NATIONAL BANK OF SERBIA

ADMINISTRATION FOR SUPERVISION OF FINANCIAL INSTITUTIONS

BANK SUPERVISION DEPARTMENT

Special Supervision Division

ANALYSIS OF BANKS' RESPONSES TO THE QUESTIONNAIRE ON ACTIVITIES REGARDING AML/CFT RISK MANAGEMENT OCTOBER 2015 – MARCH 2016

Belgrade, June 2016

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 of the next year.

The analysis of the Questionnaire aims to:

- provide an overview of the current 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,
- promote implementation of the established rules and principles of the "Know Your Client" procedure,
- ensure off-site monitoring of development of AML/CFT risk management in the overall banking system,
- detect any weaknesses and timely inform banks of potential risk exposure.

The questions in the Questionnaire are sorted into seven sections:

Section I: General bank data

Section II: Bank's activity

Section III: Clients

Section IV: Transactions

Section 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 was based on data for the October 2015 – March 2016 period submitted by banks to the NBS in the form of Questionnaire responses. The presented data may, therefore, exhibit certain inconsistencies and are mostly analytical in character. Before the analysis, data were checked for calculation and logical errors.

All of the thirty banks operating in Serbia in the period covered by the Questionnaire submitted their responses within the set deadline.

Contents:

1. Key findings

The analysis of responses to the Questionnaire for the October 2015 – March 2016 period indicates that, in the data collection and processing stages, a considerable number of banks (12 in total, or 40%) did not perform logical checks of data accuracy before submitting the responses to the NBS. To illustrate, the total number of clients often differed from the total number of clients as disclosed in breakdowns by resident status, risk level (low-, medium- and high-risk clients) and type of actions and measures taken (simplified, general or enhanced). In effect, a number of banks included clients with "dormant" or "sleeping" accounts in the total clients figure, but excluded them from the classification by CDD actions and measures taken, as this is not foreseen in the regulations.

During the analysis, 12 banks were asked to correct the calculation and logical errors detected in the submitted data.

The overall conclusion of the analysis is that banks had medium exposure to the AML/CFT risk in the analysis period. The key findings of the analysis are as follows:

- all banks set up their own AML/CFT risk management systems (in line with their size, number of clients, range of products offered to clients, etc.), applying an AML/CFT risk assessment approach and taking into account the findings of the National Money Laundering Risk Assessment;

- of the 13,498,671 clients in the entire banking sector, 64.106% were classified as medium-risk, 35.347% as low-risk and 0.547% as high-risk in terms of money laundering;

- the number of business relationships terminated due to the impossibility to take CDD actions and measures increased from 2,344 in the prior period to 31,550 in the observed period, reflecting an improvement in banks' CDD processes;

- the number of offers to establish a business relationship and/or to execute a transaction refused due to the impossibility to take CDD actions and measures increased to 1,383 or by 33.4%, indicating increasing use of this legal requirement by the banks as an instrument of AML/CFT risk management;

- 29 of the 30 banks use some type of software solution to monitor transactions and clients, as well as to detect suspicious transactions and clients. Most banks implemented one or more indicators of the Administration for the Prevention of Money Laundering (hereinafter: Administration) for recognizing ML and/or FT transactions, while 23 banks developed their own indicators for recognizing suspicious transactions and clients and included them in their software. Banks, therefore, went even beyond legal requirements in an effort to ensure more effective and better-quality AML/CFT risk management;

- in their internal acts, all banks defined the frequency for monitoring transactions depending on the assessed risk level, particularly for the highest-risk clients, and the periods during which connected cash transactions are to be monitored;

- further improvement of IT solutions within current systems may help diminish operational risks resulting from human error and lead to more effective human resources management (especially in case of staffing reductions), by enabling employees to focus on improving the quality of analysis of clients' activities and/or transactions selected by the bank's system on the basis of programmed parameters – indicators;

- all banks prepared lists of FT-related individuals and entities, drawing from the lists of the UN Security Council, EU and OFAC;

- at end-March 2016, 99.31% of all clients were residents and 0.69% were non-residents;

- the number of clients which established a business relationship without being physically present declined by 21,283, while the number of clients who are foreign officials fell by 373 from the prior period;

- the number of executed cash transactions in the overall banking sector declined by 14% from the prior period;

- in view of the fact that ML, and in particular FT risk management, is gaining significance both globally and at home, the function of compliance officers and their deputies in all obligors, banks in particular, needs to be strengthened further;

- the number of suspicious transactions reported to the Administration increased by 7% (20 transactions) from the prior period; 4 banks did not report any suspicious transactions;

- banks increasingly used the legal option of temporarily suspending a transaction (five banks suspended 10 transactions) which was not the case in prior periods;

- all banks regulated the internal controls system in their internal acts. AML/CFT controls are set out in the internal controls plans of 29 banks, while one bank did not reply to this question;

- in the past year, 28 banks conducted AML/CFT controls, one bank did not conduct such control and one bank did not reply to the question;

- in 24 banks, the compliance officer/his deputy reports to the Executive Board on internal control findings, while in 20 banks the findings are reported to the Managing Board;

- 25 banks conducted internal audit of AML/CFT related activities in the analysis period. Of the remaining five banks, two conducted internal audit in 2014, two in 2013 and one by 30 June 2015.

