NATIONAL BANK OF SERBIA

ADMINISTRATION FOR SUPERVISION OF FINANCIAL INSTITUTIONS
BANK SUPERVISION DEPARTMENT

ANALYSIS OF BANKS' RESPONSES TO THE QUESTIONNAIRE ON ACTIVITIES REGARDING AML/CFT RISK MANAGEMENT

for the period April–September 2017

December 2017

Introductory note

To enhance supervision efforts, in 2006 the National Bank of Serbia established the practice of off-site monitoring and analysis of banks' activities regarding AML/CFT risk management. The analysis is carried out twice a year on the basis of data submitted by banks in the form of replies to the Questionnaire on Banks' Activities Regarding AML/CFT Risk Management (hereinafter: Questionnaire).

The Questionnaire covers the following periods: from April to September of the current year and from October of the current to March next year.

The analysis of the Questionnaire aims to:

- provide an overview of the state of affairs in the process of identifying, measuring and managing AML/CFT risk in the overall banking system in the most recent six-month period,
- provide off-site monitoring of the development of AML/CFT risk management system in the overall banking system,
- detect any weaknesses and timely inform banks about potential risk exposure.

The Questions in the Questionnaire are sorted into seven groups:

Part I: General bank data

Part II: Bank's activity

Part III: Clients

Part IV: Transactions

Part V: Reporting to the Administration for the Prevention of Money Laundering (Administration)

Part VI: Employee training

Part VII: Internal audit and internal control

The analysis is based on data for the April –September 2017 period submitted by banks to the NBS in the form of the Questionnaire responses. The presented data may, therefore, exhibit certain inconsistencies and are mostly analytical in nature. Of the 30 banks operating in Serbia in the period covered by the Questionnaire, 28 submitted their responses within the set deadline and two banks after that deadline.

Contents:

I KEY FINDINGS

The overall conclusion is that, as in the previously analysed period, banks had medium exposure to AML/CFT risk.

Due to the size of the sector and the branched out network, the number and type of clients, as well as the number of performed transactions, banks are exposed to AML/CFT risk. Namely, as at 30 September 2017, 30 banks established business relations with clients at a total of 2,363 locations, while cash transactions could be performed at a total of 5,150 locations in Serbia. The total number of clients in the banking sector on the said date was over 12.5 million, of which around 11.9 million were natural persons (around 80,000 were non-residents), 411,000 legal persons (8,000 were non-resident legal entities) and 354,000 entrepreneurs. In the observed period, over 332 million cashless and more than 100 million cash transactions were performed.

However, the banking sector is the most organised sector in terms of taking measures to mitigate AMT/CFT risk which, in the period under review, is reflected as follows:

- 29 banks set up their own AML/CFT risk management systems applying an AML/CFT risk assessment approach and taking into account the findings of the National Money Laundering Risk Assessment;
- in their internal acts, all banks defined the transaction monitoring frequency depending on the assessed risk level, particularly for the highest-risk clients, and the duration of monitoring of connected cash transactions;
- 29 of the 30 banks use some type of software solution to monitor transactions and clients in order to detect suspicious transactions and clients. Most banks implemented more than 10 indicators of the Administration for identifying ML and/or FT transactions, while 22 banks developed their own set of indicators for identifying suspicious transactions and clients and incorporated them in their own software solution.
- the number of offers to establish a business relationship were refused due to the impossibility to take CDD actions and measures increased by 103 or 10% relative to the previous period, indicating that banks use this legal requirement as an instrument of AML/CFT risk management;
- all banks prepared lists of FT-related individuals and entities, drawing from the lists of the UN Security Council, EU and OFAC;
- all banks regulated the internal controls system by their internal acts, all banks envisaged internal AML/CFT control in their internal control plans, 24 banks stated that they had set out the AML/CFT controls in their internal audit plans for 2017;
- all banks pay due attention to training, primarily of front-office staff or the staff executing transactions.

However, despite the measures undertaken to mitigate the AML/CFT risk, some facts were detected that might have an indirect or direct impact on the quality of AML/CFT risk management and they primarily relate to the following:

- the number of cases in respect of which ten banks outsourced CDD actions and measures to a third person increased by 92,124 from the prior period. This leads us to conclude that banks using this option ought to be particularly alert when managing potential risk exposure in this segment of their operations;
- the number of transactions with clients from high-risk destinations increased by 7.56% from the previous period;
- the total number of non-resident legal persons increased by 204 from the prior period, while the number of natural persons – non-resident bank clients rose by 1,658, with the number of non-resident natural persons from high-risk countries increased by 165 from the previously analysed period;
- the number of clients per employee increased by four and the number of performed cashless and cash transactions per employee rose significantly, by 2,450 relative to the previously analysed period, which means that employees had greater workload relative to the prior period;
- the turnover of employees who perform activities and measures stipulated by the Law and who are in direct contact with clients, which is more than 10% relative to the total number of employees, rose by 13.34% compared to the previous period;
- in six banks, the compliance officer and his deputy, as well as other employees tasked with matters concerning AML/CFT, also perform other tasks on a daily basis, in addition to their activities on implementing provisions of the Law;
- the number of suspicious transactions reported to the Administration decreased by 9.80% from the prior period; three banks did not report any suspicious transactions and one bank reported 20.92% of the total suspicious transactions reported to the Administration, which certainly suggests a need for additional training.

