory authority. It is up to you as a bank to determine how exactly you interpret this. The supervisory authority will assess the result.

Transaction monitoring is not new for banks. The areas of concern and the examples presented in this document serve as a supplement to prevailing laws and regulations and the previously published guidances on this subject such as the DNB Guidance on the *Wwft* and SW;[1] DNB Guidance on the Anti-Money Laundering and Anti-Terrorist Financing, preventing the misuse of the financial system for money laundering and terrorist financing purposes and controlling integrity risks, and the Q&A Assessment of Ongoing Due Diligence Process (*Wwft* and *SW*) of December 2013.

1 *Wwft:* Anti-Money Laundering and Anti-Terrorist Financing Act *(Wet ter voorkoming van witwassen en het financieren van terrorisme)*, SW: 1977 Sanctions Act.

1.2 About this document

This document provides you with guidance on how to set up and improve your transaction monitoring process. In preparing this guidance we have made use of the most important findings from the thematic examination conducted in 2016 "Post-event transaction monitoring process for banks".[2] Given the ongoing terrorist threat in the Netherlands and Europe, this examination focussed specifically on transaction monitoring in relation to terrorist financing risks, which is why we have included specific good practices on this subject in this document. When developing solutions and measures you should of course take into account your institution's own circumstances. You have to make your own considerations in this respect.

This document provides an overview of the statutory requirements that banks must fulfil, and how we envisage compliance with transaction monitoring in accordance with international standards and good practices. We expect the sector to take due notice of this, and where necessary improve its business management.

This document is structured as follows: In Chapter 2 we present a diagram of what a transaction monitoring process can look like. This chapter also includes the maturity model that we used in our 2016 examination. Chapter 3 describes the good practices for each element of this model and examples of what not to do. We have included a glossary at the end of this document.

2 The transaction monitoring theme was the subject of a cross-sectoral examination conducted in various sectors (four banks, four payment institutions, three money transfer offices, and six trust offices). Comparable guidances have been prepared for the other sectors.

2 Summary

Transaction monitoring is an essential measure for reporting unusual transactions to the Financial Intelligence Unit – Netherlands (FIU-NL), to control integrity risks in the area of money laundering and terrorist financing.

This entails the following:

1. Banks must ensure the transaction monitoring process reflects the risks of money laundering and terrorist financing that emerge from the SIRA. When determining the risk profile for a customer and or "customer peer groups" banks must also include expected transaction behaviour.
2. Banks must have developed sufficient policy for transaction monitoring and have adequately elaborated this policy in underlying procedures and operating processes.
3. Banks must have an (automated) transaction monitoring system in place and have a substantiated and adequate set of business rules (detection rules with scenarios and threshold values) to detect money laundering and terrorist financing. Banks must periodically test these business rules, in terms of both technical aspects and effectiveness.
4. Banks must have an adequate process for notification and dealing with alerts. Banks must ensure they fully and immediately notify FIU-NL of executed or proposed unusual transactions. In this process, for each alert considerations and conclusions are documented underlying decisions to close or escalate an alert.
5. Banks must have structured their governance with regard to transaction monitoring in such a way that there is clear segregation of duties, for example through the three lines of defence model.
6. Banks must offer their staff tailored training programmes. Staff must be aware of the risks of money laundering and terrorist financing.

3 Legal context and scope

3.1 Transaction monitoring: statutory obligation for continuous monitoring

Banks have a statutory obligation to take measures to counter money laundering and terrorist financing. In this respect they must pay particular attention to unusual transaction patterns and transactions of customers that due to their nature typically carry a higher risk of money laundering or terrorist financing. If there are grounds to assume that a (proposed) transaction is linked to money laundering or terrorist financing, banks must report this transaction to the FIU-NL[3] without delay. To be able to this it is crucial that banks have in place an effective transaction monitoring process.[4]

With reference to the DNB Guidance on the *Wwft* and *Sw*, we confirm the following[5]: as the *Wft* (ethical operational management) and the *Wwft* are focused on the same objective, the procedures a bank uses for the implementation of the *Wft* and the *Wwft* can be integrated so that the requirements under the two Acts can be met in the same manner. Measures to combat money laundering and terrorist financing, based on the *Wft* are set out in greater detail in the *Wwft*. The principal goal remains that banks should know who they are doing business with and for what purpose the business relationship is used.

In order to exercise adequate continuous monitoring, banks must pursuant to Section 10 of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft – Bpr*) conduct a systematic integrity risk analysis (SIRA). Integrity risks are defined here as the "threat to the reputation of, or the current or future threat to the capital or the results of a financial institution due to insufficient compliance with the rules that are in force under or pursuant to the law."[6] This therefore includes risks of money laundering and terrorist financing. If on the basis of the SIRA a bank notes any new or residual risks, it must address these in adequate policies, procedures and measures.

Specifically with regard to risks relating to money laundering and terrorist financing, under the Anti-Money Laundering and Anti-Terrorist Financing Act *(Wwft)* banks must carry our checks on their customers.[7] This must include establishing the purpose and the intended nature of the business relationship. They are also obliged to monitor the business relationship and the transactions conducted for the duration of that relationship on an ongoing basis.[8] This way banks can ensure that the transactions conducted correspond to the knowledge they have of their customers and their risk profiles, where necessary investigating the

3 For the sake of brevity, referred to hereinafter as "unusual transactions".

4 Section 14(4) of the Decree on Prudential Rules for Financial Undertakings *(Besluit prudentiële regels Wft – Bpr)* and Sections 2a(1) and (3) under d, of the *Wwft*.

5 See page 7 of this Guidance.

6 Section 1 of the *Bpr*.

7 Sections 2a(1) and 3(1) of the *Wwft*.

8 Section 1(1), under m, of the *Wwft* defines a transaction as follows: "an act or a combination of acts performed by or on behalf of a customer of which the institution has taken note in the provision of its services to that customer."

origin of the funds used in the relevant business relationships or transactions.[9] We understand that it is not always possible to draw up individual risk profiles for each customer in advance, given the large number of customers in specific segments, e.g. banking services for private individuals or smaller SMEs. In order to take a more practical approach, banks can categorise their business relations according to peer groups, for example. Peer groups can be defined on the basis of a number of customer characteristics, for example sectors, country of incorporation, legal form, countries in which the customer is active, etc.

The term "continuous monitoring" is a key aspect in the process of the transaction monitoring and banks can interpret it according to their risk-based approach. In this regard risk-based is intended to mean that they will devote most attention to the largest risks they have identified. They must always be able to substantiate this risk-based approach on the basis of the results of the integrity risk analysis. Banks are expected to have a system in place for monitoring transactions and generating alerts for potentially unusual transaction patterns and transactions for further processing. In order to be able to identify such transaction patterns and transactions, they are expected to identify red flags and describe them in business rules. in this process they should focus especially on non-standard transaction patterns, including unusual transactions and transactions that by their nature entail increased risk of money laundering or terrorist financing.[10]

Executed or proposed unusual transactions must be reported to the FIU-NL without delay upon their unusual nature becoming known.[11] This means that banks must therefore also have specific procedures and operational processes in place to assess and process transaction alerts and provide notification of unusual transactions.[12] In order to safeguard these procedures and measures, banks must ensure their staff are familiar with the provisions of the *Wwft* to the extent relevant for the performance of their duties, and that they are trained on a regular basis. This should enable them to carry out thorough customer due diligence and to recognise and report unusual transactions.[13]

9 Section 3(2), under d, of the *Wwft*.
10 Section 2a(1) of the *Wwft*.
11 Section 16 of the *Wwft*.
12 Section 16 of the *Wwft* in conjunction with Sections 17 and 18 of the Decree on Prudential Rules for Financial Undertakings (Besluit prudentiële regels - *Bpr*).
13 Section 35 of the *Wwft*.