- in the course of audit, 21 banks identified irregularities; 19 banks removed the detected irregularities within the set deadlines, while two banks failed to do so;

- all banks pay due attention to training, primarily of front-office staff or staff engaged in the performance of transactions. However, the analysis points to a need for further training in a number of banks, primarily of staff within the business network who report on clients and transactions suspected of ML and/or FT to the compliance officer, as only 6.5% of all internal reports were filed to the Administration in the form of reports on suspicious transactions.

The following findings should also be highlighted as they may affect, directly or indirectly, the quality of AML/CFT risk management:

- as the number of locations where it is possible to establish a business relationship with a client declined by 51 from the prior period, while the number of locations where cash transactions can be made increased by 21, it may be concluded that new technology is increasingly used for performing cash transactions;

- total employment in the banking sector fell by 212 in absolute terms from the prior analysis period to 24,193 as at 31 March 2016, of which 14,733 were employees who are in direct contact with clients and their transactions. As staffing reduction in the banking sector continued, while the average number of clients and transactions per employee increased from the prior period, this could affect the quality of AML/CFT risk management.

- the fluctuation of AML or front office staff was between 10 and 50% in 20% of the banks, also indicating likelihood of additional ML/FT risk exposure;

- the number of cases in respect of which seven banks entrusted CDD actions and measures to a third person increased by 40,467 from the prior period. This leads to a conclusion that banks which used this legal option ought to be particularly committed to the management of risk exposure in this segment;

- the total number of natural persons – non-resident bank clients decreased by 5.13% from the prior period. Despite this reduction, however, the share of non-resident natural persons from high-risk countries increased;

- the number of non-resident legal persons increased by 168 in absolute terms, with a slight increase in the number of non-resident legal persons from high-risk and off-shore destinations;

- the number of transactions with clients from high-risk and off-shore destinations increased by a total of 9.35% relative to the prior period while the number of non-resident clients from these countries went up, potentially exposing banks to elevated ML/FT risk.

2. General data on banks

As at 31 March 2016, 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 2,896 locations or 51 locations less than in the prior analysis period. Four banks can establish business relationships with clients at up to 10 locations, 11 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 (of which one bank – at 1,102 locations).

At sector level, a cash transaction can be made at a total of 3,500 locations (up by 21 locations from the prior period). Five banks have up to 10 such locations, 11 banks between 11 and 50, nine banks perform cash transactions at between 51 and 100 locations, three banks at between 101 and 200, and two banks at over 200 such locations. Though the number of locations where it is possible to establish a business relationship declined, the number of locations where cash transactions can be made increased.

Total banking sector employment as at 31 March 2016 was 24,193 persons. Analysis of staffing levels reveals a continuation of the staffing reduction trend, with total employment down by 212 persons at end-March relative to end-September 2015.

At banking sector level, the average number of clients per employee directly engaged in client- and transaction-related operations was 916, while the number of cashless and cash transactions per employee was 27,134[1] in the September 2015 – March 2016 period. The number of bank clients per employee increased by 16 from the prior period, whereas the number of cashless and cash transactions per employee increased by 777 from the prior period. This means that, in the analysis period, employee workload increased from the prior period, which, by extension, may signal likelihood of omissions in taking AML/CFT actions and measures.

In 6 of the 30 banks (20%), the fluctuation of AML or front-office staff was between 10 and 50%, indicating possibility of further ML/FT risk exposure.

As the number of clients and the number of cashless and cash transactions per employee increased in the period under review relative to the prior period, resulting in higher staff workload, and as AML or front-office staff declined by 20%, 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.

3. Compliance officer function

As Questionnaire responses reveal, 22 banks have a special organisational unit which deals exclusively with implementing the Law on the Prevention of Money Laundering and Terrorism Financing (hereinafter: Law), whereas in 8 banks these tasks are performed by other business units. In 8 banks, the compliance officer/his deputy and other staff in charge of AML/CFT activities are tasked to perform on a daily basis other duties as well in addition to activities relating to the implementation of the provisions of the Law.

The compliance officer occupies a managing position in only 8 banks, while in 22 banks this is not the case.