In their responses, all banks noted that they have aligned their risk management systems and internal acts with the Decision on Risk Management by Banks (RS Official Gazette, Nos 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 – other decision, 43/2013, 92/2013, 33/2015, 61/2015, 61/2016 and 45/2011 – hereinafter: Decision). However, based on the analysis of responses to subsequently provided questions regarding the implementation of the Decision, it was determined that banks do not fully implement the Decision in terms of AML/CFT risk.

Firstly, in the Risk Management Strategy (hereinafter: Strategy), certain banks did not include the AML/CFT risk in accordance with the definition stated in the Decision. Also, in certain cases the Strategy does not include long-term goals, risk propensity or even basic principles of acceptance and management in terms of the stated risk. The risk management policy does not regulate all areas stipulated in the Decision, namely: manner of organising AML risk and clear distinction of responsibilities of employees in all stages of the process, manner of assessing bank's risk profile and methodology for identifying and measuring this risk, i.e. assessing the AML/CFT risk, measures for mitigating the risk and rules for implementing those measures. Not all banks managed to fully establish adequate internal organisation, i.e. organisational structure, including the obligation requiring that authorisations and responsibilities for matters pertaining to AML/CFT risk management may not be entrusted to that member of the Executive Board who has already been entrusted with authorities and responsibilities about assuming this risk, while some banks did not define the jurisdiction and responsibility of any member of the Executive Board for managing AML/CFT risk. Lastly, it is underlined that in a large majority of cases the obligations stipulated by the Decision, which pertain to the AML_/CFT risk, are regulated by inadequate internal acts, e.g. procedures, guidelines, rulebooks and instructions in stead of the Strategy or politics for managing risks.

Failure to regulate the process of AML/CFT risk management can result in significant exposure of the bank and other risks, primarily reputational risk and risk of penalties and sanctions pronounced by a regulatory body, and consequently legal and operational risks and the risk of unconscientious business practice, therefore it is necessary that banks once again look into the implementation of the Decision when it comes to the AML/CFT risk and immediately take all necessary activities in order to ensure its appropriate implementation.

II GENERAL BANK DATA

As at 30 September 2017, there were 30 banks licenced by the NBS in the Republic of Serbia. According to Questionnaire responses, banks have a wide organisational network and establish business relationships with clients at a total of 2,363 locations, or 48 locations more than in the prior analysis period. Six banks can establish business relationships at up to 10 locations, nine banks at between 11 and 50 locations, eight banks at between 51 and 100 locations, five banks at between 101 and 200 locations, and two banks at over 200 locations.

At sector level, a cash transaction can be made at a total of 5,150 locations (down by 96 locations from the prior period). Six banks have up to 10 such locations, eight banks between 11 and 50 locations, 10 banks perform cash transactions at between 51 to 100 locations, two banks have between 101 and 200 such locations and four banks over 200 such locations.

Total banking sector employment as at 30 September 2017 was 23,344 persons, while the number of employees directly engaged in client- and transaction-related operations was 14,969 (64.12%). The analysis of staffing levels reveals a continuation of the staffing reduction trend, with total employment at end-September down by 462 persons relative to end-March 2017, or by 671 (2.79%) relative to the same period in 2016.

At banking sector level, the average number of clients per employee directly engaged in client- and transaction-related operations was 845, while the number of cashless and cash transactions per employee was 28,874[1] in the April–September 2017 period. The number of bank clients per employee increased by four from the prior period, and the number of cashless and cash transactions per employee rose significantly by 2,450 from the previously analysed period. This means that, in the analysed period, employee workload increased from the prior period due to a rise in the number of clients and the total number of cash and cashless transactions carried out, while the share of employees directly engaged in client- and transaction-related operations relative to the total number of employees remained largely unchanged.

In nine of the 30 banks (30%), the turnover of AML or front-office staff was between 10% and 50%, while in all other banks bank it was below 10%. The 13.43% increase in the share of banks where the turnover of these employees is between 10% and 50% relative to the previously analysed period indicates the possibility of additional exposure to AML/CFT risk. This fact suggests that banks need to further upgrade or automatize to the largest possible extent their processes and the established AML/CFT system in order to enable higher-quality implementation of actions and measures for detecting and preventing money laundering and terrorism financing, and adequate AML/CFT risk management.

[1] The amount concerns the number of transactions excluding e-banking transactions as the latter are performed without direct engagement of bank employees.

Further improvement of IT solutions within existing systems can have an important impact on the level of operating risks that might arise through human error and enable more efficient human resource management (especially in conditions of a reduced number of employees), by enabling employees to dedicate more attention to improving the quality of clients' business analysis, i.e. their transactions which the banking system sets out based on the programmed parameters – indicators.

III COMPLIANCE OFFICER FUNCTION

As Questionnaire responses reveal, 23 banks have a special organisational unit which deals exclusively with implementing the Law, whereas in seven banks these tasks are performed by other organisational units. In six banks, the compliance officer/his deputy, as well as other employees tasked with matters concerning AML/CFT, also perform other tasks on a daily basis, in addition to their activities on implementing provisions of the Law.

The compliance officer is in a managing position in ten banks, while in 20 banks this is not the case. The share of banks where the compliance officer is in a managerial position increased by 6.66% relative to the previously analysed period.