3.2 Scope of guidance

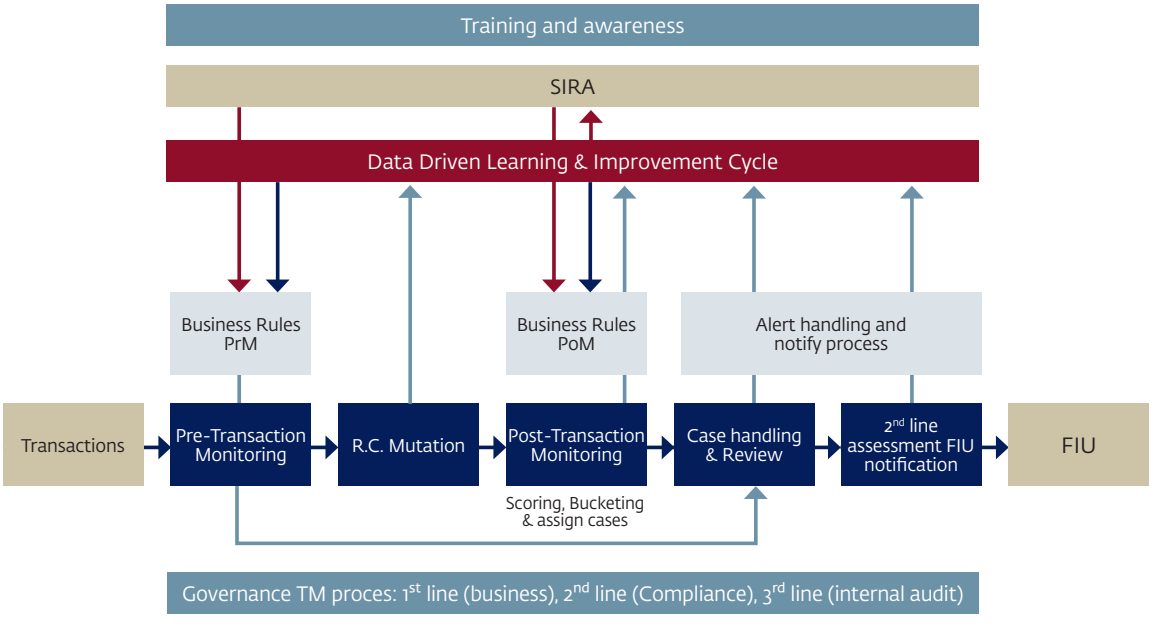
This guidance applies to the following: Banks having their registered offices in the Netherlands, as defined in Section 1(1) of the *Wwft*; branches of foreign banks having their registered offices in the Netherlands as defined in Section 1(1) of the *Wwft*; internationally operating banks as meant in Section 2(1) of the *Wwft*. In other words, if these banks have branches or subsidiaries in a state that is not a EU/EEA Member State, these branches or subsidiaries must structure their transaction monitoring process in accordance with the *Wwft* requirements.

4 Transaction monitoring

4.1 The transaction monitoring process

The transaction monitoring process can appear as follows:

Figure 1 The transaction monitoring process



Transaction monitoring can be conducted in various ways. As shown in the diagram it is possible to have pre-transaction monitoring[14] and post-event transaction monitoring, in other words transactions can be monitored both beforehand and afterwards.

Pre-transaction monitoring

Pre-transaction monitoring is carried out before effecting the transaction, and mainly applies to situations of face-to-face contact between the customer and the bank employee. For example when a customer visits a bank to exchange a quantity of banknotes in certain denominations or foreign currency, or to make a cash deposit. Another example is trade finance, in which a bank is expected to carry out a specific proposed transaction. In the case of post-event transaction monitoring the transaction has already been carried out by the bank and transaction monitoring occurs afterwards.

We stress that banks should also have a pre-transaction monitoring process in place, with appropriate measures to detect unusual transactions when or preferably before they are conducted.

We believe pre-transaction monitoring, either as an automated or a manual process, can effectively contribute to the detection of unusual transactions as it is in this stage that actual customer contact takes place. As such, the front office has a substantial responsibility in detecting unusual transactions such as money laundering and terrorist financing. This is relevant when a clear profile of expected transactions is drawn up at the start of the customer relationship for monitoring purposes. This will allow the institution to detect unusual proposed transactions even before they are effected, and notify them to FIU-NL without delay.

Good practice

A bank notes that a requested transaction from its Trade Finance Services department relates to products that differ from the customer's regular business. The transaction is put on hold and reported to the MLRO.[15] Further inquiry reveals that the customer has shifted its business to a new market. The customer is asked to submit documentary evidence, which is then presented to the MLRO. The MLRO approves the transaction, after which it is effected.

14 In the case of post-event transaction monitoring the transaction has already been carried out by the institution and transaction monitoring occurs retrospectively, while in the case of pre-transaction monitoring the transaction has not yet been carried out.

15 MLRO means Money Laundering Reporting Officer, a second-line function.

Post-event transaction monitoring

This guidance document describes the post-event transaction monitoring process, because banks are primarily able, based on non-cash settlement of transactions, to detect money laundering and terrorist financing risks in this manner.

Customer due diligence is part of the transaction monitoring process. Customer due diligence provides banks with knowledge of its customers, including the purpose and intended nature of the business relationship with the customer. This knowledge enables the bank to conduct risk based assessments to ascertain whether the transactions carried out have unusual patterns that could indicate money laundering or terrorist financing. The bank must tailor its transaction monitoring to the type of customer, the type of services provided and the risk profile of the customer or customer segment. This means monitoring can have a different set-up for the various customer segments and products to which the bank provides its services.

Step 1: risk identification

The first step in the transaction monitoring process is risk identification. During the identification process a bank must systematically analyse the money laundering and terrorist financing risks that particular customers, products, distribution channels or transactions pose. The bank then documents the results of this analysis in the SIRA. The SIRA is applied to policy, business processes and procedures relating to transaction monitoring. A bank may have various SIRAs, for example a separate SIRA for subsidiaries or a SIRA for each business line. A bank must document how it translates the results of the SIRA, as well as the resulting processes and procedures themselves.

When identifying and analysing risks, a bank must classify its customers in various risk categories, such as high, medium and low, based on the money laundering and terrorist finance risks attached to the business relationship with the customer. To determine the customer's risk profile, a bank should prepare a transaction profile based on expected transactions or expected use of the customer's (or customer group's) account.[16] By preparing a transaction profile in this way (through peer grouping) a bank can sufficiently monitor transactions conducted throughout the duration of the relationship to ensure they are consistent with its knowledge of the customer and their risk profile. By identifying the expected transaction behaviour of their customer, a bank can assess whether the transactions the customer carries out are consistent with its knowledge of the customer.

16 For further information on how institutions can do this, please refer to our Guidance on the *Wwft* and *SW*.

A feasible transaction profile in any case meets the following six criteria:

1 Current: the transaction profile is up-to-date and is dated. All relevant changes to the profile are made promptly.
2 Complete: the transaction profile contains all bank account numbers, names of beneficiaries and authorised representatives.
3 Specific: the expected items and money flows are clearly described in terms of e.g. amounts, services and frequency. The (threshold) amounts indicated are well-substantiated and can actually contribute to recognising unusual transactions.
4 Clear: financial flows are represented in clear and simple diagrams.
5 Substantiated: the transaction profile is substantiated with relevant documents clarifying and explaining the forecast financial flows.
6 Documented: the transaction profile is documented in the customer file.

Step 2: detection of patterns and transactions

For the second step, detecting the unusual transaction patterns and transactions that may indicate money laundering or terrorist financing, a bank must have a transaction monitoring system in place. Before making use of such a system the bank should ensure that all data are fully and correctly included in the transaction monitoring process. This can be data concerning the customer, the services and the transactions. If there are large numbers of transactions then it is appropriate to have an automated transaction monitoring system in place to be able to safeguard the effectiveness, consistency and processing time of the monitoring.

The system must at least include pre-defined business rules: detection rules in the form of scenarios and threshold values. In addition to this, more advanced systems may also be needed, and in applicable cases may be essential, depending on the nature and the size of the transactions and the nature of the institution in question. So for example, a highly advanced system would be less necessary for a bank with a limited number of simple transactions. It may also be the case that a bank considers the use of a highly advanced system, which makes use of artificial intelligence (AI) for example, to be essential.[17]

In any case, the responsibility for effectively detecting unusual transactions remains with the bank. A bank must have a good understanding of its systems, and should not just rely on the algorithms provided by external suppliers. When opting for an AI-based system, it may therefore be advisable to involve staff with relevant expertise.

