Post-event transaction monitoring process for payment service providers

Guidance

DeNederlandscheBank

EUROSYSTEEM

15 September 2017

Westeinde 1, 1017 ZN Amsterdam – P.O. Box 98, 1000 AB Amsterdam
Telephone +31 (0)20 524 91 11 – E-mail: info@dnb.nl
Website: www.dnb.nl

Contents

1 Introduction

1.1 What is the purpose of this guidance?

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 payment service providers, 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 transaction monitoring.

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

As gatekeepers for the Dutch financial system, payment services providers are expected to adequately monitor transactions. They must remain alert at all times. There are statutory requirements which an institution must meet in this regard, and it is our task to supervise compliance with these rules and regulations. All payment services providers are therefore obliged to conduct transaction monitoring, although this obligation and its supervision is principle-based. This means that the practical interpretation of this requirement is not prescribed in detail by laws and regulations, or by the supervisory authority. This guidance provides you with indications on how to set up a transaction monitoring system. It is up to you as a payment services provider to determine how exactly you interpret this. The supervisory authority will assess the result.

Transaction monitoring is not new for payment services providers. The areas of concern and the examples presented in this document serve as a supplement to prevailing laws and regulations and the previously published guidance documents on this subject such as the DNB Guidance on the *Wwft* and *SW*, version 3.0, April 2015[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 our 2016 thematic examination: 'Post-event transaction monitoring process for payment service providers'.[2] 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.

While we only conducted the examination among licensed payment service providers, exempt payment services providers should also adequately monitor their transactions on the basis of the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en terrorismefinanciering - Wwft*).

This document provides an overview of the statutory requirements that payment service providers 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 operations. This documents focuses on the existing market situation. This means that the customers of the payment service providers will primarily be merchants. We are still considering whether the Payment Services Directive 2 (PSD2) will have implications in this respect, particularly in terms of the new services indicated in PSD2, the customers for which will be primarily natural persons.

This document is structured as follows: In Chapter 4 we depict and describe what a transaction monitoring process can look like. This chapter also includes the maturity model that we used in our 2016 examination. Chapter 5 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 guidance documents 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. Payment service providers ensure the transaction monitoring process reflects the risks of money laundering and terrorist financing from the SIRA. When determining the risk profile for a customer and or 'customer peer groups' payment service providers also include expected transaction behaviour.
2. Payment service providers have developed sufficient policy for transaction monitoring and have sufficiently elaborated this policy in underlying procedures and operating processes.
3. Payment service providers 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. Payment service providers periodically test these business rules, in terms of both technical aspects and effectiveness.
4. Payment service providers have an adequate process for notification and dealing with alerts. They 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. Payment service providers have structured their governance with regard to transaction monitoring in such a way that there is clear segregation of duties, for example via the three lines of defence model.
6. Payment service providers offer their staff tailored training programmes. Staff are aware of the risks of money laundering and terrorist financing.

3 Legal context and scope

3.1 Transaction monitoring: statutory obligation for continuous monitoring

Payment service providers 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, they must immediately report this transaction to FIU-NL without delay.[3] To be able to do this it is crucial that payment services providers have in place an effective transaction monitoring process.[4]

With reference to the DNB Guidance on the *Wwft* and *SW*, version 3.0, April 2015 we confirm the following:[5] As the *Wft* (ethical operational management), and the *Wwft* are focused on the same objective, the procedures a payment service provider 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 main objective is that payment service providers should know who they are doing business with and for what purpose the business relationship is used.

In order to exercise adequate continuous monitoring, payment service providers 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 they note any new or residual risks, payment services providers 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*) payment service providers 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 payment

3 For the sake of brevity, referred to hereinafter as 'unusual transactions'.
4 Sections 2a(1) and 3(2) under d, of the *Wwft*.
5 See pages 5 and 6 of this Guidance.
6 *Bpr* Sec. 1.
7 Sections 2a(1) and 3(1) of the *Wwft*.
8 Section 1(1m) of Wwft defines a transaction as: '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.'