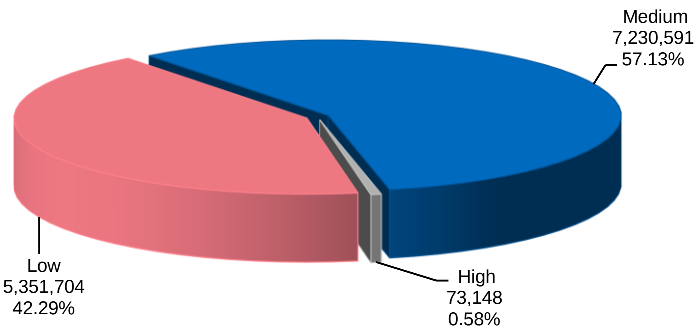
All banks made sure that compliance officers and their deputies cooperate with other organisational units by regulating this cooperation in their internal acts.

In view of the increasing the significance of the ML and in particular of the FT risk worldwide, the strengthening of the function of the compliance officer and his deputy should be an imperative for the domestic banking sector as well.

IV ACTIVITY OF BANKS

In accordance with the NBS Decision on the Guidelines for Assessing the Risk of Money Laundering and Terrorism Financing (RS Official Gazette, Nos 46/2009 and 104/2009), all banks, except one, prepared risk analyses and assessment of exposure to the ML/FT risk, taking into consideration the findings of the National Money Laundering Risk Assessment. Depending on the assessment of client exposure to the ML/FT risk, banks classified their clients as low-, medium- or high-risk, as shown in Chart 1.

Chart 1 **Banking sector clients by degree of risk as at September 2017**



According to submitted data on client classification by degree of exposure to the ML/FT risk, 13 banks classified over 70% of their clients in the low-risk category, while 15 classified the majority of their clients (over 80%) in the medium-risk category.

Questionnaire responses show that, despite classifying 5,351,704 of the 12,655,443 clients in the low-risk category, banks took simplified CDD actions and measures in respect of 1,116,500 clients only, which is broadly the same as in the prior period.

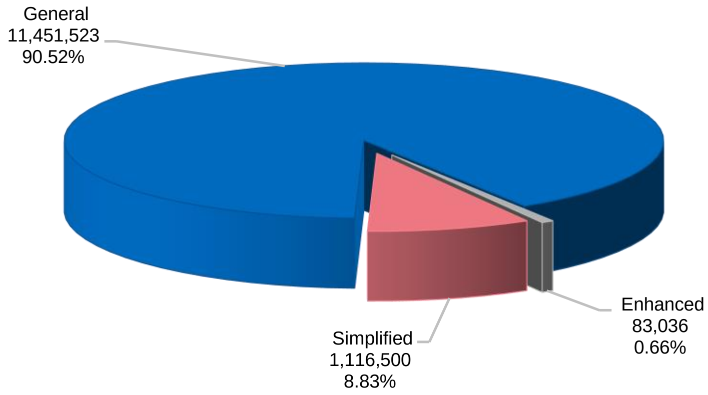
The table below shows a comparative overview of clients by risk level and by CDD actions and measures:

Table 1 **Structure of banking sector clients by risk level and actions and measures applied**

Risk level	No of clients	% share	Applied measures	No of clients	%share
Low	5,351,704	42.29	Simplified	1,116,500	8.82
Medium	7,230,591	57.13	General	11,451,523	90.52
High	73,148	0.58	Enhanced	83,036	0.66
			No measures	4,384	
	12,655,443	**100**		**12,655,443**	**100**

Pursuant to the Law, banks are required to apply general, simplified or enhanced CDD actions and measures. In the analysed period, general actions and measures were taken in respect of 90.52% clients at banking sector level. Enhanced actions and measures were taken in respect of 0.66%, and simplified in respect of 8.82% clients, as shown in Chart 2.

Chart 2 **Banking sector clients by CDD actions and measures as at September 2017**



Of the total number of cases where simplified CDD actions and measures were taken, in just two banks they were taken in respect of 996,740 clients, while all other banks took these measures in respect of 119,760 clients. Questionnaire responses also show that 13 banks took simplified CDD actions and measures in respect of low-risk clients, five banks did not take these measures at all, while 12 banks took them in respect of only a small proportion of low-risk clients.

In their responses, all banks stated that their internal acts define monitoring intervals on the basis of client risk level.

Banks stated that they terminated a business relationship with a client if they were not able to take CDD actions and measures. According to Questionnaire responses, in the April–September 2017 period, 11 banks terminated their business relationships with 11,857 clients. Of this, only one bank did so with 11,053 clients due to their not updated data in the system and clients' passive status over a period longer than three years. In the observed period, 19 banks did not report a single case of terminating a business relationship. Ten banks refused the offer to establish a business relationship and/or execute a transaction in 1,133 cases, due to the impossibility to take CDD actions and measures. Of this number of cases, 1,089 pertain to one bank only.

Ten banks outsourced individual CDD actions and measures to a third person and thus obtained data and documentation about 399,280 clients (of which 399,042 were clients of two of these banks). All banks stated that they kept official written record of the assessment of grounds to suspect money laundering or terrorism financing in respect of all cases in which they refused the offer to establish a business relationship or execute a transaction for the above reasons.

All banks replied that they received no applications to open anonymous accounts, coded or bearer savings passbooks, etc. aiming to conceal the identity of the client.

Information systems of all banks have the capacity to detect multiple connected cash transactions of the same client amounting to a total of EUR 15,000 or more.