17 The application of artificial intelligence involves the computer itself learning to recognise specific patterns based on a pattern recognition or cluster algorithm. An algorithm is a method used to calculate certain quantities and functions.

Step 3: data analysis

A bank should analyse its transaction data using its transaction monitoring system and relevant intelligent software. The system generates alerts on the basis of business rules. An alert is a signal that indicates a potentially unusual transaction. Any alerts are investigated. The findings of this investigation must be adequately and clearly recorded. When the findings of the investigation reveal that the transaction is unusual, the bank must notify this to FIU-NL without delay. A bank must have sufficiently described and documented the considerations and decision-making process as to whether or not to report a transaction. When a bank fails to meet its notification duty – even if this is not deliberate – it constitutes an economic offence.

Step 4: assessment, measures and documentation

The bank must then assess the consequences of the notification to FIU-NL and a possible feedback report from FIU-NL for the customer's risk profile and determine whether any additional control measures have to be taken. The final part of the transaction monitoring process is to ensure all the details of the process are properly recorded. In this connection, the bank keeps the data relating to the notification of the unusual transaction and records them in readily accessible form for five years after the notification was made, allowing the transaction to be reconstructed.

4.2 Maturity model

When conducting the thematic examination (post-event) transaction monitoring at payment service providers, we used a maturity model we had developed ourselves for transaction monitoring. This model takes into consideration the relevant *Wft* and *Wwft* requirements and is intended to indicate where a bank is in the transaction monitoring process with regard to maturity. In this model the degree of compliance in six areas is assessed according to a four-point colour-coded scale:

- Red: completely non-compliant
- Orange: insufficiently compliant
- Yellow: sufficiently compliant
- Green: best practice

Banks can use this maturity model to determine their own ambitions, while ensuring they achieve a "yellow" score as a minimum. The level of ambition is dependent on the bank's risk profile. A yellow score means that a bank complies with the minimum statutory requirements (sufficiently compliant).

The figure below provides a further elaboration of the maturity model for the post-event transaction monitoring, including the possible scores for the six areas of assessment.

Section 5 of this guidance presents our outcomes and examples (good practices and not so good examples of interpretation of the standard.
The good practices illustrate how banks have been able to achieve a yellow or green score in that area.

Figure 2 maturity model for (post-event) transaction monitoring

1 SIRA/risk profile	2 Design of AML/CFT policy and procedures	3 TM system/ business rules
■ SIRA not conducted ■ No customer risk profiles	■ No transaction monitoring policy or procedures	■ No system in place for transaction monitoring commensurate with the institution's risk profile ■ No AML/CFT indicators or business rules to recognise unusual transactions
■ A SIRA has been conducted, but its scenarios and risks lack sufficient depth ■ Scenarios and risks in the SIRA have not been translated into transaction monitoring policy and procedures ■ There are customer risk profiles, but no ex ante transaction risk profiles	■ Institution has designed transaction monitoring policy and procedures, but they are too general and insufficiently detailed, so that material aspects are lacking	■ System for transaction monitoring insufficiently matches the institution's risk profile ■ Institution uses a limited number of AML/CFT indicators and business rules to recognise unusual transactions
■ A SIRA with sufficiently challenging scenarios and risks has been conducted ■ Scenarios and risks in the SIRA have been sufficiently translated to transaction monitoring policy and procedures, but only at a general level ■ Institution has categorised customers according to groups of transaction risk profiles	■ Transaction monitoring policy and procedures have been designed and are in existence. They have been sufficiently worked out and contain material aspects ■ Institution is able to monitor transactions in a proper, timely and complete manner using the framework	■ System for transaction monitoring sufficiently matches the institution's risk profile ■ The institution uses a complete set of AML/CFT indicators and business rules (including red flags and modus operandi) to recognise unusual transactions ■ The institution uses backtesting in the periodic assessment of its business rules ■ Changes to the system and business rules with respect to money laundering and terrorist financing are reactive
■ Scenarios and risks in the SIRA accurately and fully reflect the institution's specific risk profile ■ Moreover, the SIRA is continuously adjusted to reflect developments in the area of money laundering and terrorist financing ■ SIRA forms the basis for the periodic updates of the transaction monitoring framework ■ Detailed ex ante transaction risk profiles	■ Transaction monitoring policy and procedures have been demonstrably incorporated in the institution's work process and their operating effectiveness has been demonstrated ■ Transaction monitoring policy and procedures are up to date and fully aligned with the most recent developments in the area of money laundering and terrorist financing ■ Active cooperation and consultation on policy with other financial institutions	■ Institution has an automated and self-learning transaction monitoring system commensurate with its risk profile ■ Institution is pro-active towards developments in money laundering and terrorist financing, i.e. in its adjustments to system and business rules ■ Institution uses backtesting when introducing new AML/CFT indicators and business rules ■ Structural use of pattern recognition and network analyses to recognise unusual transactions

4 Alerts processing and notification process	5 Governance: 1st, 2nd and 3rd line	6 Training en awareness
■ No alerts processing or unusual transactions notification processes defined ■ Processing of transaction monitoring alerts is not laid down or followed up ■ (Intended) unusual transactions are generally not immediately reported to FIU	■ No segregation of duties between 1st, 2nd and 3rd lines ■ Responsibilities of 1st, 2nd and 3rd line have not been described ■ No second line monitoring ■ No independent internal control ■ Periodic management information about TM results unavailable	■ Relevant employees have no knowledge or awareness of money laundering and/or terrorist financing risks or controls ■ No training available in the area of AML/CFT
■ Alerts processing and unusual transactions notification processes are capacity-driven rather than risk-based ■ Alerts processing is insufficiently recorded (no considerations/ conclusions) and there is no follow-up ■ (Intended) unusual transactions are incidentally (immediately) reported to FIU	■ Segregation of duties for 1st, 2nd and 3rd line has been designed ■ Inadequate description of responsibilities of 1st, 2nd and 3rd line ■ Second line monitoring (SLM) and independent internal control has been designed, but its operating effectiveness is insufficient in terms of frequency and/ or quality (SLM programme, checks performed, reporting) ■ Periodical management information about TM results are available to a limited degree	■ Employees have insufficient knowledge or awareness of money laundering and/or terrorist financing risks or controls ■ Incidental training sessions in the area of AML/CFT (only reactive, for instance in response to audit findings or incidents). Their content lacks quality (absence of material elements)
■ Alerts processing and unusual transactions notification processes have been sufficiently defined, including escalation to the 2nd line ■ Processing of transaction monitoring alerts is laid down and followed up ■ (Intended) unusual transactions are immediately reported to FIU	■ Segregation of duties for 1st, 2nd and 3rd line has been designed and is in place ■ Responsibilities of 1st, 2nd and 3rd line are adequately described ■ Second line monitoring and independent internal control have been designed and exist. Their frequency and quality are adequate (suboptimal operating effectiveness) ■ Findings from 2nd and 3rd line monitoring activities are adequately followed up by the 1st line (reactive) ■ Management information about results is adequate, in essence providing direction	■ Employees and senior management have sufficient knowledge and awareness of money laundering and/or terrorist financing risks and controls ■ Training programme has been designed based on distinctive levels in the organisation (from management to staff member) ■ Obligatory and optional training sessions on AML/CFT are offered periodically, their quality is sufficient and they contain material elements
■ Alerts processing and money laundering notification processes have been defined and the institution is pro-active towards developments in money laundering and terrorist financing ■ Processing of transaction monitoring alerts is consequently documented and followed up ■ Institution acts as a fully-fledged discussion partner of the investigative authorities and chain partners	■ Segregation of duties has been designed and exists for 1st, 2nd and 3rd line and its operating effectiveness has been demonstrated ■ Responsibilities of 1st , 2nd and 3rd line have been described clearly and completely and 1st line pro-actively takes final responsibility for transaction monitoring ■ High-quality second line monitoring is conducted very frequently (operating effectiveness) ■ High-quality independent internal checks of transaction monitoring take place regularly (operating effectiveness) ■ Elaborate management information is available about TM results and provides direction	■ All employees and senior management have extensive knowledge about and are fully aware of money laundering and terrorist financing risks and controls ■ Senior management acts as a role model ■ Obligatory and optional training sessions on AML/CFT are regularly offered and relate to cases tailored to the institution ■ New developments in the area of money laundering and terrorist financing are immediately applied to the organisation's day-to-day practice (e.g. FIU-NL cases)

5 Guidance

5.1 SIRA

Banks must ensure the transaction monitoring process reflects the risks of money laundering and terrorist financing that emerge from the SIRA.