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

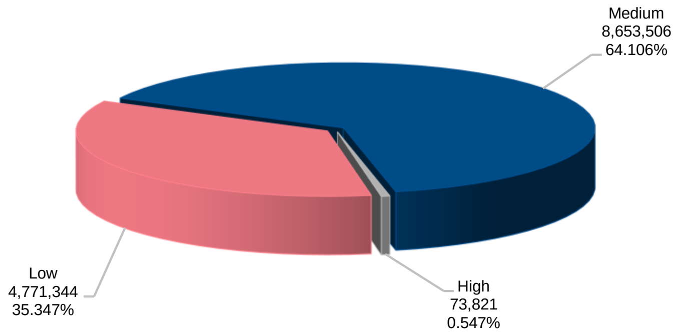
In view of the increasing significance of the ML, and in particular of the FT risk worldwide, the strengthening of the function of compliance officer and his deputy should be an imperative for the domestic banking sector as well.

[1] This figure is exclusive of e-banking transactions, as these transactions take place without direct engagement of the bank's employees.

4. Banks' activity

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 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 assessed degree 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 March 2016**



According to submitted data on client classification by degree of exposure to the ML/FT risk, eight banks classified over 80% of their clients in the low-risk category, while 18 classified the majority of their clients (over 80%) in the medium-risk category.

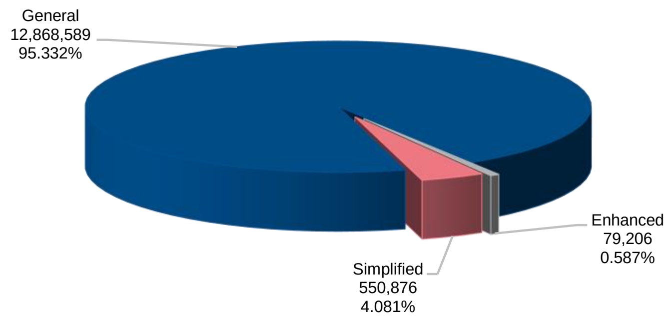
Questionnaire responses show that, despite classifying 4,771,344 out of 13,498,671 clients in the low-risk category, banks took simplified CDD actions and measures in respect of 550,876 clients only, which is broadly the same as in the prior period.

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

Risk level	No. of clients	% share	Applied measures	No. of clients	% share
low	4,771,344	35.347	simplified	550,876	4.081
medium	8,653,506	64.106	general	12,868,589	95.332
high	73,821	0.547	enhanced	79,206	0.587
	13,498,671	**100**		**13 498 671**	**100**

Pursuant to the Law, banks are required to take general, simplified or enhanced CDD actions and measures. Based on Questionnaire responses, in the analysis period, general actions and measures were taken in respect of 95.332% clients at banking sector level. Enhanced actions and measures were taken in respect of 0.587%, and simplified – in respect of 4.081% clients, as shown in Chart 2.

Chart 2 **Banking sector clients by CDD actions and measures as at March 2016**



Of the total number of cases where simplified CDD actions and measures were taken, one bank alone took simplified CDD actions and measures in respect of 443,663 clients, while all other banks took these measures in respect of 107,213 clients. Questionnaire responses also show that 14 banks took simplified CDD actions and measures in respect of low-risk clients, seven banks did not take these measures at all, while nine 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 the frequency for client monitoring in on the basis of client risk level.

Further, all banks confirmed that their internal acts define the frequency for monitoring transactions performed by clients classified as highest-risk, as well as periods for monitoring connected cash transactions.

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 September 2015 – March 2016 period, 11 banks terminated business relationships with 31,550 clients for the above reason. Of this, three banks terminated business relationships with 31,447 clients or 99.67%, of which one bank accounted for 24,008 cases of terminated business relationships (76.10% of all terminated business relationships), and the remaining eight banks terminated their business relationships with 103 clients. In the analysis period, 18 banks did not report a single case of terminating a business relationship and one bank did not reply to this question. Ten banks refused the offer to establish a business relationship and/or execute a transaction in the total of 1,383 cases, due to the impossibility to take CDD actions and measures. According to banks, in each case where they refused the offer to establish a business relationship or to execute a transaction for the above reasons, banks made official records in writing and assessed whether there were grounds to suspect money laundering or terrorism financing.

According to Questionnaire responses, seven banks entrusted the performance of individual CDD actions and measures to a third person and obtained data and documentation on 178,537 clients (of which 178,145 were clients of two banks).

All banks responded that they had 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.

According to submitted responses, ten banks monitor connected transactions for at least one day, seven banks for a week, three banks for a fortnight, seven banks for up to 30 days, one bank for six months, and one for a year, while one bank monitors connected transactions for a longer period of time, depending on the risk level. Given the large number of cash transactions per employee at banking sector level and the quantity of cash circulating in the sector, banks should further upgrade their system for monitoring cash transactions to ensure timely identification and analysis of connected transactions and mitigate the ML/FT risk.