services providers can ensure that the transactions conducted correspond to the knowledge they have of their customers and their risk profiles, where necessary investigating the origin of the funds used in the relevant business relationships or transactions.[9] We realise that it is not always possible to prepare a risk profile in advance for each customer. In order to take a more practical approach, a payment service provider can categorise its business relations according to peer groups, for example. This involves that payment service provider defining its own peer groups 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 transaction monitoring process and payment service providers can interpret it according to their risk-based approach. In this regard risk-based is intended to mean that they will devote the 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. We can understand that for payment service providers, the risk of money laundering is higher than the risk of terrorist financing, and they will therefore devote more attention to the former area. Payment services providers are expected to have a system in place for monitoring transactions and generating alerts for potentially unusual transaction patterns and an alerts handling process. In order to be able to recognise 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 notified to FIU-NL without delay upon their unusual nature becoming known.[11] This means that payment service providers 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, payment service providers 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 receive regular training to identify and report unusual transactions and perform effective and exhaustive customer due diligence.[13]

9 Section 3(2d) 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:

- Both licensed and exempted payments service providers.
- Electronic money institutions if they provide payment services.
- Branches of foreign payment service providers with offices in the Netherlands.

There is a wide range of payment institutions, which will only become greater with the implementation of the PSD2. These include for example: issuers, acquirers, PSPs, PIN payment processors and all sorts of combinations thereof. Each type of institution has a different information position with regard to the merchant and the merchant's customer. In this guidance document examples are given – such as red flags – which may be more relevant for one institute than for another type of institute. It is up to you to judge which information is relevant is for your type of institute.

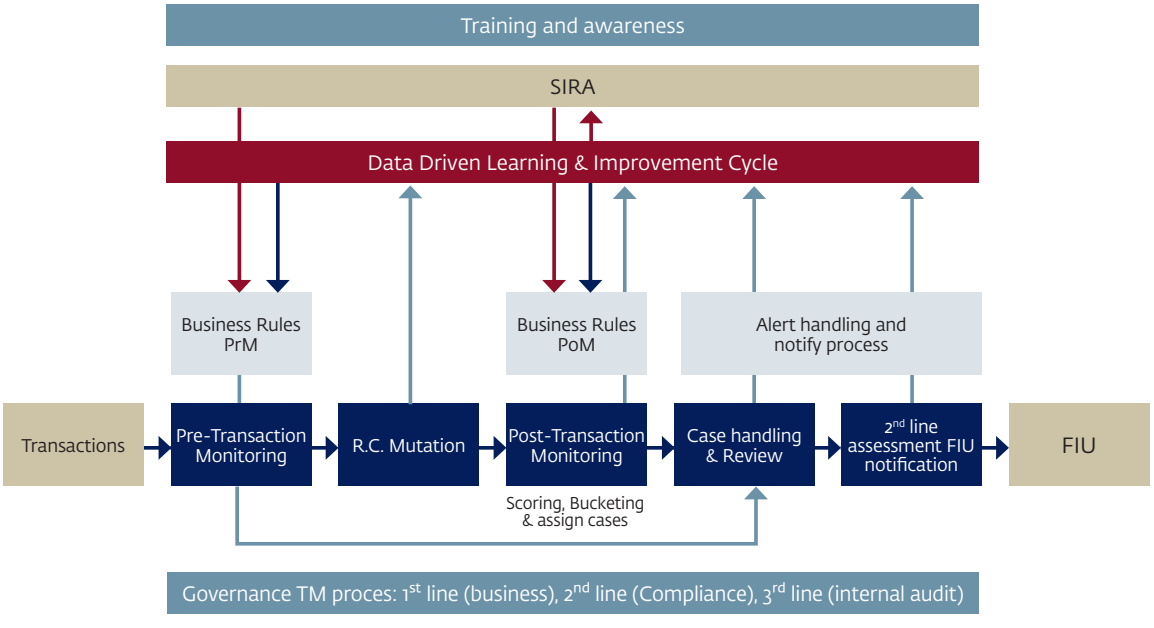
Another guidance document has been prepared for banks, money transfer offices and trust offices. These can be found on our website.

4 Transaction monitoring

4.1 The transaction monitoring process

The transaction monitoring process can be structured as follows:

Figure 1 The transition 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 occurs before the transaction has been carried out. Pre-transaction monitoring will in the payment service provider sector be primarily conducted to detect (credit card) fraud. In other sectors pre-transaction monitoring will be used when cash is exchanged, sent or deposited in an account. In the case of post-event transaction monitoring, the transaction has already been carried out by the payment service provider and transaction monitoring occurs afterwards.