Integrity risks are described in law as the "threat to the reputation of, or the current or future threat to the capital or the results of a financial institution due to insufficient compliance with the rules that are in force under or pursuant to the law."[18] They include risks of financial and economic crime, money laundering, terrorist financing, non-compliance with sanctions, corruption (bribery), and conflicts of interest. To ensure that banks adequately manage the integrity risks, the legislator has provided for various requirements that they are obliged to comply with. The SIRA[19] plays a central role in this process. This risk analysis at operational level, in which both the first-line and the second-line staff are involved, provides the basis for a bank's integrity policies that must be regularly reviewed, and should be translated into procedures and measures. The results of the SIRA must affect the entire organisation, and must also be reflected in the risk analyses at customer level. Below we have shown an example of a bank where that is not the case.

We observed that most of the banks we examined had not translated the risks of money laundering and terrorist financing from their SIRA into their transaction monitoring process. For example, an institution we examined did business with merchants from a high-risk country. This was already identified in the SIRA, but was not included in the transaction monitoring process. We also found that the banks we examined made a distinction between money laundering and terrorist financing in their SIRA, but not in their transaction monitoring process. Some banks seemed to hardly consider terrorist financing scenarios, if at all.

18 Pursuant to Sections 10(1) and 10(2) of the *Bpr*, an institution must have a SIRA in place. If this reveals any new or residual risks, the institution must address these through adequate policies, procedures and measures.

19 For a further description of the SIRA, please see the document: "Integrity risk assessment – more where necessary, less where possible" http://www.toezicht.dnb.nl/en/2/51-234066.jsp.

5.1.1 Risk profile: expected transaction pattern

In determining the customer due diligence risk classification (low, medium, high), the bank must assess the customer's expected transaction behaviour.

Under the *Wwft* banks must prepare a customer risk profile as part of the customer due diligence process. This involves assessing several factors relating to the customer, such as the sector(s) and countries in which they are active, the products and the services obtained from the bank and the distribution channel. On this basis the bank can determine the risk classification of the customer. Depending on the risk, mass retail customers could be included in homogeneous peer groups.

Customers are subject to periodic review and their details are updated based on relevant events. The underlying reasons on which the risk classification is based are also used for the bank's transaction monitoring process. When customers do not have a risk classification, it is in any case not possible to provide a risk-oriented basis for the transaction monitoring system. Based on knowledge of the customer, the bank can check whether the transactions they carry out match the picture it has of the customer and the expected transaction profile.

To determine expected transaction behaviour, during periodic monitoring (i.e. periodic CDD review), the bank can for example obtain information about:

- (expected) incoming (and outgoing) flows of funds, including volumes, types of counterparties and countries; the types of transactions, distribution channels and their frequency (credit card, non-cash transfers, cash withdrawals and deposits, funding, foreign currency, etc.).

Possibly by using peer grouping the bank may deploy advanced data analysis techniques in preparing the expected transaction profile.

The expected transaction profile plays an essential role in detecting unusual transactions and hence preventing money laundering and terrorist financing, as banks can only mark transactions as unusual if they know what exactly qualifies as an unusual transaction. If it appears from certain transactions or account developments that the customer's transaction behaviour is deviating from its risk profile, the bank must establish whether there is the possibility of unusual transactions, and whether further actions have to be taken, such as for example a re-evaluation of the customer's risk profile. The bank must also assess the effectiveness of the alerts that are generated in the event of a potential unusual transaction. Good cooperation between different individuals and departments is essential in this respect.

As the bank establishes the customer's expected transaction behaviour when entering into a business relationship with that customer, it is primarily dependent on information that the customer itself provides about the expected transactions. We expect banks to assess during the periodic risk-based reviews, or during event-driven reviews, whether the expected transaction behaviour is still sufficiently in line with actual practice. This information can be compared with the transaction behaviour of other customers in comparable sectors or customers with a comparable risk profile.

Good practice

In order to establish expected transaction behaviour, a bank has divided its customer portfolio, on the basis of various customer characteristics, into homogeneous customer groups (peer groups). For each one of these customer groups, with the help of data analysis, and on the basis of several relevant risk indicators from the customer portfolio, the bank establishes an expected transaction pattern. When this expected transaction pattern cannot be established on the basis of known customer characteristics, the bank does this through an analysis of historic transaction behaviour, or through a customer survey. For each customer, the actual transaction behaviour is compared on an ongoing basis with the expected transaction pattern. This comparison involves several risk indicators, such as cash deposits and international payments. Statistically significant deviations from the expected transaction behaviour are automatically detected by the transaction monitoring system and investigated in accordance with the standard alert handling process to verify whether this presents a possible risk of financial economic crime.

5.2 Policies and procedures

Banks have developed sufficient policy for transaction monitoring and have sufficiently elaborated this policy in underlying procedures and operating processes.

Banks have a statutory obligation to have in place policies, procedures and processes in order to effectively detect unusual transaction patterns or transactions that may involve money laundering and/or terrorist financing. Effective policy means that a risk assessment and risk profile is prepared for each customer or customer group, and that the expected transaction behaviour is taken into account in the risk assessment. A risk score and customer risk profile must be recorded for each customer and customer group, including a description of expected activities and transactions in view of the products and services they purchase. Related policy must be worked out in procedures and working processes, describing how the bank and its staff should act in certain circumstances.

We expect that the outcome of the SIRA with regard to the risks of money laundering or terrorist financing are reflected in policy and procedures for the transaction monitoring process.

Good practice

A bank indicated in its policy that it took additional control measures for customers with a high-risk profile. In carrying out its SIRA, the bank found that PEP customers have a high-risk profile by default. As part of its SIRA process and in line with its policy, the bank decided to mitigate this inherently higher risk by applying stricter monitoring to the transactions of these customers. To do so, it added tailored controls for this specific customer group to its regular transaction monitoring system.

5.3 The transaction monitoring system

Banks must have an (automated) transaction monitoring system in place and have a substantiated and adequate set of business rules (detection rules with scenarios and threshold values) to detect money laundering and terrorist financing.

We expect banks to have a transaction monitoring system in place that reflects their own risk profile. The transaction monitoring system is preferably a system in which data from several sources can be imported, such as from open sources and sources from commercial providers.

There is no simple yes or no answer to the question of whether a bank must have an automated system in place for post-event transaction monitoring. To determine its approach to monitoring, each bank must weigh up the costs, risks and the method it intends to apply. The monitoring method is strongly dependent on the nature and scope of the bank and the number of transactions it conducts on a daily basis. It is important to be aware that it is not a statutory requirement for transaction monitoring to be automated. It is therefore up to the bank to determine whether monitoring should be manual or automatic. However this decision must be sufficiently substantiated. Accordingly we expect a bank to be able to explain why a manual transaction monitoring system suffices if it conducts tens of thousands of transactions on a daily basis. This could for example be the case if the bank can demonstrate it has sufficient suitable resources for manual monitoring.

5.3.1 Use of business rules

As described in section 4.1, banks make use of a set of business rules to detect unusual transactions. Business rules are intended to mean the set of detection rules applied in the transaction monitoring system, which comprise applied scenarios and particular threshold values, such as amounts in currency and numbers of transactions or combinations of amounts and numbers of transactions. The method by which these business rules are determined, is essential for the effectiveness of a bank's transaction monitoring process. We expect the business rules included in the transaction system to be risk-based and traceable to the outcomes of the SIRA. Traceable is intended to mean that there is a link is between the business rules and the residual risks resulting from the SIRA. The bank must clearly describe this link.

