REVIEW OF TRANSACTIONS NOT AUTHORISED BY CUSTOMERS FOR 2019

Bank of Russia

CONTENTS

This review was prepared by the Financial Sector Computer Emergency Response Team (FinCERT) of the Information Security Department of the Bank of Russia.

Cover photo: Shutterstock/FOTODOM

12 Neglinnaya Street, Moscow 107016
Bank of Russia website: www.cbr.ru

ABBREVIATIONS

FinCERT AIPS	Automated Incident Processing System
Feed-Antifraud AS	Feed-Antifraud Automated System
Malware	Malicious software
RBS	Remote banking service
BR IBBS Package	A package of documents of the Bank of Russia on standardisation in ensuring the information security of the banking system of the Russian Federation, which describes a unified approach to building the information security system of banking sector institutions based on the requirements of Russian legislation
Mobile devices	Subscriber mobile communication devices, mobile telephones, smartphones, PDAs and other devices used by the customers of credit institutions for funds transfers
Transactions not authorised by customers	Funds transfer transactions having attributes of funds transfers without customer authorisation, as established by Bank of Russia Order No. OD-2525, dated 27 September 2018
Bank of Russia Regulation No. 382-P	Regulation No. 382-P, dated 9 June 2012, 'On the Requirements to Protect Information Related to Funds Transfers and on the Procedures for the Bank of Russia to Control the Compliance with the Requirements to Protect Information Related to Funds Transfers'
Federal Law No. 161-FZ	Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System'
Federal Law No. 167-FZ	Federal Law No. 167-FZ, dated 27 June 2018, 'On Amending Certain Laws of the Russian Federation for Countering Embezzlement'
Reporting form 0403203	Reporting form 0403203 'Information on Detection of Incidents Related to the Violation of Information Security Requirements in Funds Transfers' established by Bank of Russia Ordinance No. 2831-U, dated 9 June 2012, 'On Reporting by Payment System Operators, Payment Infrastructure Operators, Funds Transfer Operators on Information Protection during Funds Transfers'
Reporting form 0409258	Reporting form 0409258 'Information on Unauthorised Payment Card Transactions' established by Bank of Russia Ordinance No. 4212-U, dated 24 November 2016, 'On the List, Forms and Procedure for Compiling and Presenting Credit Institutions Reporting Forms to the Central Bank of the Russian Federation'
EMP	Electronic means of payment
CNP transaction	Card Not Present transaction; an internet transaction made by using payment card details (without presenting their tangible medium)

INTRODUCTION

The analysis and monitoring of transactions not authorised by the customers of credit and non-bank financial institutions operating in the financial sector has been an objective of FinCERT for more than four years. The goal of this activity is to identify and prevent such transactions in cooperation with information exchange participants as well as to create a knowledge base on the structure of such transactions.

This review contains data on the number and value of transactions not authorised by customers in 2019. The review is based on the information submitted by reporting funds transfer operators and payment infrastructure operators to the Bank of Russia under Reporting forms 0403203 and 0409258.

In most cases, data for 2019 are provided as per Form 0403203, while in the previous report they were provided as per Form 0409258. This is done to describe the actual situation in a more complete and accurate manner, which was the purpose for amending Form 0403203.

As was expected in the previous year, the 2018 amendment to Reporting Form 0403203 and the imposition of stricter requirements on financial sector institutions with regard to the complete and timely submission of data resulted in a material increase in the quality and volume of the data submitted.

Funds transfer operators and payment infrastructure operators may use this review to plan their risk management, internal control and information security activities, including for the purpose of recording the number and nature of incidents that occurred during the operation of information infrastructure facilities and in the implementation of requirements for information security during funds transfers.