Post-event transaction monitoring

This guidance document describes the post-event transaction monitoring process, because payment service providers 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 payment service providers with knowledge of their customers, including the purpose and intended nature of the business relationship with the customer. Customers in this sector will currently mainly comprise merchants. However the entry into force of the PSD2 will see the introduction of new services, the customers for which will also often be natural persons. With knowledge of the customer, payment service providers will be able to conduct risk-based assessments to ascertain where the transactions carried out have unusual patterns that could indicate money laundering or terrorist financing. Payment service providers must tailor how they monitor customer transactions according to: the type of client (in which sector is the customer active, are Politically-Exposed Persons (PEPs) involved, the type of service provided to the customer's (iDeal, credit card, payment terminals, etc.) and the customer's risk profile. Monitoring can be set up differently for each customer and product.

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.

Step 1: risk identification

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

When identifying and analysing risks payment service providers should also place their custom in various risk categories, such as high medium and low, based on that money laundering and terrorist finance risks attached to the business relationship with the customer. To determine the customer's risk profile they should prepare a transaction profile based on expected transactions or expected use of the customer's (or customer group's) account.[15] By preparing a transaction profile in this way (through peer grouping) payment service providers can sufficiently monitor transactions conducted throughout the duration of the relationship to ensure these are consistent with the knowledge they have of the customer and their risk profile. By identifying the expected transaction behaviour, payment service providers can assess whether the transactions carried out are consistent with their knowledge of the customer. For the majority of payment service providers, a merchant's transaction profile will be prepared on the basis of peer grouping.

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

1. Current: the transaction profile is up-to-date and has a date. All relevant changes to the profile are made promptly.
2. Complete: it includes all account numbers and all relevant activities (such as websites used by the merchant).
3. Specific and substantiated: the suspect flows of funds are clearly described, including the expected amounts (in view of the type of merchant) and the frequency of the payments (the number of orders the merchant's customers have placed). The (threshold) amounts indicated are well substantiated and can actually contribute to recognising unusual transactions.
4. Documented: the transaction profile is documented in the customer file.

15 For further information on how institutions can do this, please refer to pages 29-32 of our Guidance on the *Wwft* and *SW* (version 3.0 of April 2015).

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, payment service providers must have a transaction monitoring system in place. Before making use of such a system the payment service provider 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 smaller payment services provider with a limited number of simple transactions. It may also be the case that a payment services provider considers the use of a highly advanced system, which makes use of artificial intelligence for example, to be essential.[16]

In any case, the responsibility for effectively detecting unusual transactions lies with the payment services provider. Payment service providers should have a good understanding of the systems, and should not just rely on the algorithms provided by external suppliers.

Step 3: data analysis

With help from transaction monitoring system and the use of software, payment service providers should analyse their transaction data. 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 the investigation of the alerts must be adequately and clearly recorded. When the findings of the investigation reveal that the transaction is unusual, it must be notified to FIU-NL without delay. Payment service providers should have sufficiently described and documented the considerations and decision-making process about whether or not to report a transaction. In case of uncertainty as to whether a transaction is unusual, they should in any case notify it to FIU-NL. When a payment service provider fails to meet its notification duty – even if this is not deliberate – it constitutes an economic offence.

16 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 4: assessment, measures and documentation
The payment service provider then assesses the consequences of the notification to FIU-NL (and a possible feedback report from FIU-NL) for the customer's risk profile and determines 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 recorded. In this connection, the payment service provider keeps the data relating to the report of the unusual transaction, records it in readily accessible form for five years after the report 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 what the stage of maturity the payment services provider is in the transaction monitoring process. In this model the degree of compliance in six areas is assessed according to a four-point scale:

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

Payment service providers can use this maturity model to assess their own ambitions, while ensuring they achieve a minimum score of 'yellow'. A payment services provider's level of ambition is dependent on its risk profile. A yellow score means that a payment services provider 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 and not so good examples of interpretation of the standard. The good examples illustrate how a payments services provider has 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

Payment service providers ensure the transaction monitoring process reflects the risks of money laundering and terrorist financing 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'.[17] 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 payment service providers adequately manage integrity risks, the legislator has provided for various requirements that they are obliged to comply with. The SIRA[18] 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 integrity policies. These must be regularly reviewed, and should be translated into procedures and measures. The results of the SIRA must have an influence on the entire organisation, and must also be reflected in the risk analyses at customer level. Below is an example of a payment services provider where that is not the case.