All banks confirmed that their internal acts define the frequency for monitoring transactions performed by clients classified as highest-risk, as well as intervals for monitoring connected cash transactions. According to the submitted responses, 11 banks monitor connected transactions for at least one day, eight banks for a week, three banks for a fortnight, four banks for up to 30 days, one bank for three months, one for six months, one for a year, while one bank monitors connected transactions for a longer period of time, depending on the risk level.

When preparing their own lists of individuals and entities designated as related to terrorism financing, all banks stated that they mostly drew on the lists produced by the UN Security Council, EU and OFAC.

In Questionnaire responses, 29 banks stated they use special software solutions for identifying suspicious transactions and persons, and only one bank replied it did not use any such software. Banks also listed the indicators included in the software which they selected from the List of indicators for recognising suspicious transactions or persons and the List of indicators relating to terrorism financing published on the Administration's website.

The table below shows how many indicators for recognising suspicious transactions relating to money laundering published on the Administration's website were included in the software solutions of 27 banks:

Table 2 **Number of included indicators relating to money laundering**

Number of included indicators for banks	Number of banks
Fewer than 10	6
10–19	14
20–29	6
30–37	1

According to Questionnaire responses, indicators for recognising FT-related suspicious transactions are included in the software of 27 banks, as follows:

Table 3 **Number of included indicators relating to terrorism financing**

Number of included FT-related indicators	Number of banks
Fewer than 5	17
5–10	7
More than 10	3

Also, 22 banks stated 333 other indicators (from their own indicator lists) which they included in their software for the recognition of suspicious transactions and/or persons.

The table below shows the number of banks applying their own indicators:

Table 4 **Number of included indicators developed by banks**

Number of included indicators developed by banks	Number of banks
Fewer than 5	4
5–9	6
10–19	9
20 to 25	0
50	3

Other indicators included in software solutions of banks are most often indicators identified from experience in monitoring client transactions and operations which can be expressed in the programming language and, as such, implemented in the information system. The fact that the number of own indicators increased by nine relative to the previous period indicates that banks are increasingly active in raising the quality of AML/CFT activities, going even beyond regulatory requirements in order to upgrade their ML/FT risk management.

To efficiently manage the ML/FT risk, all banks should continue enhancing their system for monitoring transactions and clients in order to ensure timely risk identification and assessment, and take appropriate actions and measures in respect of their clients.

VI INTERNAL AUDIT AND INTERNAL CONTROLS

According to Questionnaire responses, all banks regulated the internal controls system in their internal acts.

In the majority of banks, internal control of implementation of the Law is within the remit of the organisational unit in charge of internal audit, and at the same time of other organisational units such as the compliance unit, unit in charge of supervising "network" operations or the unit in charge of AML/CFT activities only.

According to Questionnaire responses, internal audit plans of 24 banks envisage AML/CFT-related audit of their operations in 2017. During the past year 20 banks carried out audit of this segment of their operations, while one bank is still in the process of conducting the audit. Of the remaining eight banks, one conducted internal audit in 2014, three in 2015 and four in 2016.

In the course of the audit of AML/CFT-related activities of the bank, 18 banks identified omissions in the bank's procedures, while two banks were unable to respond to the above question, as the audit procedure was still under way.

The most commonly identified irregularities were: incomplete client files, outdated client data, incorrect client classification by exposure to the ML/FT risk, incomplete client data entries in the bank's system or data that cannot be accessed by other employees of the bank, shortcomings in internal trainings carried out by the AML department, insufficient information in analyses of detected potentially suspicious transactions, incomplete procedural framework for AML/CFT, deficiencies or non-compliance of internal acts pertaining to different business processes, inadequate systemic solutions in terms of risk level monitoring, etc.

All banks which identified irregularities in the course of internal audit (18 banks) set deadlines for their removal; of this number, 12 banks removed the irregularities within the set deadline, while in six banks the deadline has not yet expired.

With regard to notifying the bank's Executive and Managing Boards on AML/CFT-related internal audit findings, the compliance officer informed the Executive Board about its findings in three banks, whereas the Managing Board was notified about the findings in 13 banks.

In the analysis period, 28 banks conducted internal control of AML/CFT activities. Irregularities were detected in 25 banks. Most frequently, internal control findings related to the following:

- inadequate or incomplete documentation at the time of client identification for the purpose of establishing a business relationship or performing a transaction,
- outdated client records in the bank's system,
- incorrect client classification by degree of ML/FT risk exposure,

- the system's inability to fully monitor the ML/FT risk.

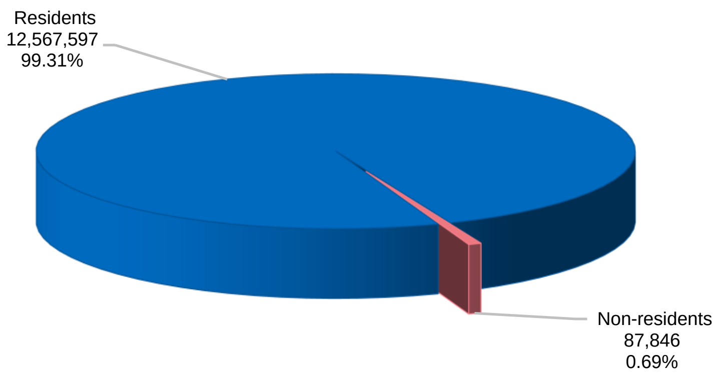
All banks which detected irregularities in the course of internal controls set a deadline for the removal of such irregularities, and 20 took measures to remove them. In seven banks, the compliance officer notified the bank's Executive Board on AML/CFT findings of internal control, while in 21 banks the compliance officer notified the bank's Managing Board of the findings.