When preparing these business rules, the bank must take various factors into consideration, such as:

- the type of customer, e.g. private individuals and business customers;
- the customer segment, e.g. a distinction between private banking and retail, broken down into other segmented target groups such as for example professional sports;
- the customer risk profile that was prepared during the CDD and possibly adjusted at a later stage;
- the transaction's country of origin or country of destination; e.g. high-risk country, EU or non-EU country;
- the product, e.g. savings, real estate finance or trade finance;
- the distribution channels, e.g. physical presence of the customer or online;

- the nature and frequency of transactions, e.g. cash or non-cash;
- the customer's risk profile classification, e.g. low, medium or high;
- international transactions effected from off-shore countries through the Netherlands to other off-shore countries.

The bank must ensure there is sufficient diversification in the business rules, certainly in the case of several customer segments, countries, products and types of transactions.

An example of a business rule in the retail segment could be the following: customers within a specific age group, e.g. 18-25 years, crossing certain limits with respect to the size and frequency of non-cash transactions.

Other examples concern dormant accounts,

- e.g. if an account is "dormant" for six months but then suddenly becomes active;
- a substantial difference (to be determined by the bank) in an account balance with respect to the average balance over the past three months;
- transactions to or from high-risk countries, financial organisations or countries with whom the customer did not do business with before;
- a scenario for "consultancy payments".

In establishing business rules, the bank also considers other transactions of the customer or transactions in past periods, how long a customer has had a relationship with the bank, comparisons with a customer's age group, and whether or not the customer is in a high-risk postal code area or country,[20]

Good practice

In conducting its SIRA, a bank identified an inherent corruption risk ensuing from transactions of customers classified as PEPs. The bank decided this risk had to be mitigated to an acceptable level in order to continue providing banking services for this customer group. It therefore implemented specific business rules for PEP transactions in its transaction monitoring process.[21]

20 All of course in accordance with the applicable privacy regulations.

21 PEP means Politically Exposed Persons; PEPs are subject to enhanced customer due diligence.

Banks must document how they have arrived at the definition of a business rule, what they do to maintain business rules on an ongoing basis and how they periodically test rules, for example, through the use of backtesting. Backtesting means the bank retrospectively tests the effectiveness of the business rules applied and where necessary makes adjustments. For a further explanation please refer to section 5.3.3.

5.3.2 Business rules in relation to terrorist financing

We expect banks to translate specific indicators for terrorist finance into business rules, and to include these in their transaction monitoring systems. Just setting transaction limits is not sufficient, as a transaction's value is in itself not an indication of terrorist finance. Banks must therefore connect rules about transaction limits to other indicators of terrorist financing, for example lower threshold values for transactions with high-risk countries or regions, in conjunction with certain types of customers, such as foundations.

Detecting terrorist financing is not a static process, but requires the bank to continuously adapt its set of business rules to reflect the dynamic nature of activities linked to terrorist financing.

A lower limit can also be set based on the customer's risk profile:
in the case of high-risk clients the bank would for example apply lower limits in the transaction monitoring system.

Our examinations revealed that the selection of high-risk countries that banks apply in relation to terrorist financing is limited or not up to date. A high-risk country list is often prepared on the basis of the FATF warning lists and the Corruption Perception Index (CPI), but with no consideration of countries which may be related to terrorism or terrorist financing. Recent publications have for example reported on possible financing of dubious charitable institutions, religious communities and/or non-profit organisations, often in the form of foundations created by people or institutions from certain countries, such as the Gulf States. Not all banks have included these countries in combination with foundations in their high-risk country list. We expect banks to closely follow developments in terrorism and terrorist financing, to adjust their lists of high-risk countries accordingly, and then apply this to their transaction monitoring system.

5.3.3 Periodic evaluation of business rules: backtesting

Business rules must be periodically reviewed and tested for effectiveness.

We expect banks to get the the effectiveness of their transaction monitoring system to the desired level and to maintain it. In this regards we expect banks to periodically evaluate this system to assess whether the business rules applied are effective or ineffective. This could for example be the case if business rules are to loosely defined or have thresholds and values that are too high, and as a result there are almost no alerts resulting from a certain business rule. Banks must therefore conduct periodic reviews to assess whether certain business rules have incorrectly not generated any alerts and existing rules require adjustment.

Rules can be evaluated through backtesting. Based on the results of backtesting, banks can make the necessary adjustments to the business rules of their transaction monitoring system.

Backtesting can be conducted in different ways such as:

1. Retrospective analysis of a selection of transactions which under a previous system configuration did not generate an alert. The aim of this is to assess whether it was correct that these transactions did not produce an alert (a true negative) or whether certain transactions are in fact indicative of unusual behaviour (a false negative). If false negatives are observed, the business rules must be expanded or stricter threshold levels applied.
2. An analysis of transactions which are identified as possibly unusual through a route other than post-event transaction monitoring. The aim of this type of backtesting is to analyse the extent to which the transaction and monitoring system is able to detect unusual transaction patterns and transactions.
3. A test involving analysis of business rules with many or only false positive alerts. The aim of this test is to review how these business rules can be adjusted to generate more true positives.
4. A test involving retrospective analysis of the timeliness of notifications in order to improve this.

The aim of these tests is to further optimise the business rules and make them more effective in order to generate more true positive alerts. At the same time, these tests also help the bank to conduct transaction monitoring as efficiently as possible.

Good practice

A bank has a system in place to periodically evaluate the effectiveness of all the business rules, and based on a large number of variables (100+) creates an overview of the variables that potentially improve the business rules. During the periodic review a business rule for international transactions came to light with many more false positives for transactions with the EU than for outside the EU. The bank supplemented this observation with a data and risk analysis, to verify whether the risk was still fully covered by the business rule in the event of adjustments. The bank then adjusted the business rule by raising the threshold value for transactions within the EU compared to the threshold for transactions outside the EU. In this way, the feedback loop resulted in a more effective business rule.

5.3.4 Data analysis

We have observed that banks take various initiatives to develop more advanced technologies in order to analyse their transaction and customer data. Banks have considerable historical data they can use to better predict, analyse and ultimately assess individual customer transaction patterns or transaction patterns and behaviour of groups of customers. We encourage banks to make use of advanced data analysis and artificial intelligence in their transaction monitoring. Advanced technology, such as the use of big data and data modelling techniques, increases the possibilities an institution has for detecting potentially unusual transaction patterns and deviant transaction behaviour.

By using more advanced technology, banks will reduce the risk of contributing towards money laundering or terrorist financing, as they will be able to more effectively detect and anticipate unusual customer behaviour.

Two examples of specific technology for different parts of available data are;

- full-text search and text mining of available free-form[22] text and additional unstructured information related to the transaction, such as agreements and other transaction documents. This may vary from searching for keywords to identifying significant word patterns or code words in transaction details, such as "family support" or "gift"[23], which may be an indication of terrorist financing.
- pattern and network analyses to detect underlying connections between transactions.

When applying advanced technologies such as full-text search, text mining, machine learning and clustering, it is important to measure the quality of the algorithms based on a reference set that includes manually-identified suspicious patterns. In other words, this means you "label" the patterns to identify what the patterns are and where they are hidden in the tested data. You can also conduct this measurement based on a manual analysis of the sample checks. We note that information retrieval and text mining apply measurement values such as precision and recall, the application of which can help to indicate the quality and reliability of automatic data analyses.

5.3.5 Transaction pattern analyses

With the help of a transactions monitoring system, banks can detect transaction patterns or networks or combinations of transactions. This is understood to mean a set of transactions of one or several customers which at an aggregated level could indicate money laundering or terrorist financing. We encourage the use of predictive analytics to improve the effectiveness of the transaction monitoring. Predictive analytics should offer the possibility of being able to detect automated and standard broader transaction patterns and structures and transaction networks.