We observed that most of the payment services providers we examined had not applied the risks of money laundering and terrorist financing from their SIRA to 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.

17 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.

18 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 payment services assesses the customer's expected transaction behaviour.

Under the *Wwft* payment services providers 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 and the products and the services obtained from the payment services provider. On this basis, payment services providers can determine the risk classification of their customers.

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 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 payment service provider can check whether the transactions they carry out match the picture they have of the customer and the expected transaction profile.

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

- (expected) incoming (and outgoing) flows of funds, including volumes;
- the countries in which the customers have their clients, and from which transactions will therefore mainly originate;
- the types of transactions and their frequency (credit card, non-cash transfers, foreign currency, etc.);
- the time lapses between purchase and payment, refunds or charge backs;

Based on the expected transaction profile of a customer, you can then check whether the actual transactions are consistent with that profile.

- Do the amounts involved match the expected transaction behaviour?
- Does the frequency of the transactions reflect expected transaction behaviour?
- Is the time frame for the transactions in line with the expected transaction behaviour?
- Does the total volume of the transactions reflect expected transaction behaviour?

The payment services provider regularly verifies whether customers still match their risk profile drawn up when the provision of services started. Payment service providers can after all only detect unusual transactions if they have a good picture of their customers' activities. If it appears from certain transactions or account developments that the customer's transaction behaviour is deviating from its risk profile, the institution 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. Good cooperation between different individuals and departments is essential in this respect.

As payment service providers establish the customer's expected transaction behaviour when entering into a business relationship with that customer, they are primarily dependent on information that the customer itself provides about the expected transactions. Particularly with start-ups, this is difficult for the customer to determine. When establishing the expected transaction profile of start-ups, payment service providers can use peers as a comparison (for example by looking at start-ups of customers in comparable sectors). During periodic risk-based reviews or during event-driven reviews, payment service providers should assess whether the expected transaction behaviour is still sufficiently in line with reality. This information can be compared with the transaction behaviour of other customers in comparable sectors or customers with a comparable risk profile.

Good practice

During the customer onboarding process, a payment services provider divides its merchants in peer groups. These groups are formed on the basis of certain factors, such as the sectors in which the merchants are active. During the monitoring process the payment services provider makes use of models through which it can automatically review the transaction behaviour of a merchant to check whether it is in line with the transaction behaviour of its peers.

Good practice (in this case at a bank, but could also be of interest for larger payment institutions)

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

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

A payment services provider has 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.

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

Policy and procedures form the basis for the work process at a payment services provider. They provide a clear indication of how the payment services provider gives operational interpretation to transaction monitoring.

They also allow the most important outcomes of the SIRA to be traced back to the transaction monitoring process. Following procedures is enforced through functionalities in the system

5.3 The transaction monitoring system is

Payment service providers 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 payment services providers to have a transaction monitoring system in place that reflects their own risk profile. For larger institutions, 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. A manual transaction monitoring system often suffices for smaller, exempt payment services providers which have limited volumes of transactions.

There is no simple yes or no answer to the question of whether a payment services provider must have an automated system in place for post-event transaction monitoring. To determine its approach to monitoring, each payment services provider 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 payment service provider 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 payment services provider to determine whether monitoring should be manual or automatic. However this decision must be sufficiently substantiated. Accordingly we expect payment services providers 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 payment services provider can demonstrate it has sufficient suitable resources for manual monitoring.

Good practice

A payment services provider uses an automated self-learning system in which data from several sources (both open and closed sources) is imported to detect transactions or transaction patterns which may relate to money laundering or terrorist financing.

