boulevard de Berlaimont 14 – 1000 Brussels
Tel: +32 2 221 38 12
Company number: 0203.201.340
RLP (Trade Register) Brussels
www.nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

Communication

Public

Brussels, 10 October 2023

Reference: NBB_2023_08

Contact person:
Charlotte le Beau de Hemricourt / Stéphane Folie
Phone +32 2 221 56 35 / 31 41
charlotte.lebeaudehemricourt@nbb.be /
stéphane.folie@nbb.be

Horizontal analysis of a sample of transactions carried out through tied agents of various payment institutions

Scope

Institutions engaged in money remittance that fall within the scope of the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash.

Summary/Objectives

The Bank has performed a horizontal analysis of a sample of transactions carried out through tied agents of various payment institutions (money remitters) under its supervision. This communication aims to highlight points of attention and best practices for the sector as a whole.

Structure

1) Supervision of agents
2) Data quality
3) Due diligence measures
4) Atypical facts and transactions

Dear Madam,
Dear Sir,

As part of its supervisory powers with regard to anti-money laundering and countering the financing of terrorism (hereinafter “AML/CFT”), the National Bank of Belgium (hereinafter “the Bank”) has performed a horizontal analysis of a sample of transactions carried out through tied agents of various payment institutions engaged in money remittance that are subject to its AML/CFT supervision.

Based on the analyses performed and additional information received, the Bank has identified best practices but also shortcomings in the supervisory procedures and systems of certain institutions. These are organised around the following four themes: supervision of agents, data quality, due diligence measures, and atypical facts and transactions.

The main findings of the Bank’s analysis are set out below, along with its expectations and recommendations.

A copy of this communication will be sent to your institution’s accredited statutory auditor(s)[1].

Yours faithfully,

Pierre Wunsch
Gouverneur

[1] Where applicable.

MAIN FINDINGS OF THE HORIZONTAL ANALYSIS

The Bank has performed a horizontal analysis of transactions carried out in 2021[2] through tied agents of various payment institutions engaged in money remittance (hereinafter “money remitters”) subject to AML/CFT supervision. The Bank carried out a similar analysis in 2018, on the basis of which it published Communication NBB_2018_21 for the attention of the sector. This new communication is intended to supplement the previous one. As a reminder, the first analysis mainly highlighted the following:

- certain cases revealing shortcomings in the supervision of agents;
- the poor quality of customer information collected, making it difficult to monitor transactions properly;
- post-transaction scenarios to identify one-to-many and many-to-one schemes being applied over fixed periods expressed in months or quarters and not “floating” periods of a certain number of calendar days, or the absence of adequate scenarios to identify the activities of money mules.

To carry out its analysis, the Bank selected five payment institutions operating in Belgium and subject to AML/CFT supervision by the Bank that represent a very significant market share of the remittance business based on the transfer of funds through agents. Transactions carried out via a digital application were not included in the analysis.

For each of the institutions chosen, the Bank selected two points of service (i.e. agents) using a risk-based approach. These agents were selected based on the fact that the average amount of transactions carried out at their point of service was higher than the averages recorded for all tied agents of the payment institution.

The analysis covered all transactions carried out at each selected point of service over a twelve-month period, and included a materiality threshold.

This communication aims to set out the main findings and points of attention identified in the analysis, as well as best practices for the sector as a whole.

In this respect, it may also be useful to refer to the Report of the European Banking Authority of 16 June 2023 on ML/FT risks associated with payment institutions[3].

The main findings are organised around the following four themes: supervision of agents, data quality, due diligence measures, and atypical facts and transactions.

2 The analysis took into account the responses to the questionnaire on inherent ML/FT risks communicated to the Bank by 31 May 2022 in accordance with Circular NBB_2022_06 (the so-called "AML/CFT Questionnaire").

3 Report on ML/TF risks associated with payment institutions.pdf (europa.eu). In addition to outlining the risks traditionally associated with the sector, this Report also highlights emerging risks arising from new business models or new activities that may constitute a gateway to the financial system for ML/FT operations.

FINDINGS AND BEST PRACTICES IDENTIFIED

SUPERVISION OF AGENTS

The Bank notes that certain agents in the sample stand out positively in terms of both the quality of the data collected and the limited number of transactions that could raise questions. This should be seen in connection with the supervision of agents, which, based on the sample analysed by the Bank, has improved overall in terms of both frequency and quality compared with the 2018 analysis. However, the Bank notes significant disparities between money remitters in, on the one hand, the depth and quality of the analyses carried out in preparation to the visit to the agent and, on the other hand, in the follow-up to the visit as part of the supervision of the agent (e.g. transaction analyses and verification of the quality of the registered data).

Given the crucial role played by agents in payment institutions' AML/CFT systems, the Bank once again stresses the importance of supervising agents and following up on this supervision. It is essential that payment institutions develop and implement an annual agent review plan that adequately covers their agent network using a risk-based approach.