5.3.6 Business rules in relation to terrorist financing

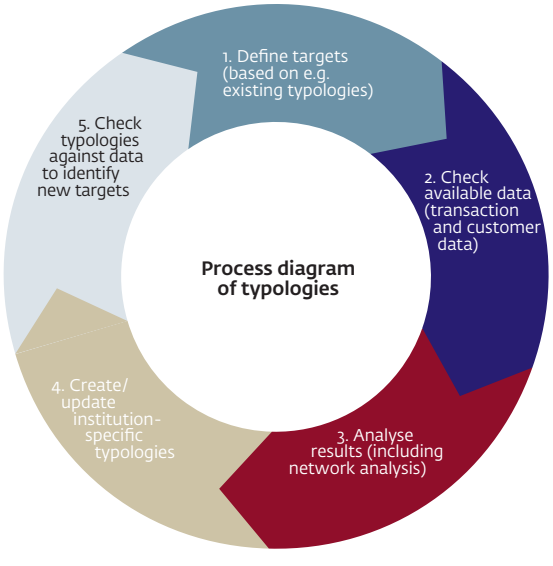
Data analysis with the help of targets and typologies plays a key role in combating terrorist financing. Banks have large quantities of transaction and customer data at their disposal. To detect business relationships with individuals that may have a connection to terrorist financing and identify new typologies, it is important to design a process for continuous analysis of this data.

22 Transactions contain text in free format fields, and software technologies can be used to retrieve valuable information from large quantities of such texts, e.g. specific patterns and trends. Using software technologies, the texts are structured and decompiled, transformed, fed into databases and then evaluated and interpreted.

23 Source: The Egmont Group of Financial Intelligence Units, A global Financial Typology of Foreign Terrorist Fighters; November 2015.

Below is a good practice of a process diagram[24] from a money transaction office, used to analyse the behaviour of targets and identify new typologies. This kind of analysis may also be useful for banks.

Figure 3 Process diagram of typologies



Step 1:
A target is in scope based on public information or existing typologies.

Step 2:
The bank checks whether the target appears in its files.

Step 3:
If the target is included in the files, their transactions are analysed, focussing on the transaction characteristics and the countries and/or individuals or entities involved.

Step 4:
If it is established that the transaction patterns identified could indicate terrorist financing, the patterns are translated into new typologies.

Step 5:
The bank translates the typologies into transaction monitoring scenarios. The transaction monitoring process is then used to identify new targets, and the cycle begins again. This continuous process has proved to be very valuable in detecting unusual transactions.

24 Source: Western Union.

5.3.7 IT control measures to safeguard quality and completeness of data

Banks must safeguard the quality and completeness of the data that is used in the transaction monitoring system, for example, through technical segregation of duties and completeness controls.

Banks must safeguard the quality and completeness of the data that is used in the transaction monitoring system, for example, through technical segregation of duties and completeness controls.

We expect the quality and completeness of the data used in an automated transaction monitoring system to be adequately safeguarded. Important control measures in this respect are the (technical) segregation of duties and controls on the completeness of data. The (technical) segregation of duties is a fundamental part of safeguarding data quality. This ensures that no undesired or uncontrolled adjustments are made to data. Segregation of duties can occur in various ways: segregation is between two processes such as entry and authorisation, but also technical segregation of duties between the test environments and the production environment.

In order to safeguard completeness, it is important that the transaction monitoring system includes all transactions with associated data from the source systems. It is possible to safeguard the completeness of data in various ways. This depends on the IT landscape and the source systems used. Banks must decide in advance which transactions and associated data to control. They must subsequently establish control measures in both the source systems and the transaction monitoring system. These measures relate both to the quality of the data and to its completeness.

The measures taken must be underpinned by adequate management of the IT landscape for the transaction monitoring process. We therefore advise banks to periodically control whether this IT landscape still meets the requirements set, and wherever these requirements still reflect the risks:

- Does the IT component of the risk analysis for the transaction monitoring process continue to reflect changing circumstances.
- Based on a risk analysis, are the IT control measures applied from all the source systems to the transaction monitoring system, including all platforms in between, still effective?
- Does the process not have a single point of failure and is knowledge of the transaction monitoring system sufficiently safeguarded?
- Does the documentation describe the actual situation, in IT technical and non-IT technical terms, such as business rules?
- Is management of general IT controls sufficient?

At the banks we examined, end-to-end control between the source systems and the transaction monitoring system was virtually absent. As a result, there are no checks to establish the completeness of the transactions from the source systems that are fed into the transaction monitoring system. The risk is that not all transactions will be monitored, and the transaction history will be incomplete as a result.

We found a key-man exposure risk regarding the transaction monitoring system in the majority of the institutions we examined: just one or two employees had knowledge of the system. There is a high risk of knowledge loss if few employees know how the systems work, which means these systems cannot be properly maintained, or that incidents cannot be resolved.

During our examination, we established for various banks that business rules developers have access to the production, test and approval environments of the transaction monitoring system. This means they could use their rights to directly adjust business rules for transaction monitoring in the production environment, without the intervention of the responsible owner. It is only possible to prevent developers from making adjustments to business rules without any form of checks by compliance with internal procedures and ensuring these are periodically controlled.

5.4 Alert handling and notification process

As described above, banks must notify FIU-NL of executed or proposed unusual transactions promptly upon their unusual nature becoming known. Prompt notification to FIU-NL is one of the key elements of the AML/CFT process. FIU-NL investigates all notified transactions and, in the event these transactions are marked as suspect, reports them to the investigative authorities. As a result, notification of unusual transactions may lead to criminal prosecution, which is why a bank's notification duty is essential in the AML/CFT process.

The sections below set out guidelines for the alert handling and notification process.

5.4.1 Alertafhandelingsproces

Banks must have an adequate process for notification and dealing with alerts. In this process, for each alert considerations and conclusions are documented underlying decisions to close or escalate an alert.

Banks must have procedures and working processes in place to assess and handle alerts. We expect banks to have sufficient insight into the audit trail and the processing times of follow-up actions for alerts. These procedures and working processes should ensure that the processing time from generating an alert to notification to FIU-NL is as short as possible and that the right priorities are set when dealing with alerts.

We expect banks to record the considerations and conclusions for closing an alert or for reporting the transaction as unusual to FIU-NL. As described earlier it is important in this respect to document whether the transaction in question reflects the customer's transaction behaviour but also to verify whether such a transaction is logical and plausible for the type of customer and the sector in which the customer is active.

We observed during our examination that escalation of alerts to the second line was largely absent from the alerts handling process. It is therefore important that banks offer clear guidelines for those cases in which escalation from the first line to the second line (compliance) is necessary. Please note: We also expect banks to be able to adequately substantiate any conclusion, based on consideration of risks, to not notify FIU-NL.

We came across the following examples of failure to comply with requirements:

At a bank an alert was generated based on two cash deposits by a second-hand car dealer. The bank closed the alert for two reasons: firstly because cash transactions fit in with the customer's transaction pattern – this customer frequently made cash transactions – and secondly because the values matched the prices of the second-hand cars listed, around EUR 20,000. The alert file does not substantiate whether it is common practice to pay for cars in this price range in cash. We requested a transaction overview, which showed that over EUR 550,000 in cash was deposited with the bank in a period of nine months. The bank did not (demonstrably) investigate the plausibility of these cash deposits.

Closing an alert solely on the grounds that cash deposits fit within the transaction profile does not qualify as sufficient follow-up. The frequency of deposits and whether their size is plausible must also be taken into account. In cases like these we expect banks to conduct more extensive analysis of such cash deposits in order to arrive at a substantiated decision to notify or not notify FIU-NL.

A private customer made some twenty cash deposits at a bank, totalling EUR 50,000. Recently, the customer made a cash deposit of EUR 25,000, which was then immediately debited from the customer's current account. The same day the customer made another cash deposit, of EUR 20,000 and also deposited several smaller amounts in EUR 500 banknotes. The alert handler classified the alerts as non-notifiable, but the alert file does not show how they arrived at this conclusion.

Good practice

A bank's transaction monitoring system generated an alert following substantial cash deposits into a business account. As a follow-up, a broad analysis of the customer and transaction profile was made, which established that the account is held by a well-known beach restaurant on the Dutch coast, and that the CDD file did not contain any specific risks. An additional background investigation into the customer also revealed a transparent situation, and no issues from the past.