VI CLIENTS

Charts 3 to 5 show the composition of banking sector clients based on the Questionnaire data.

Chart 3 shows the absolute and relative percentage of residents versus non-residents in the overall banking sector in September 2017.

Chart 3 **Banking sector clients in September 2017**



Relative to the prior period, the proportion of resident versus non-resident clients remained the same; at end-September 2017, residents accounted for 99.31% (12,567,597) and non-residents for 0.69% (87,846) of total clients.

As in the prior period, natural persons were dominant among resident clients (93.97%), while domestic legal persons and entrepreneurs accounted for 3.21% and 2.82% respectively, mildly increasing their share in the total number of resident clients – as shown in Chart 4 below.

Chart 4 **Resident banking sector clients in September 2017**

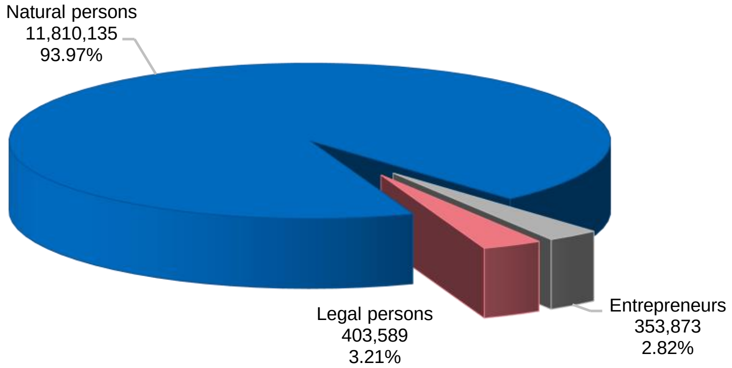


Chart 5 shows the structure of non-resident banking sector clients and the share of clients – natural and legal persons from high-risk countries and offshore countries and territories in the total number of non-resident clients.

The number of clients – non-resident natural persons increased by 1,658 to 79,764 persons (90.80%), and the number of non-resident legal persons rose by 204 from the prior period and equalled 8,082 (9.20%).

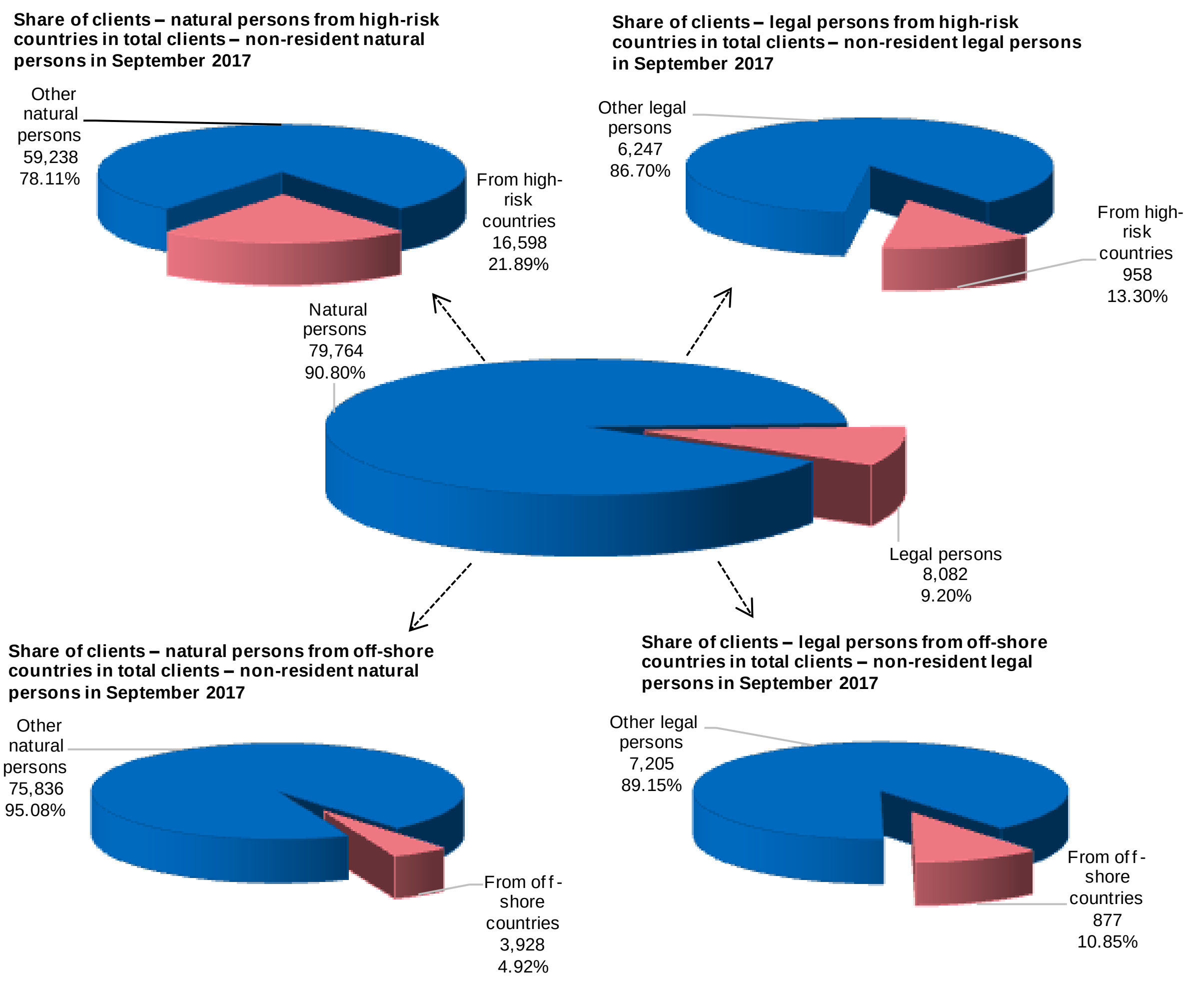
The number of non-resident natural persons from high-risk countries increased by 165 in absolute terms relative to the previous analysis period, though their share in the total number of non-resident clients declined to 21.89% (by 0.57%) due to an increase in the total number of non-resident natural persons in the analysed period. The number of non-resident legal persons from high-risk countries fell by 146 and their share in the total number of non-resident clients edged down from 16% in the previous analysis period to 13.30% in the period of this analysis.