A best practice identified is to analyse, for the supervised agent, the volume of transactions close to but not exceeding the institution's monitoring thresholds. In addition, the supervision of agents should not be limited to periodic visits to them. Another best practice identified is to review the transactions carried out by agents for their own account.

DATA QUALITY

The Bank notes a significant improvement in customer identification data compared with the previous analysis. The more extensive and systematic use of electronic identity card (eID) readers makes it easier to identify customers correctly by e.g. preventing data entry errors.

However, the Bank notes that several money remitters still have a number of customers registered under multiple "unique" identifiers (hereinafter "IDs") in their databases. These duplicate entries for the same customer compromise detection controls that are based on the transaction volume (in number and amount) recorded for each unique ID of the customer.

With regard to data on the beneficiaries of customers, the Bank notes that, in the majority of cases, there is no system that effectively prevents duplicate entries for the same beneficiary. As a result, the same beneficiary may be assigned different IDs. The Bank considers that, at the very least, when the same customer sends funds on several occasions to the same beneficiary, the latter should have only one ID in the relevant money remitter's system. Duplicate entries for the same person render checks based on the consolidation of transaction data by customer and/or by beneficiary ineffective.

DUE DILIGENCE MEASURES

Upon exceeding certain transaction thresholds, in terms of amount or number of transactions, an alert may be generated requiring additional information to be provided, the transaction to be approved by the compliance function or, where appropriate, the transaction to be blocked. The Bank notes a wide disparity in the thresholds used by money remitters to determine the due diligence measures to be applied.

Institutions are required to develop and periodically review an overall risk assessment, in which they identify the risks to which they are exposed and set out measures to reduce these risks, including the application of appropriate thresholds. These thresholds should be determined and justified on the basis of this assessment, and this process should be duly documented. If the thresholds are set too high, the due diligence measures laid down by the institution are purely theoretical, as they will almost never be applied in practice. In this case, the thresholds cannot be used to reduce the risks identified. The Bank therefore urges money remitters to ensure that their thresholds are appropriate for the transactions carried out by their customers.

With regard to the period over which transaction thresholds are calculated, the Bank stresses the importance for institutions to also define thresholds calculated over average and long periods. It notes that the majority of scenarios designed to identify one-to-many and many-to-one schemes are calculated over short periods. These scenarios should therefore be supplemented with thresholds adapted to longer periods. In addition, they should be calculated based on “floating days” (e.g. a transaction carried out on February 24 is added to all transactions carried out by the same customer since January 25), rather than to calendar months.

Furthermore, transaction thresholds alone are not sufficient to determine the due diligence measures to be applied. If they have not yet done so, institutions should establish scenarios that take other risk factors into account. In order to implement the risk-based approach and allocate the institution's resources in the best possible way, transaction thresholds can be combined and adapted according to these other risk factors. These risk factors may include, but are not limited to:

- the number of beneficiaries of the customer as determined based on the institution’s overall risk assessment. This number may vary depending on the corridors used, the origin of the customers or the characteristics of suspicious transactions reported in the past;
- the means of payment used for incoming and outgoing funds: cash transactions remain riskier than other types of transactions (e.g. via bank card).

The Bank has also noted shortcomings in the due diligence measures defined and applied by money remitters. It has found that, in the majority of cases, only purely declarative information is requested from customers when certain thresholds and/or a certain level of risk are/is exceeded and/or certain scenarios are triggered. In addition, the information requested from customers is generic and limited, making it difficult to use their answers for due diligence purposes. For example, the source of funds is very often reported as “salary” and the customer’s occupation is stated as either “worker” or “pensioner”, regardless of the amount of the transactions carried out by the customer. Furthermore, information provided by the customer on different occasions is sometimes contradictory (e.g. relationship with the counterparty), and these contradictions do not result in an in-depth ex-post analysis.

A declarative approach is acceptable up to a certain level of risk but, above that level, it is necessary to obtain evidence and carry out a detailed analysis to corroborate the information provided by the customer. The appropriate level of risk above which additional due diligence measures are required should be determined, justified and documented by the institution. The Bank reiterates that the overall risk assessment is the central element of the institution’s AML/CFT system. It enables the institution to identify and appropriately manage the inherent ML/FT risks to which it is exposed through its activities, and to implement appropriate risk reduction and due diligence measures.

In line with the above, the Bank notes that very few of the transactions in its sample were analysed in terms of the customer’s financial capacity and, consequently, the source of funds. In many cases, the institution did not analyse the consistency of the transaction with the customer's declared income, even for large transactions. The Bank also found that institutions very rarely collected evidence, even though, in the case of a large cash payment, they could request and analyse payslips or account statements proving the withdrawal. In this regard, the Bank notes that money remitters should ask questions if a customer withdraws cash in order to transfer funds, when remuneration is systematically paid by bank transfer and the money remitter offers the option to pay by card. The Bank also urges institutions to define criteria for the maximum age of supporting documents requested from customers, particularly in the case of account statements.