In Questionnaire responses, 29 banks stated they use special software solutions for recognising 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 website of the Administration for Prevention of Money Laundering.

Also, 23 banks specified other indicators (from their own lists of indicators) which they included in the software for recognising suspicious transactions and/or persons.

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 26[2] banks:

Number of included indicators for banks	Number of banks
less than 5	2
5–9	7
10–14	6
15 and more	11

[2] Of the remaining four banks, one did not have the software and three did not answer this question.

According to Questionnaire responses, indicators for recognising FT-related suspicious transactions are included in the software of 24 banks, as follows:

Number of included FT-related indicators	Number of banks
less than 3	11
3–10	11
more than 10	2

Also, the number of indicators developed by banks and included in their software has been rising. The table below shows the number of banks applying their own indicators:

Number of included indicators developed by banks	Number of banks
less than 5	9
5–9	4
10–19	7
21 to 25	1
50	2

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. This shows 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.

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

5. 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 27 banks envisage AML/CFT-related audit of their operations in 2016. During the past year, 25 banks carried out audit of this segment of their operations. Of the remaining 5 banks, two conducted internal audit in 2014, two in 2013, and one by 30 June 2015. In the course of audit of AML/CFT-related activities of the bank, 24 banks identified omissions in the bank's procedures, while one bank was unable to respond to the above question, as the audit procedure was still under way. The most commonly identified omissions were: incomplete client files, outdated client data, incorrect client classification by exposure to the ML/FT risk, incomplete client data entered in the bank's system or data that cannot be accessed by other employees of the bank, outdated lists of risky states, deficiencies or inconsistencies between internal acts pertaining to different business processes, omissions in the systemic solution relating to risk level monitoring, etc. All banks which identified irregularities in the course of internal audit (24 banks) set deadlines for their removal; of this number, 13 banks removed irregularities within the set deadline, one bank failed to remove the irregularities, while in 10 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 of the findings in 24 banks, whereas the Managing Board was notified of the findings in 20 banks.

According to Questionnaire responses, 29 banks included AML/CFT-related internal controls in their internal control plans.

In the analysis period, 28 banks conducted internal control of AML/CFT activities. Irregularities were detected in 22 banks. Most frequently, internal control findings related to:

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

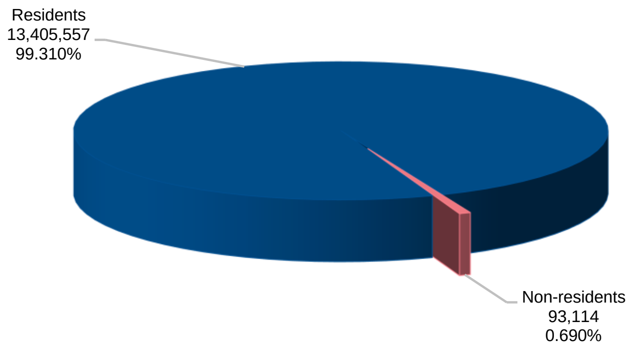
All banks which detected irregularities in the course of internal controls set a deadline for the removal of such irregularities, and 18 took measures to remove them. In 19 banks, the compliance officer notified the bank's Executive Board on AML/CFT findings of internal control, while in 18 banks the compliance officer notified the bank's Managing Board of the findings.

6. Clients

Charts 3 to 5 show the composition of banking sector clients in March 2016, based on the Questionnaire data.

Chart 3 shows the absolute and relative shares of residents and non-residents in the overall banking sector in March 2016.

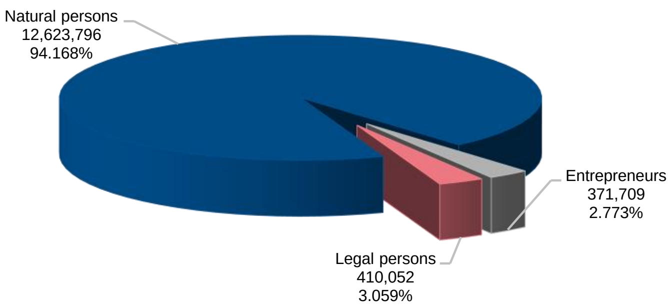
Chart 3 **Banking sector clients in March 2016**



Relative to the prior period, the share of residents in the total number of clients increased slightly; at end-March 2016, residents accounted for 99.310% of all clients and non-residents for 0.690%.

Like in the prior period, natural persons were dominant among resident clients with a share of 94%, while domestic legal persons and entrepreneurs, mildly increasing their share in the total number of resident clients, each accounted for 3%. This client structure is shown in Chart 4.