Chart 5 also shows the share of clients from offshore countries in total non-resident clients. Offshore destinations are countries and/or territories applying double taxation policies which are very advantageous for companies that do not operate in those countries, but have a registered head office there while doing business in their local market.

Despite the increase in the total number of non-resident natural persons in this relative to the previous period, the number of natural persons from offshore countries declined from 4,944 to 3,928 persons, while in the total number of non-resident legal persons, the number of legal persons from off-shore countries edged down from 979 to 877 – as shown in Chart 5 below.

The number of clients who established a business relationship without being physically present decreased from 4,058 as at 31 March 2017 to 3,844, while the number of clients who are foreign officials equalled 773 as at 30 September 2017, an increase of six from 31 March 2017.

Chart 5 **Non-resident banking sector clients in September 2017**



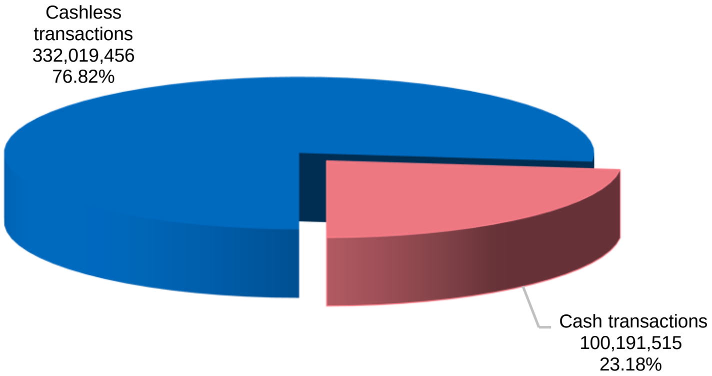
VII TRANSACTIONS

In the observed period, banks performed 332,019,456 cashless transactions, or 10.96% more than in the prior period. The number of cash transactions performed at banking sector level was 100,191,515 or 6.70% more than in the prior period. The share of cash transactions in total transactions was approximately the same as in the prior period and equalled 23.18%.

The number of cashless transactions performed by e-banking was 69,856,520 in the analysed period, up by around 6.99% from the prior period.

Chart 6 shows the structure of performed cash and cashless transactions in the banking sector in the April–September 2017 period, while Chart 6a gives an overview of cashless (excluding e-banking transactions) and cash transactions in the period from H1 2010 until and including the period under review.

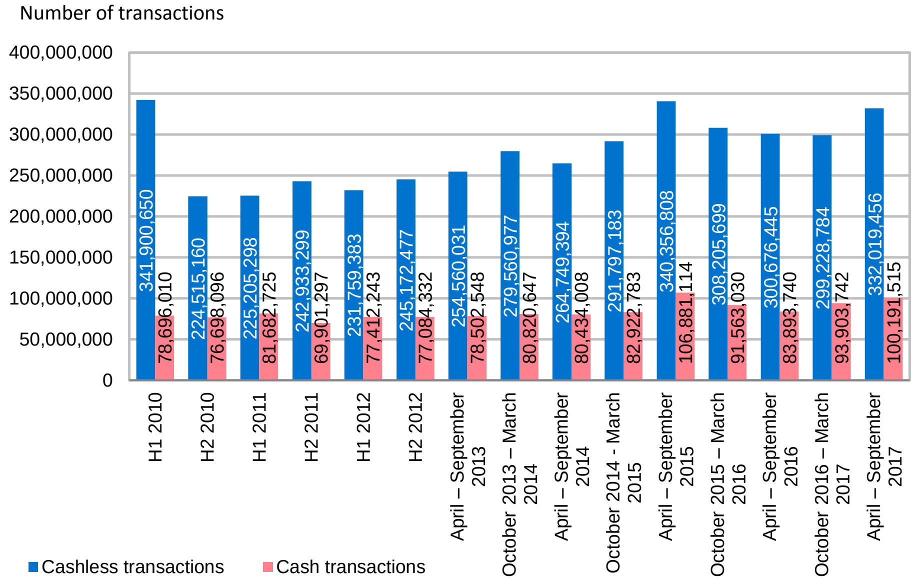
Chart 6 **Structure of transactions performed in the banking system in the April– September 2017 period**



Banks performed 197,190 cash transactions of the value of the RSD equivalent of EUR 15,000 or more at the middle exchange rate of the NBS, which is approximately 0.20% of the 100,191,515 total cash transactions made.