5.3.1 Use of red flags/scenarios

Based on the outcomes of the SIRA, the payment services provider should establish scenarios/red flags to identify potentially unusual transaction patterns and transactions. These scenarios can then be used to develop business rules. Based on the examples of indicators below the following scenarios could be prepared:

- the time of the underlying transaction or transactions (transactions are for example conducted outside the opening hours of the payments terminal location.
- the time periods between purchase and payment, refunds or charge backs;
- the frequency and size of refunds and charge backs to the merchant's individual customers;
- the relationship between the initial purchasing amount and the amounts of pay-out, refunds, or charge backs;
- the use of different bank or credit card numbers for the initial purchase and the pay-out of cash;
- the ratio between stakes paid in and winnings received;
- the time periods between the moment of paying in stakes and receiving winnings;
- the merchant's customer uses many different IP addresses;
- payments from IP addresses in high-risk countries;
- frequent use of the same credit card at a merchant;
- multiple payments made at a particular merchant using credit cards with the same BIN from an exotic bank;
- changes in transaction behaviour which cannot be explained by the activities of the merchant;
- certain merchants which receive many payments in bitcoins and PayPal compared to other payment methods or compared to merchants in the same peer group.

Chapter 8 of DNB's Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act mentions red flags for credit card transactions.

5.3.2 Use of business rules

As described in section 4.1, a payment services provider makes 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 payment service provider'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. This link must be set out by the payment services provider.

When preparing these business rules, the payment services provider takes various factors into consideration, such as:

- the type of customer; e.g. a PEP
- the customer segment; e.g. gambling, gaming, erotic, charitable foundations, hospitality, online retailers with chemicals, online retailers selling anonymous phone and SIM cards, traders in gold, coins, bitcoin/crypto currency exchange, hosting services, administrative consultancies, consultancy, training and education, travel or crowdfunding,
- the transaction's country of origin or country of destination; e.g. high-risk country, EU or non-EU country
- the product; e.g. credit cards from high-risk countries, bitcoin, prepaid cards, e-wallets or PaypPl
- the nature of the transaction;
- e.g. customer to customer, customer to merchant, charge backs of refunds

The payment service provider ensures there is sufficient diversification in the business rules, certainly in the case of several customer segments, countries products and types of transactions.

It is important payment services providers 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 payment services provider retrospectively tests the effectiveness of the business rules applied and where necessary makes adjustments to the business rules, for a further explanation please refer to section 5.3.3.

Good practice

The outcomes of a payment service provider's SIRA show there is an elevated risk attached to accepting bitcoins. The payment service provider anticipates this in its transaction monitoring process by implementing a specific business rule for bitcoins.

5.3.3 Business rules in relation to terrorist financing

We realise that terrorist financing is more difficult for payment service providers to detect than for example, it is for banks, seeing as banks have more information available. However, we do expect payment service providers to have translated specific indicators for terrorist finance in their business rules, and to have then included 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. Payment service providers 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, whether or not this is in conjunction with certain types of customers, such as foundations, travel agencies, online retailers selling chemicals, crowd funding platforms and e-currency (bitcoin) traders.

In their monitoring, payment service providers must be alert in facilitating foundations collecting funds to provide assistance in crisis and conflict areas. Red flags for these foundations include the following:

- Messages of a religious nature on the website.
- News reports about the involvement of the foundation or its representatives in making intolerant statements.
- Donations of an unusually high value.
- Donations involving many small amounts from the same source.

Our examinations revealed that the selection of high-risk countries that payment service providers 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 payment service providers have included these countries in combination with foundations in the high risk country list. We expect payment service providers 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.

Detecting terrorist financing is therefore not a static process, but notably an area where payment services providers must make continual adjustments to the business rules. A lower limit can also be set based on the customer's risk profile: in the case of high-risk clients you would for example apply lower limits in the transaction monitoring system.

5.3.4 Periodic evaluation of business rules: backtesting

Business rules must be periodically reviewed and tested for effectiveness.

We expect payment service providers to get the the effectiveness of their transaction monitoring system to the desired level and to maintain it. In this regards we expect payment service providers to periodically evaluate this system to assess whether the business rules applied are effective or ineffective. The latter 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. Payment services providers 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, payment service providers can make any 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 produce an alarm. The aim of this is to assess whether it was correct that these transactions did not produce an alert (a true negative) or wherever certain transactions are are in fact now indicative of unusual behaviour (a false negative). If false negatives are observed the institution must expand the business rules or raise threshold levels.
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 payment services provider to conduct transaction monitoring as efficiently as possible.

Good practice (in this case at a bank, but could also be of interest for larger payment institutions)

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 within 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.