Chart 4 **Resident banking sector clients in March 2016**



The structure of non-resident banking sector clients, and the share of clients – natural and legal persons from high-risk countries and off-shore countries and territories in the total number of non-resident clients, is shown in Chart 5.

The number of clients – non-resident natural persons declined by 4,555 persons from the prior period to 84,232, while the number of non-resident legal persons increased by 168 in the same period.

In this period, the number of non-resident natural persons from high-risk countries increased to account for 17.676% of all non-resident clients, while the number of non-resident legal persons from high-risk countries also increased slightly, accounting for 10.978% of all clients.

Chart 5 also shows the share of clients from off-shore countries in total non-resident clients. Off-shore 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 the local market. As at March 2016, the share of natural and legal persons from off-shore countries in total non-resident clients changed relative to March 2015. Namely, though the total number of non-resident natural persons declined, the number of natural persons from off-shore countries increased from 3,781 to 4,233 persons, while the number of legal persons from off-shore countries rose from 1,093 to 1138 – as shown in Chart 5 below.

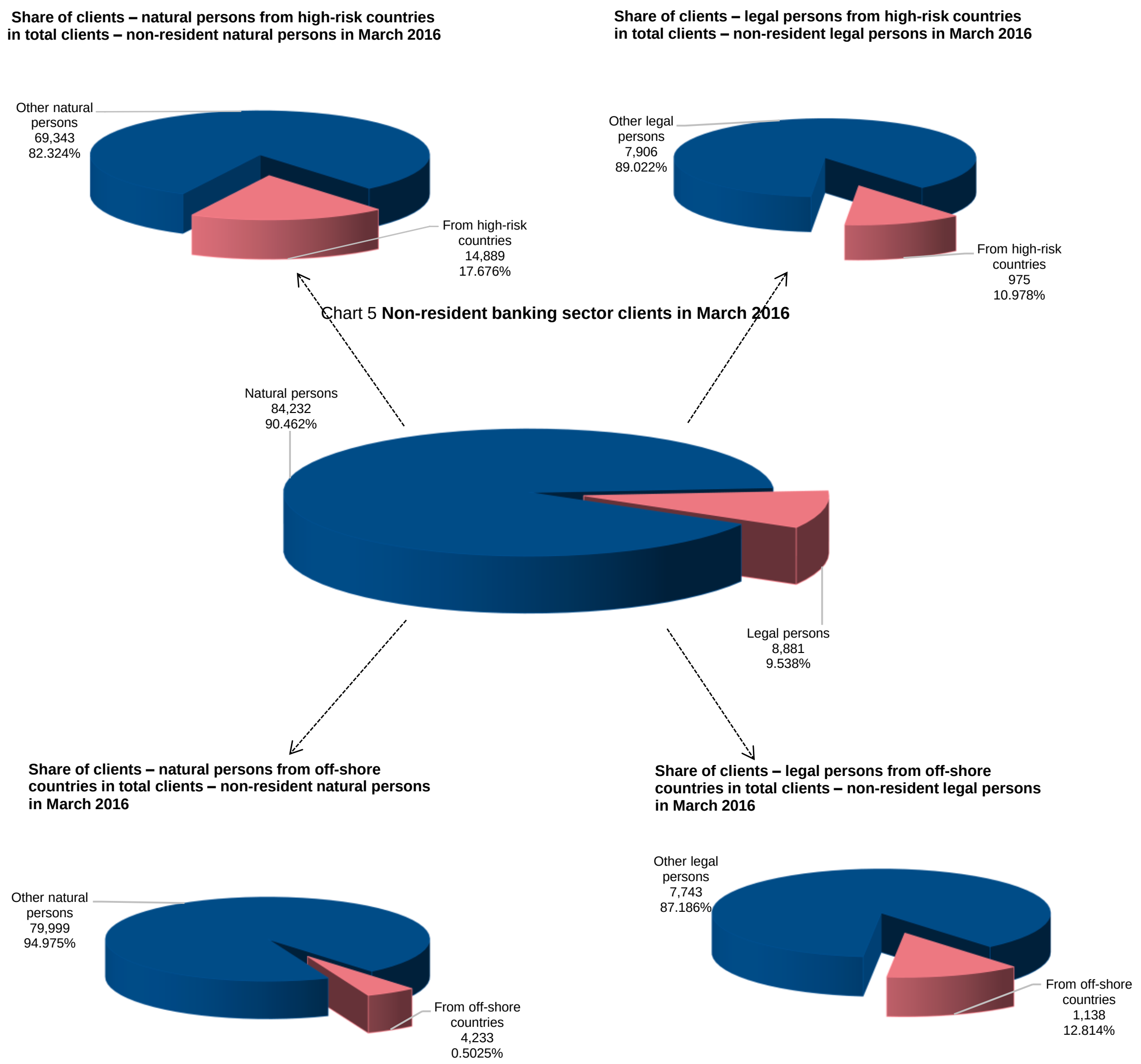


Chart 5 **Non-resident banking sector clients in March 2016**

The number of clients who established a business relationship without being physically present fell from 25,874 as at 30 September 2015 to 4,592, while the number of clients who are foreign officials fell by 373 from 30 September 2015 to 685 as at 31 March 2016.