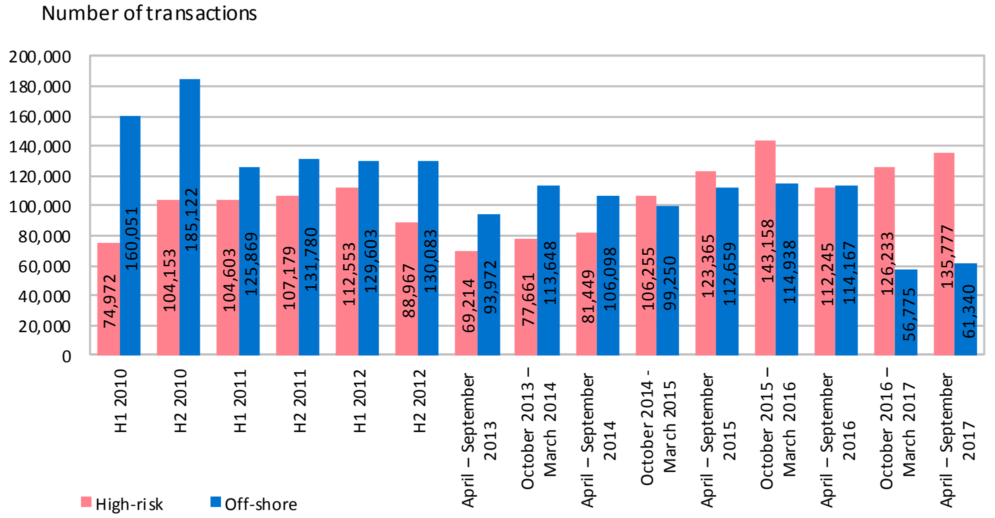
The number of such cash transactions decreased by 31,096 in absolute terms from the prior period.

Chart 6a **Structure of transactions performed in the banking sector by period**



The number of transactions with clients from high-risk geographical areas was 135,777, or 9,544 transactions more than in the prior period, while the number of transactions with clients from off-shore geographical areas was 61,340, up by 4,565 transactions from the prior period, as shown in Chart 7.

Chart 7 **Movements in the number of transactions with clients from high-risk and offshore areas by period**

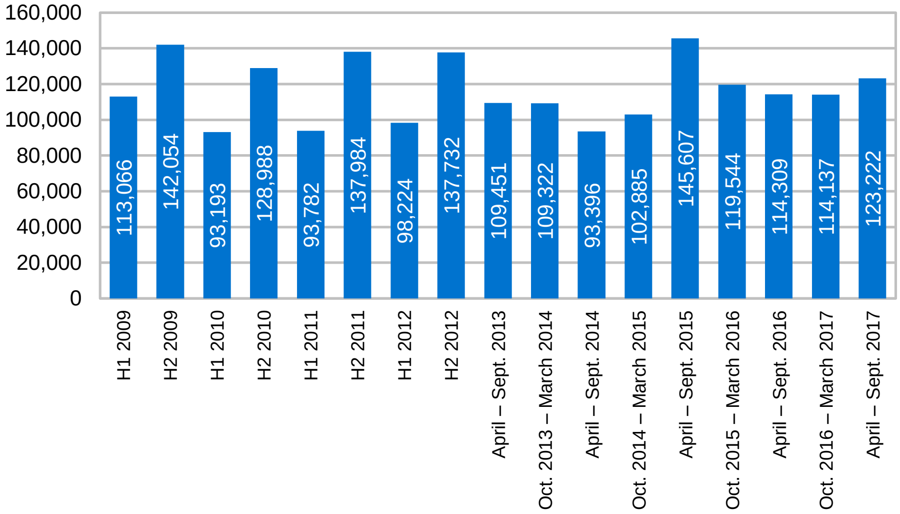


VIII REPORTING TO THE ADMINISTRATION

The number of reported cash transactions of the value of the RSD equivalent of EUR 15,000 or more at the NBS middle exchange rate as at the transaction date came at 123,222 (Chart 8) in the observed period, while the total number of registered cash transactions of the same value was 197,190. The number of reported cash transactions of the value of EUR 15,000 or more increased by 7.96% from the prior period.

Reported cash transactions of the value of the RSD equivalent of EUR 15,000 or more accounted for 62.49% of all registered cash transactions of that value, down by 5.51% from the prior period. In absolute terms, the number of cash transactions in the RSD equivalent of EUR 15,000 or more which were not reported to the Administration was 73,968. This should include transactions which banks, according to regulations, are not required to report to the Administration, and which relate to transactions of clients – public enterprises, direct and indirect budget beneficiaries, clients to which simplified CDD measures apply in accordance with the Law and cash transactions involving money transfers from one client account to another, if these accounts are held with one and the same bank, conversion of a client's account balance into another currency, where the money stays in the account with the same bank, placing account balances on fixed term deposit accounts or renewal. For this reason, the number of transactions reported to the Administration is much lower than the total number of registered cash transactions of the value of the RSD equivalent of EUR 15,000 or more.