5.3.5 Data-analysis

We have observed that payment services providers take various initiatives to develop more advanced technologies in order to analyse the transaction and customer data. Larger payment services providers 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 payment service providers 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, a payment service provider will reduce the risk of contributing towards money laundering or terrorist financing. This is because the payment service provider will be able to more effectively detect and anticipate unusual customer behaviour. We note however, that this only applies to larger institutions as the smaller institutions will have less data available.

When applying advanced technologies such as 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 the patterns must be “labelled” to identify what the patterns are and where they are hidden in the tested data. It is also possible to conduct this measurement based on a manual analysis of the sample checks.

Good practice

A payment services provider has an automated, self-learning system in place based on artificial intelligence, to which data from several sources can be imported and then used to identify financial flows in real time. In this respect, historical transactions are a determining factor in identifying the potentially unusual nature of expected transactions.

5.3.6 Transaction pattern analyses

With the help of a transactions monitoring system, payment service providers can detect transaction patterns or networks or combinations of transactions. This is understood to mean a set of transactions of one or several clients 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.

Good practice

A Payment service provider has several customers that trade in gold. The pattern analysis shows that two large payments were made close together with the same IBAN number to purchase gold at two different dealers. It is notable that one person made purchases at two different dealers within a short period of time. The payment service provider reports both unusual transactions to FIU-NL.

5.3.7 IT control measures to safeguard quality and completeness of data

Payment service providers safeguard 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. Payment service providers 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 you 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?

During our examination, we established that for various payments service providers, the developers of the business rules have access to the production, test and approve all environments of the transaction monitoring system. This means that developers are able to make use of their rights to directly (without the intervention of the responsible owner) adjust business rules for transaction monitoring in the production

environment. 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.

At the payment services providers 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.

It was striking the majority of the payment services providers we examined were subject to a key-man exposure risk regarding the transaction monitoring system: 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.

5.4 Alert handling and notification process

As described above, payment services providers 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 payment service provider's notification duty is essential for detecting money laundering and terrorist financing.

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

5.4.1 Alert handling process

Payment services providers 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

A payment services provider must have procedures and working processes in place to assess and handle alerts. We expect a payment services provider 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 also expect a payment services provider to document, for each alert, the considerations and conclusions on which it has based its decision to either close the alert or report it as unusual to FIU-NL. As described earlier it is important in this respect to document where the transaction in question reflects the customers 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.

At the payments services providers we examined, we observed that escalation of alerts to the second line was largely absent from the alerts handling process. It is therefore important that payment services providers 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 the payment services provider to be able to adequately substantiate any conclusion, after consideration of the risk to not notify the FIU-NL.

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

One of the payment service providers we examined, with several foreign gambling site customers, distributed high gambling winnings (EUR 60,000). When asked whether this was usual, the reply was that it was such high payouts were usual for these sites. The institution could not see the stakes deposited by the parties in question, as the merchants used another payment services provider for this.

There is insufficient follow-up of the alert if it is closed solely on the grounds that the distribution of high amounts fits within the transaction profile. Payment services providers must also consider the risk of facilitating these payments, where they are unable to see the stakes deposited.

5.4.2 Capacity and resources to assess alerts

We expect payment service providers 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 payment services provider. To achieve this, the payment services provider can prepare KPIs defining estimated time for dealing with every type of alert. These KPIs must of course be periodically evaluated.

Good practice

One of the payment services providers from our thematic examination worked on the principle of 'quality before speed' when handling alerts.[19] Alert analysts 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.

19 Speed means dealing with alerts as quickly as possible in order to prevent backlogs.

5.4.3 Notification process

Payment service providers must have an adequate process for notification and dealing with alerts. They must ensure they fully and immediately notify FIU-NL of 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 they 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, they run the risk that FIU-NL and the law enforcement services will misinterpret the relevant information. If an incident does occur payment service providers must of course report it to DNB.[20]

Payment service providers must of course ensure that they fully and immediately notify FIU-NL of executed or proposed unusual transactions.[21] 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. Notifications based on subjective indicators should also clearly describe why the transaction or series of transactions is unusual. Payment service providers must also supply as much additional information as possible from the analysis about both the payer and payee (also for example information from open sources and about transaction patterns).