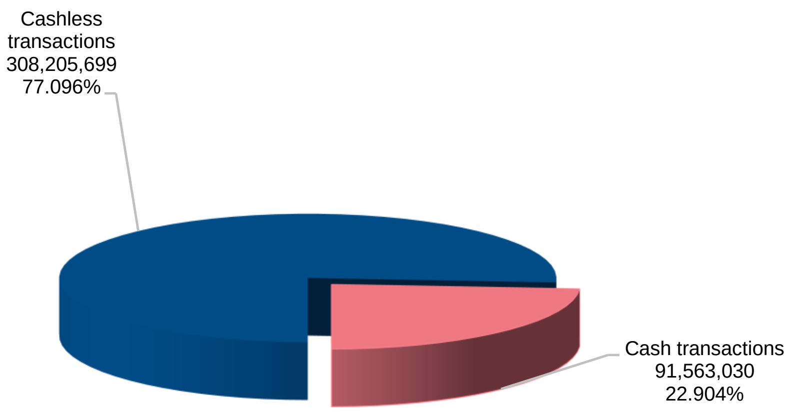
7. Transactions

In the reviewed period, banks performed 308,205,699 cashless transactions, or around 9.45% less than in the prior period. The number of cash transactions performed at banking sector level was 91,563,030, or around 14.33% less than in the prior period.

The share of cash transactions in total transactions decreased marginally from the prior period to 22.904% (compared to 23.898% in the prior period).

Chart 6 shows the structure of performed cash and cashless transactions in the banking sector in the October 2015 – March 2016 period, while Chart 6a gives an overview of cashless and cash transactions in the period from H1 2010 until and including the period under review.

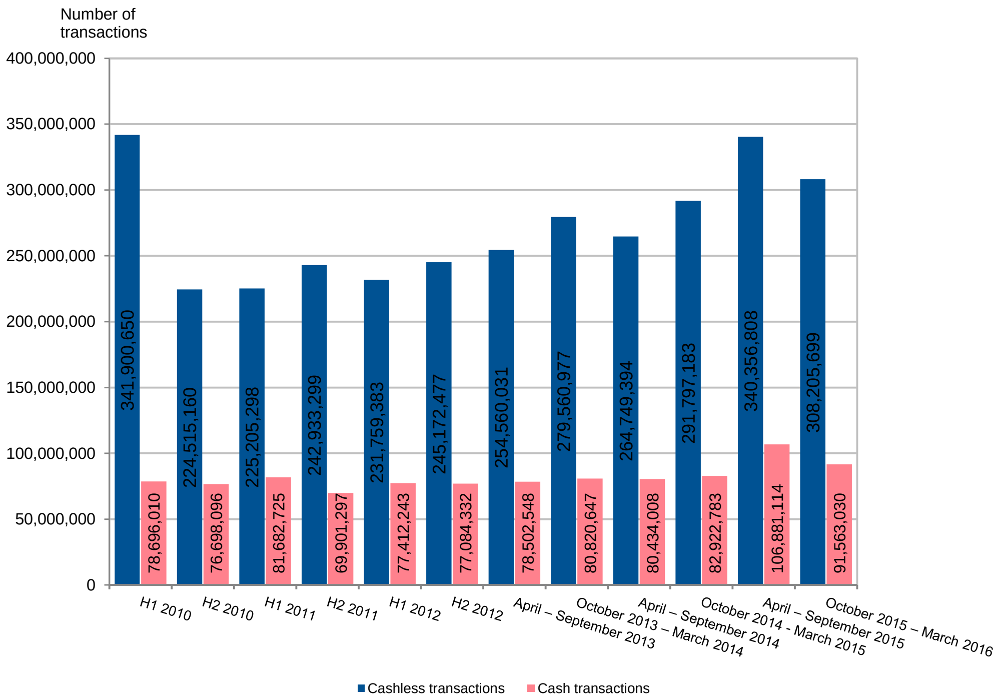
Chart 6 **Structure of transactions performed in the banking system in the October 2015 – March 2016 period**



Banks performed 207,130 cash transactions amounting to the RSD equivalent of EUR 15,000 or more at the middle exchange rate of the NBS, which is approximately 0.23% of the 91,563,030 total cash transactions made.