Chart 8 **Number of cash transactions worth ≥ EUR 15,000 reported to the Administration for the Prevention of Money Laundering by period**

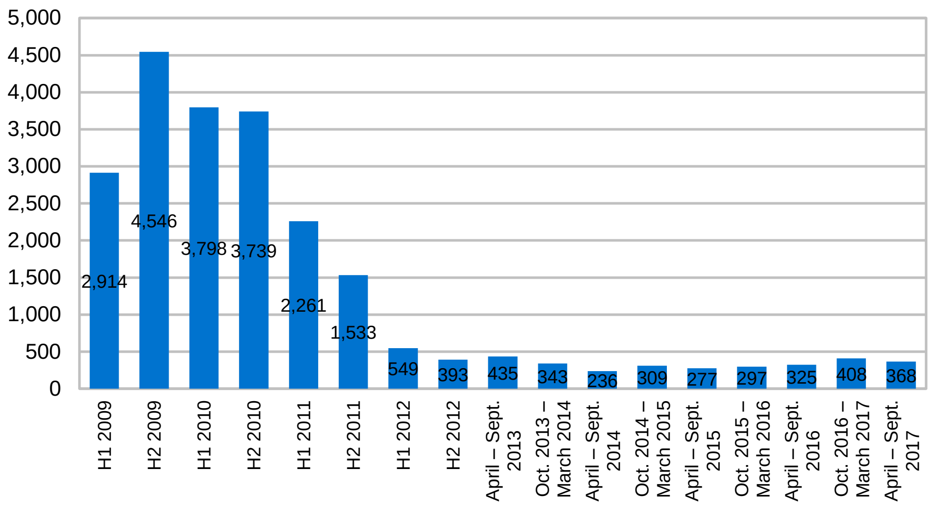


In the analysis period, the Administration received reports on 368 transactions (one bank alone reported 77 transactions) designated as suspicious on the basis of indicators for identifying suspicious transactions (hereinafter: suspicious transactions), which is 9.80% less relative to the results from the prior Questionnaire (Chart 9). In this period, the number of reports on suspicious transactions filed with the Administration decreased by 40.

In the period under review, three banks did not report any suspicious transactions, nine banks reported up to five suspicious transactions, four banks reported five to ten transactions, ten banks – 10 to 20 transactions, and four banks reported more than 20 such transactions, with one of these banks reporting 77 suspicious transactions.

In the analysis period, four banks used the legal option to temporarily suspend the execution of 12 transactions. Of this, two banks temporarily suspended the execution of one transaction each, one bank temporarily suspended three transactions and one bank temporarily suspended seven transactions. Relative to the prior period, when four banks temporarily suspended the execution of 19 transactions, in the analysis period banks used this legal option less often.

Chart 9 **Number of suspicious transactions reported to the Administration fo the Prevention of Money Laundering by period**



According to Questionnaire responses, front-office staff submitted to the compliance officer 3,364 internal reports on suspected ML risk in relation to a client or a transaction. There were no internal reports on suspected terrorism financing in the analysis period. The number of internal reports submitted by bank staff to the compliance officer decreased by 410 in absolute terms (by 10.86%) from the prior period. Of all internal reports on suspected money laundering submitted by bank staff to the compliance officer, 124 (or 3.96%) were not submitted to the Administration. To be more precise, on the basis of 3,364 internal reports on suspected money laundering, compliance officers filed 3,240 reports on suspicious transactions to the Administration, which makes up around 96.31% of the total number of submitted internal reports.

The significant increase in the percentage of suspicious transactions reported by compliance officers on the basis of internal reports submitted by front-office staff or their transactions, relative to a mere 4.37% in the previous analysis period, suggests that in the observed period closer attention was paid to the quality of reports and staff training in this particular segment.

IX EMPLOYEE TRAINING

According to Questionnaire responses, front-office jobs are carried out by a total of 14,969 employees. This is 91 persons more than in the prior period, while the relative share of front-office staff in total banking sector employment is almost the same as in the previous period.

All banks prepared their programme of annual professional education, training and professional development of employees engaged in the detection and prevention of money laundering and terrorism financing and adjusted it to the different job positions within the bank.

Banks carry out employee training according to their annual plan and programme. The majority of banks organise such training at least once a year or an as-needed basis, at the time of hiring new staff or in case of changes in legal and internal regulations. Training is most often carried out by compliance officers and their deputies, trained managers of organisational units and Compliance Division staff. Typically, training is done online, or through presentations in training centres, interactive trainings, PowerPoint presentations, local network publications, external seminars, lectures, learning about new money laundering and terrorism financing trends and techniques. On the banks' intranet pages, employees can access all guidelines and legal regulations pertaining to this segment of activity, while e-mails are also used as needed in order to inform organisational units about their AML/CFT-related obligations.

In 27 banks, all front-office staff and employees executing transactions have already completed their annual training plans, while in three banks the plans will be carried out by the year's end. Upon the completion of training, all banks test the knowledge of their staff and keep the tests scores in the manner and for the duration regulated by law.

According to Questionnaire responses, employees in all banks were aware of the consequence of the failure to apply laws and follow procedures and to act upon control findings.

* * *

To conclude, based on the Questionnaire responses for the period April–September 2017, we detected an increase in the number of banks which did not perform the logical testing of data accuracy before submitting those data to the NBS (20% of banks in the prior period versus 23.33% in this analysis period). The largest number of detected omissions pertain to the misalignment of data on the total number of clients relative to their sum in the representation of their composition by residence, failure to respond to questions in the Questionnaire regarding client classification in terms of risk degree and implemented indicators for detecting suspicious transactions regarding ML/FT, therefore in the coming period banks have to ensure additional controls in order to provide accurate data to the NBS.