Payment service providers 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. This also means that all relevant information relating to notifications is kept confidential, with due regard

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

21 FIU-NL will check all the reported transactions against information from the databases of various investigative authorities for example. FIU-NL will also analyse transactions at the request of the investigative authorities or foreign FIUs. In addition, FIU-NL takes a thematic approach to investigating unusual transactions. This involves analysing transactions to determine their relevance for the law enforcement and investigative authorities. If this is the case the unusual transaction is declared suspicious and is reported. Apart from in exceptional situations, the payment service provider will be notified that the transaction has been declared suspicious. FIU-NL publishes relevant information on its website for each reporting group, including cases, see https://www.fiu-nederland.nl/en/legislation/relevant-cases. For further information and questions about unusual transactions, visit https://www.fiu-nederland.nl/en or call +31 88-6629500.

to the conditions and exceptions provided for in the law. The payment services provider establishes the guiding principles for this in its policies and procedures. We expect that the payment services provider ensures 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 payment services provider 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 payment services provider takes the results of this analysis into account for the customer's current risk assessment.

Good practice

A payment services provider has a customer that operates a bitcoin exchange. The customer is classified as high risk and as a result its transactions are subject to additional scrutiny. Analysis shows several instances of large bitcoin purchases using the same IBAN. The payment services immediately reports these transactions to FIU-NL.

5.4.4 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 where that 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 payment services provider receives feedback from FIU-NL stating that the report of the suspicious transaction has been passed on to the investigative authorities, the institution reassesses the customers risk profile and if necessary adjusts it.

We expect that payment services providers will 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 payment services providers, 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.

5.4.5 Objective indicators for automatic notification

In view of the nature of their activities various payment service providers often 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.

Payment service providers must always report certain transactions to FIU-NL, for example credit card transactions over EUR 15,000.[22] When an institution fails to meet its notification duty – even if this is not deliberate – it constitutes an economic offence.

22 The Appendix to Article 4 of the *Wwft* Implementation Decree lists the indicators based on which reports must be submitted.

A payment service provider we examined indicated that due to facilitating a high weekly number of credit card transactions over EUR 15,000, it had stopped reporting them to FIU-NL. It cost too much time to manually complete the form for FIU-NL, and there was no capacity available to do this. When asked why there was no tool available to automatically report these transactions to FIU-NL the reply was that there was no capacity available to do so.

5.5 Governance

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

The principle for assessing 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 payment service providers 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. Payment service providers should of course always have an independent compliance function[23] and an independent internal control function, particularly the latter.

23 Section 21 of the Decree on Prudential Rules for Financial Undertakings (*Bpr*).

Our examinations have shown that payment services providers have set up governance of transaction monitoring in various ways. Several payment services providers did not have this second-line control of the transaction monitoring activities carried out by the first line.

Many payment service providers also did not have any controls in place for customer research conducted by the second line. During the examination we also noted that not all of the institutions had an independent internal control function (the third-line function, primarily the internal or outsourced audit function) which through periodic audits evaluates the setup, existence and operation of the transaction monitoring system and process. We expect the payments services provider'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.

We expect payment service providers 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. They must also ensure that the quality assurance task for transaction monitoring is placed with the second line (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 payment services providers 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. DNB expects compliance's periodic accountability report to contain explicit management information about the most important results of its transaction monitoring.

5.6 Training and awareness

Payment service providers offer their staff tailored training programmes. Staff are aware of the risks of money laundering and terrorist financing.

We note that payment service providers have included training sessions about the Wwft in a training 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 payment service providers can make use of the cases that FIU-NL publishes every two weeks.

Good practice

One of the payment service providers we examined offers 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 payment services provider we examined has 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.

Glossary

Alert
A signal indicating a potentially unusual transaction.

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

Backtesting
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.

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

Customer due diligence
An investigation of the customer as defined in Section 1of the Wwft.

Customer risk profile
Classification of customer according to risk category, as set out in the DNB Guidance on the Wwft and the Sanctions Act.

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

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 are 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.

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

Continuous monitoring
Ongoing monitoring and control.

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 document 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 payment services providers to interpret and implement the statutory requirements.

DeNederlandscheBank
EUROSYSTEEM

De Nederlandsche Bank N.V.
P.O. Box 98, 1000 AB Amsterdam
+31 (0)20 524 91 11
dnb.nl