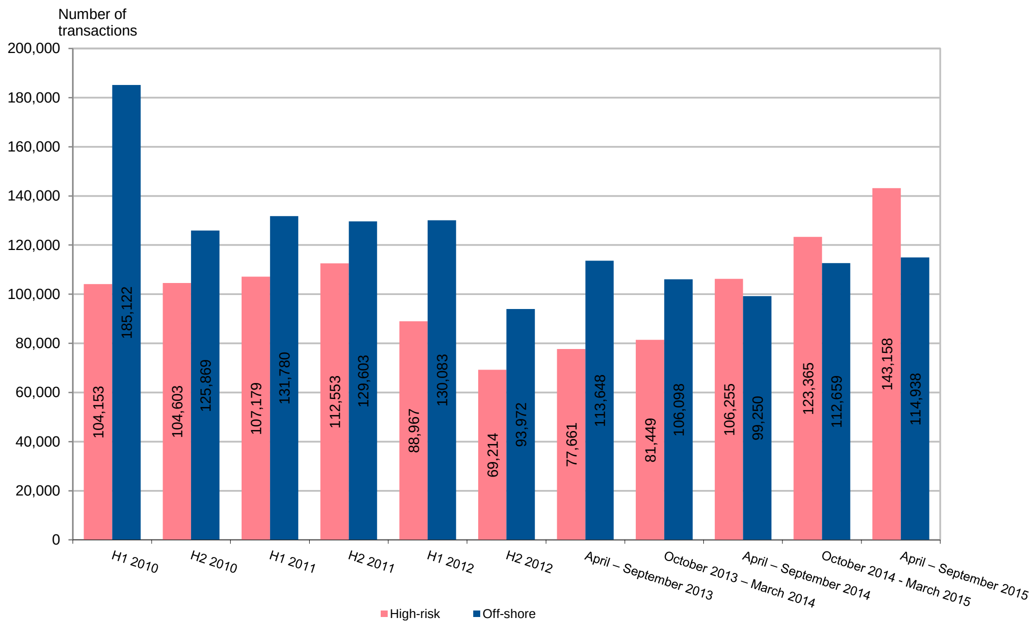
The number of the above cash transactions decreased from the prior period (by around 14%).

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



The number of transactions with clients from high-risk geographical areas was 143,158, or 18,793 transactions more than in the prior period, while the number of transactions performed with clients from off-shore geographical areas was 114,938, up by close to 2% or 2,279 transactions from the prior period, as shown in Chart 7.

Chart 7 **Movement in the number of transactions with clients from high-risk and off-shore areas by period**

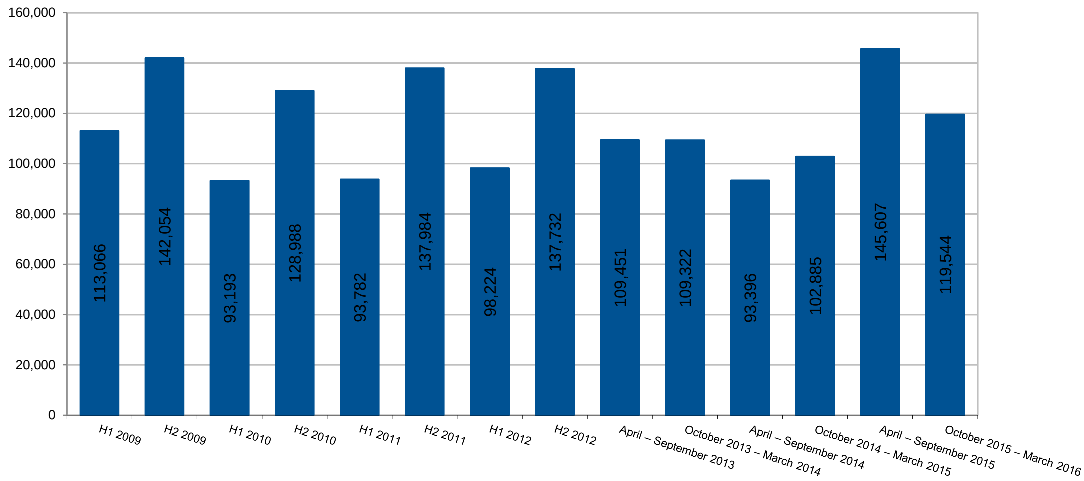


8. Reporting to the Administration

According to Questionnaire responses, the number of reported cash transactions amounting to the RSD equivalent of EUR 15,000 or more at the NBS middle exchange rate as at the transaction date came at 119,544 in the analysis period (Chart 8), while the total number of cash transactions of the same value was 207,130. The number of reported cash transactions amounting to EUR 15,000 or more decreased by 17.9% from the prior period.