The Bank deems it insufficient for institutions to be satisfied with the payer being located in a “high-income country” to justify the latter’s economic capacity to make large transactions. Nor is the existence of a "link" between the payer and the beneficiary's country sufficient to justify transactions to that country without applying any due diligence measures.

ATYPICAL FACTS AND TRANSACTIONS

Although the Bank notes that, overall, the quality of post-transaction monitoring has improved compared with the 2018 analysis, there are still some exceptions in the sector.

Best practices

Before highlighting some of the weaknesses identified, the Bank would like to list, in a non-exhaustive manner, some of the best practices identified in this area.

a) The implementation of a post-transaction scenario based on the customer's home address. The Bank considers that where a certain number of customers are domiciled at the same address, institutions should determine whether these customers' transactions are atypical and, in particular, assess their financial capacity compared to the cumulative amount of their transactions.
b) The implementation of a blocking control preventing customers from circumventing the application of pre-transaction scenarios. Customers who initiated a transaction that triggered a request for additional information may cancel the transaction but will still be required to provide this information for the next transaction, regardless of the amount or nature of that transaction.
c) Scenarios calculated over "floating" periods have become the norm within the sector. This is a significant improvement compared with the Bank's 2018 analysis.

These best practices have enabled some money remitters to identify, for example, suspicious networks using many-to-many schemes. Although these schemes are difficult to identify, some institutions combine several types of monitoring scenarios to detect this type of behaviour. By combining scenarios aimed at identifying one-to-many and many-to-one schemes, coupled with a detailed and comprehensive analysis of transactions, they are able to detect many-to-many schemes. However, institutions should ensure that the necessary analyses are carried out as soon as possible and, where appropriate, report suspicions to CTIF-CFI without delay.

Points of attention

Despite the improvements above, the Bank still notes certain shortcomings that remain relatively widespread in the sector.

a) The Bank found cases where several large transactions were placed with the same agent by different customers within a very short period of time (i.e. a few minutes), which may give the impression that these customers went to the agent together. Apart from the atypical nature of these facts, this is a common and well-known practice for so-called money mules. The Bank would like to reiterate its expectations in this area. Firstly, it expects agents to be trained to detect such transactions and to have and use a direct reporting system to alert the institution's second line of defence. Secondly, it expects institutions to implement specific ex-post scenarios and controls. Some money remitters have developed such scenarios to identify transactions where virtually identical amounts are placed with the same agent in a short space of time, as well as to detect customers who make (incoming and/or outgoing) transactions with more than two agents in a very short space of time.
b) The Bank urges money remitters to analyse the relevant statistics and, if necessary, to increase the level of risk associated with certain specific corridors that are considered "outliers" compared to the others. The Bank insists that it must be possible to distinguish particularities (both the risk and the use of the specific corridor) in certain parts of the territory for which statistical anomalies have been observed (e.g. number and average amount of transactions that are substantially higher than expected). This information may be taken into account when analysing transactions as part of the post-monitoring process (e.g. analysis of the activity of certain corridors) as well as part of the agent oversight and when reviewing transactions placed with agents.
c) The Bank reiterates the importance of analysing atypical facts, including transactions that are not completed or are cancelled after certain thresholds and/or scenarios are triggered and, hence, due diligence measures are applied. This is especially important when the institution itself blocks

a transaction for compliance reasons. The institution should analyse such facts and, where appropriate, file a suspicious transaction report. As a reminder, the Bank has long stated on its website (comments and recommendations by the NBB regarding due diligence on business relationships and occasional transactions and detection of atypical facts and transactions) that institutions should consider it an atypical fact "*when the customer renounces in extremis, unexpectedly and without credible explanation, to the execution of a transaction as soon as he is informed of the fact that such execution implies that he provides information as to his identity or that of the beneficial owners, that he discloses the purpose of the transaction or the origin of the funds involved, etc.*".

d) In a number of cases, the Bank notes a lack of due diligence with regard to customers who were the subject of a suspicious transaction report to CTIF-CFI. As a reminder, institutions that have reported a suspicious transaction are required to carry out a new individual ML/FT risk assessment, taking into account in particular the fact that the customer concerned has been the subject of a suspicious transaction report, in order to decide whether to maintain the business relationship, subject to the implementation of due diligence measures adapted to the risks thus reassessed, or to terminate the relationship (see Article 22 of the Regulation of the NBB of 21 November 2017 on the prevention of money laundering and terrorist financing). In addition, as stated on the Bank's website (see the comments and recommendations by the NBB on the reporting of suspicions, point 2.6), any information that could invalidate, confirm or modify the information included in a suspicious transaction report should be communicated immediately to CTIF-CFI, regardless of the amount and especially if the customer concerned carries out new suspicious transactions.

***