The transaction analysis showed that frequent cash deposits were made into this account, with a monthly volume fluctuating between EUR 5,000 and 15,000. In the summer period this incidentally increased to above EUR 20,000, exceeding the expected volume of cash deposits laid down in this customer's risk profile. The analysis showed that cash deposits amounted to approximately 19% of the customer's total income. Based on the guidance, the alert handler was able to confirm that this percentage is in line with the applicable ratios for this sector. Even in the summer period the ratio between cash and non-cash income remained below 20%. This could be explained from the customer's regular business activities, which commonly show a seasonal pattern and a higher income in the summer period. It was also established that the outgoing transactions mainly involved wage payments, wholesaler purchases, taxes and rent. This also fits in with regular catering business activities.

Based on the analysis, the alert handler concluded that the cash deposits were not unusual given the customer profile, and that they therefore did not need to be notified.

5.4.2 Capacity and resources to assess alerts

We expect banks to have sufficient capacity and financial resources available to conduct risk-based transaction monitoring, and their alert handling process in particular. In addition, the department that handles alerts must set realistic targets in view of the size and risk profile of the bank.

To achieve this, the bank can prepare KPIs defining the estimated processing time for dealing with every type of alert. These KPIs must of course be periodically evaluated.

Finally, the bank must structure its processes to ensure a minimum risk of delay.

Good practice

One of the banks from our thematic examination worked on the principle of "quality before speed" when handling alerts.[25] Alert analysts must have sufficient time to conduct a thorough examination and report their findings, and also have available sufficient resources, as well as access to internal and external systems and sources of information. This means that analysts must be able to consult the customer file when assessing alerts. The customer file can provide additional information for detecting transactions with an elevated risk of money-laundering and terrorist financing. The analyst can for example use the information from the customer file to assess whether the transactions are in line with the customer's activities. A list of denominations used for withdrawals and deposits are another source of information.

Good practice

Banks have the option of making high-urgency notifications to FIU-NL. One of the banks in our examination did so in a case in which the transaction patterns of an account seemed to indicate a "Ponzi scheme". Thanks to the bank's high-urgency notification the police could quickly initiate a criminal investigation after receiving FIU-NL' report, and seize the funds before they could be channelled away.

25 Speed involves dealing with alerts as quickly as possible in order to prevent backlogs.

Good practice

A bank must keep abreast of developments in money laundering and terrorist financing, and payment instruments such as bitcoin and other virtual currencies.[26] In their alert handling process, one of the banks we examined identified a customer who made a lot of cash withdrawals following non-cash transfers from companies trading in bitcoin and other crypto currencies. The bank notified FIU-NL of this, and investigation by FIU-NL and the Fiscal Investigation and Detection Service (Fiscale inlichtingen- en opsporingsdienst – FIOD) revealed that the customer was indeed a "bitcoin casher". Bitcoin cashers purchase bitcoins from traders who most likely obtained them from trading in illegal goods on the dark web, where bitcoins are a common payment instrument. The bitcoin cashers then sell these bitcoins to exchange offices on legal platforms in exchange for euros. The proceeds in euros are then withdrawn from the account in cash.

5.4.3 Alerts related to the risk of terrorist financing

We expect banks to maintain a list of red flags that could indicate terrorist financing. The list must fit the bank's risk profile and should be translated into business rules in order to detect terrorist financing risks. We also expect banks to use recent guidance documents and newsletters issued by DNB, FIU-NL and international bodies such as the Financial Action Task Force on Money Laundering (FATF).

Good practice

Based on media coverage, a bank suspected a customer of having a possible connection to jihadi groups. The bank developed an alert for this customer. This is a good practice of an institution that closely monitors developments through the media and takes action by developing an alert for this customer.

26 In July 2014, we alerted the banks to the high-risk profile of virtual currencies in a thematic examination into new payment methods.

Good practice

A bank noticed a debit card transaction by one of its customers in Eastern Turkey, close to the Syrian border. The monitoring system generated a terrorist financing alert for the transaction.

To detect such useful alerts, FIU-NL published a list of towns in the Turkish-Syrian border region in one of its newsletters.

Good practice

Two months after the debit card transaction in Eastern Turkey described above, the customer applied for a EUR 10,000 loan. A bank staff member found that this customer had already applied for a EUR 10,000 loan four months before, stating that it was meant to purchase a car. The bank then decided to investigate further and found that the funds of the first loan were almost immediately transferred to Turkey in several transactions.

The bank also found a connection to the previous alert, i.e. the debit card transaction in Turkey. The bank asked the customer several questions in order to clarify matters, but the customer was unable to give clear reasons for these transactions.

The bank then decided to refuse the second loan, and notified all transactions, i.e. the debit card transaction and the two loan applications, as unusual transactions to FIU-NL.

This case presented the following red flags:

- a debit card transaction in the Turkish-Syrian border region;
- taking out a loan, which is withdrawn from the account shortly afterwards;
- use of the loan does not correspond with the customer's statement;
- splitting up funds in smaller amounts for transfer;
- transferring funds obtained as loans to certain countries.

5.4.4 Notification process

Banks must have an adequate process for notification and dealing with alerts. Banks must ensure they fully and immediately notify FIU-NL of any executed or proposed unusual transactions.

Institutions have a statutory obligation to provide this notification as soon as the unusual nature of the transaction becomes known. In addition to notifying FIU-NL banks can also report any strong suspicions of money-laundering or terrorist financing to the police at the same time. If this is not reported immediately, there is a risk that FIU-NL and the law enforcement services will misinterpret the relevant information. Any incidents must also be reported to us.[27]

Banks must ensure they fully and immediately notify FIU-NL of any executed or proposed unusual transactions. In this respect they must have a procedure in place that defines the notification process, and what steps to take in such cases. When investigating these alerts it is important to examine the customer's earlier and related transactions, and to reconsider the customer's risk and associated transaction profile.

Banks must ensure adequate written processes are in place for immediately notifying FIU-NL of transactions for which there are grounds to suspect they are related to money laundering or terrorist financing. They must ensure that all relevant information relating to notifications is kept confidential, with due regard to the conditions and exceptions provided for in the law, and the guiding principles for this must be established in policies and procedures. We expect banks to ensure that policy and procedures are reflected in for example, appropriate access rights with regard to core systems used for case management and notifications, secure information flows and guidance/training to all staff members involved. This guidance and training is primarily important for the first-line staff who have contact with customers. It is essential that these staff know when there may be cases of unusual transactions, what questions they have to ask the customer and which information they must not under any circumstances disclose to the customer.

Good practice

A good example is a bank that provides sufficient guidance to its staff about reporting unusual transactions. It does so by discussing examples of cases on a quarterly basis and including this in the regular training programme. The bank takes the results of this analysis into account for the the customer's current risk assessment.

27 See also Section 12 of the Decree on Prudential Rules for Financial Undertakings.

The bank notifies FIU-NL immediately of any unusual transactions

The case described in 5.4.3. involved transactions with a country with an enhanced risk of terrorist financing, where the bank noticed the relationship between a customer and a jihadist based on media coverage. The bank considered this information only five months after the news was published, and then notified FIU-NL.

The bank should have dealt with this information and notified it to FIU-NL at short notice, in order to prevent FIU-NL and the investigative authorities from missing out on relevant information on potential terrorist financing. According to the bank, the alert required extra processing time for reasons of thoroughness, and there was also some backlog in dealing with alerts. Given the substantial risks to the Netherlands and its population, institutions should assess any alerts related to terrorist financing promptly and notify them to FIU-NL without delay. Banks must deal with alerts related to terrorist financing as a matter of high priority

Notification of unusually large cash deposits in high denominations

In a case involving large cash deposits in EUR 500 banknotes, the description of the bank's investigation revealed that the staff member at the relevant branch office had not been given any guidance about dealing with alerts. As a result, the staff member had failed to inquire about the origin of the funds and the reason for using EUR 500 banknotes. The alert processor therefore had insufficient information to notify the transactions to FIU-NL, while the large cash deposits and high denominations were reason enough to do so.

5.4.5 Reclassification of customer risk

If the results of the analysis provide sufficient grounds we expect the institution to re-evaluate the customer's risk profile to establish whether there are reasons to adjust this profile. This can for example be based on event-driven review. This way the institution safeguards the customers risk profile, ensuring the customer's risk classification reflects its risk of money laundering or terrorist financing. Also, if the bank receives feedback from FIU-NL stating that the report of the suspicious transaction has been passed on to the investigative authorities, the institution must reassess the customer's risk profile and if necessary adjust it.