Reported cash transactions amounting to the RSD equivalent of EUR 15,000 or more accounted for around 58% of all cash transactions in that amount, down by 10% 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 87,586. 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 are applied in accordance with Law and cash transactions involving transfer from one client account to another, if these accounts are held with one and the same bank, conversion of a client's account balance for another currency, where the money stays in the account with the bank, fixed-term depositing of balances in the client's account or its renewal. For this reason, the number of transactions reported to the Administration is much lower than the total number of cash transactions amounting to the RSD equivalent of EUR 15,000 or more.

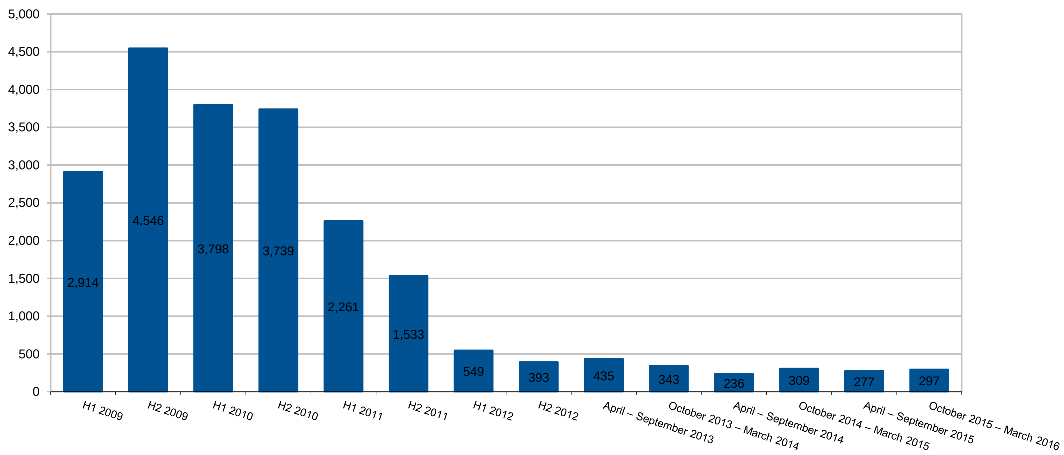
Chart 8 **Number of cash transactions worth ≥ EUR 15,000 reported to the Administration for the Prevention of Money Laundering by period**



In the analysis period, the Administration received reports on 297 transactions (one bank alone reported 64 transactions) designated as suspicious on the basis of indicators for recognising suspicious transactions (hereinafter: suspicious transactions), which is roughly 7% more relative to the results from the prior Questionnaire (Chart 9). In this period, the number of reports on suspicious transactions filed to the Administration increased by 20.

In the period under review, four banks reported no suspicious transactions (three banks in the prior period), five banks reported up to five suspicious transactions, 10 banks reported five to 10 transactions, nine banks – 10 to 20 transactions, and two banks reported more than 30 such transactions, with one of these banks reporting 64 suspicious transactions. In the analysis period, five banks used the legal option to temporarily suspend the performance of ten transactions. Of this, one bank temporarily suspended the performance of six transactions, while the remaining four temporarily suspended one transaction each. Relative to the prior period when two banks temporarily suspended the performance of five transactions, banks made increased use of this legal option in the analysis period relative to prior periods.

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 1263 internal reports on suspected ML risk in relation to a client or a transaction, and six internal reports on suspected terrorism financing. The number of internal reports submitted by bank staff to the compliance officer increased by 271 in absolute terms, or 27.31% from the prior period, but the quality of these internal reports is questionable. Namely, as Questionnaire responses show, of all internal reports on suspected money laundering submitted by bank staff to the compliance officer, 1181 (or 93.5%) were not submitted to the Administration. To be more precise, on the basis of 1263 internal reports on suspected money laundering, compliance officers filed only 82 reports on suspicious transactions to the Administration, which makes up around 6.5% of the total number of submitted internal reports.

By contrast, all six internal reports on suspected terrorism financing, which front-office staff submitted to the compliance officer in three banks, were reported to the Administration as suspicious FT-related transactions.

The relatively small percentage of suspicious transactions reported by compliance officers on the basis of internal reports submitted by front-office staff (6.5%) reveals a need for improving the quality of staff training in this particular segment.

9. Employee training

According to Questionnaire responses, front-office jobs are performed by a total of 14,733 employees. This is 64 persons or close to 0.45% less than in the prior period, indicating a continued trend of reduction of front-office staffing levels in the banking system as a whole.

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

According to Questionnaire responses, banks carry out employee training according to the 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 to legal and internal regulations. Training is most often held by compliance officers and their deputies, trained managers of organisational units and Compliance Division staff. Typically, training is in electronic form, or takes place through presentations in training centres, interactive trainings, PowerPoint presentations, publications on the local network, 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 area, while e-mails are also used as needed in order to inform organisational units about their AML/CFT-related obligations.

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