We expect banks to ensure that those responsible for analysing alerts (and if applicable receiving feedback reports) also have possibilities to reassess the customer's risk profile. We also expect these analysts to be able to indicate to the staff responsible for customer assessment that a re-evaluation is necessary. In this respect we also expect banks, through a quality assurance process, to monitor if such re-evaluations are adequately conducted. The alerts handling process can also offer insight into the effectiveness of the business rules in place. The first-line staff can play a key role in this respect and provide input for the periodic review of the business rules.

Good practice

In a local news release, a staff member read that a cannabis farm was discovered at the house of one of the bank's customers. Further investigation revealed that the customer had made several cash deposits into his own account and that of his foundation. The customer confirmed that he ran a cannabis farm in his home and deposited the proceeds of these illegal activities in cash into these accounts. He explained that he was in financial difficulties and hence resorted to illegal activities. The unusual transactions were notified to FIU-NL, the customer's risk classification was reviewed and the customer was reclassified as unacceptable.

5.4.6 Objective indicators for automatic notification

In view of the nature of their activities, many banks have to deal with transactions that meet one of the objective indicators for reporting unusual transactions. To ensure that such transactions are immediately reported, a tool or functionality can be implemented within the transaction monitoring system by which transactions meeting this objective indicator are automatically reported to FIU-NL. This allows these institutions to avoid failing to immediately report these transactions and removes the administrative burden for the party responsible for this task.

5.5 Governance

Banks must have structured their governance with regard to transaction monitoring in such a way that there is clear segregation of duties, for example through the three lines of defence model.

The principle for addressing this part of the maturity model is the three lines of defence model. This model has been chosen as it reflects the model that most banks use in their governance. This does not however imply that other assurance models could not be applied. It is nevertheless important to ensure that the model at all times safeguards the segregation of independent duties for control activities. Banks should of course always have an independent compliance function[28] and an independent internal control or internal audit function.

Good practice

All banks in our examination had an independent internal control function, usually a third-line function i.e. the internal auditor. By means of periodic audits, the independent control function assesses the design, existence and operating effectiveness of the transaction monitoring process. These audits were generally of good quality, and follow-up of the findings was adequate. One bank also monitored the monthly progress of action points established by the business based on the audit reports. The internal auditor applied a comprehensive chain approach.

28 Section 21 of the Decree on Prudential Rules for Financial Undertakings *(Besluit prudentiële regels Wft - Bpr).*

We expect the bank's organisation to be set up in such a way that the first line has a clear responsibility for transaction monitoring and that the second line (compliance) has an advisory and monitoring role but also can have a role in reporting unusual transactions to FIU-NL. [29]

We expect your institution to have clearly defined what the advisory task of compliance is in relation to transaction monitoring, for example, dealing with advice from compliance on high-risk cases. Quality assurance for transaction monitoring is performed by the second line. This is usually referred to as second-line monitoring. In this context, it is important to periodically and systematically test procedures and processes.

As a second-line function, compliance carries out a monitoring role, and periodically tests whether measures are adequate or whether they have to be adjusted. We also expect the third-line function, the independent internal control function, to check the functioning of the first and the second line with sufficient regularity. In this respect, the organisation ensures that it has sufficient capacity available, both quantitatively and qualitatively, to fulfil these roles and tasks.

We expect senior management to address signals from the first, second and third lines about possible shortcomings in the transaction monitoring process. In this respect it is important that banks have adequate and regular management information that provides insight into signals and results, so they can take timely action on this basis. In this way, in addition to its advisory and monitoring role, compliance also fulfils a reporting role with respect to transaction monitoring. At most of the banks we examined, this reporting role was in place. DNB expects compliance's periodic accountability report to contain explicit management information about the most important results of its transaction monitoring.

29 We note in this context that the following may be included in the *Wwft* (based on the Fourth Anti Money laundering Directive) with respect to the compliance function: "the compliance function monitors compliance with statutory regulations and institution-specific internal rules and is responsible for reporting unusual transactions to FIU-NL, as described in Section 16(1) of the *Wwft*."

5.6 Training en awareness

Banks must offer their staff tailored training programmes. Staff must be aware of the risks of money laundering and terrorist financing.

We note that banks have included training sessions about the *Wwft* in a programme that is updated yearly. We expect the content of this programme to be tailored to each target group, from the board and senior management to junior staff. We also expect the training to be adjusted to the level of the staff members. taking into account competencies and experience, as well as making use of relevant cases from the institution's own transaction monitoring process. When establishing the content of the training programme you can make use of the cases that FIU-NL publishes every two weeks.

Good practice

One of the banks we examined offered a training programme for alert analysts based on four different levels of experience. The training programme establishes the expected competencies for each level of experience, as well as the goals which the training should achieve. The training programme also establishes how the achievement of these goals is quantified.

Another bank we examined had an annual training programme available for the first, second and the third line. On the basis of case studies, the training programme addresses the latest developments, both in terms of the laws and regulations, as well as practical examples of possible cases of money laundering and terrorist financing, and the institution's response to this. The training programme therefore covers policy, procedures and underlying work processes, clarifying what steps to take in such cases. Some banks employed a dedicated expert in counter-terrorist financing.

Glossary

Alert
A signal indicating a potentially unusual transaction.

Alert handler
The member of staff who analyses, investigates and records the alert.

Back-testing
Testing and optimisation of a certain approach, based on historical data.

Business rules
The set of detection rules that are applied in the transaction monitoring system, comprising applied scenarios and the certain threshold values.

Continuous monitoring
Ongoing monitoring and control.

Customer
the customer is the natural or legal person with whom a business relationship is entered into or who has a transaction effected.

Customer due diligence (CDD)
Investigation as defined in Section 1of the *Wwft*.

Customer risk profile
Classification of customers according to risk categories, as set out in the DNB Guidance on the *Wwft* and *Sw*.

Event-driven review
The institution conducts a customer due diligence on the basis of an event or incident.

Expected transaction behaviour
The expected pattern of the customer's transactions.

Financial and Economic Crime
Money laundering, corruption, terrorist financing, insider trading, non-compliance with sanctions and other criminal behaviour (for example embezzlement, fraud and forgery).

Indicators
Indication or signal that a transaction may involve money laundering or terrorist financing.

Notification process
The process of reporting unusual transactions to FIU-NL, as described in Section 16(1) of the *Wwft*.

Peer grouping
Defining customer groups with common characteristics.

SIRA
Systematic integrity risk analysis, as described in Section 10 of the *Bpr*.

Targets
Targets are subjects that are associated with terrorist financing.

Transaction
An act or a combination of acts performed by or on behalf of a customer of which the institution has taken note in the provision of its services to that customer.

Transaction data
All data relating to a transaction.

Transaction profile
Determining the customer's profile based on expected transactions or expected use of the customer's account.

Typology
Characteristics, or groups of characteristics, which may point to terrorist financing.

Disclaimer

In this guidance document, De Nederlandsche Bank N.V. (DNB), sets out its expectations regarding observed or envisaged behaviour in supervision practice, that reflects an appropriate application of the legal framework relating to the requirements of transaction monitoring. This document also includes practical examples for a better interpretation.

This document guidance must at all times be read in conjunction with the published guidances on this subject such as the DNB Guidance on the *Wwft* and SW (version April 2015). You can use the good practices described in this guidance as a basis for your transaction monitoring, while also taking into consideration your institution's own circumstances. Where appropriate, a stricter application of the underlying regulations may apply.

This Guidance is not a legally binding document or a DNB policy rule as referred to in Section 1:3(4) of the General Administrative Law Act (Algemene Wet Bestuursrecht), and it does not have or aim to have any legal effect. It does not replace any legislation or any policy, supervisory or other regulation on this topic. The examples presented in this document are not exhaustive and cannot cover every eventuality. Rather, they aim to help institutions interpret and implement the statutory requirements.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 20 524 91 11
dnb.nl