OVERVIEW OF TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

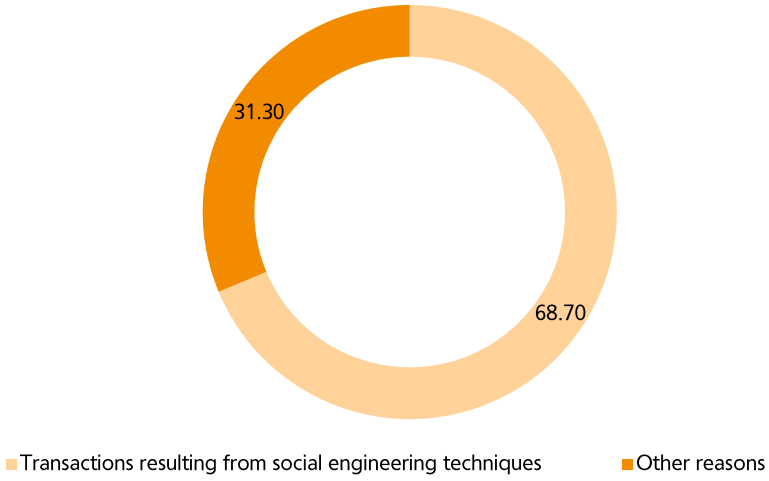
The 2018 amendment to Reporting Form 0403203 and the imposition of stricter requirements on financial sector institutions with regard to the complete and timely submission of data have resulted in a material increase in the quality and volume of the data submitted. The launch of FinCERT AIPS and Feed-Antifraud AS helped increase the detectability of transactions not authorised by customers. As a result, the data received from credit institutions showed growth in the number and volume of thefts in 2019.

In 2019, the total value of transactions not authorised by customers (both individuals and legal entities) through EMP amounted to ₽ 6,426.5 million. The number of such transactions was 576,566.

In 2019, the average amount of a transaction not authorised by the customer (individual) was ₽10,000 or ₽152,000 by a legal entity customer.

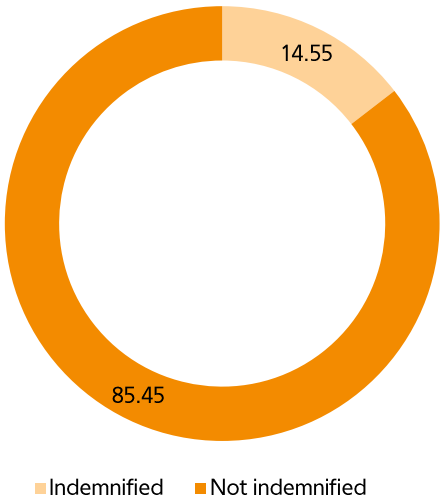
As many as 69% of all transactions not authorised by customers were successful since the customers were persuaded to independently execute the transactions through deceit or abuse of trust (so-called 'social engineering' techniques).

Figure 1
Reasons for transactions not authorised by customers (%)



Banks indemnified ₽935 million (15%, one is seven rubles stolen) to their customers. The current level of indemnification results from the high share of social engineering among transactions not authorised by customers. Due to deceit or abuse of trust, such transactions violate the respective agreements with credit institutions providing for the obligation to maintain the confidentiality of payment information. In this connection, the Bank of Russia intends to consider the possibility of changing the procedure for refunding (indemnifying) funds stolen from customers.

Figure 2
Indemnification to customers (%)



INFORMATION ON TRANSACTIONS NOT AUTHORISED BY CUSTOMERS (INDIVIDUALS)[1]

NUMBER AND VALUE OF TRANSACTIONS EXECUTED USING ELECTRONIC MEANS OF PAYMENT (INCLUDING PAYMENT CARDS)

According to the Bank of Russia, the number and value of funds transfer transactions using EMP executed by individuals amount to 40.3 billion transactions and ₽71.03 trillion respectively. The number and value of payment card transactions (using ATMs or the internet) amounted to 39.2 billion transactions and ₽63.7 trillion respectively; similar data on RBS transactions are 1.1 billion transactions and ₽7.3 trillion respectively.

Given the accomplishment of the Bank of Russia's objective of increasing the availability of financial instruments and developing new financial technologies, as well as the impact of natural competitive factors on the development of the financial sector, we continue to proceed from the forecast of growth in the number and value of such operations in our planning for the improvement of the information security of financial institutions. However, the Bank of Russia reckons that the distrust of financial customers toward the security of remote banking services can affect these trends and constrain overall market growth. Hence, enhancing the security of financial services is an objective that the Bank of Russia is seeking to achieve in the interests of both credit and financial institution consumers and the institutions themselves.

NUMBER AND VALUE OF TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

In this review, data on the number and value of transactions not authorised by customers (individuals) are provided in accordance with the data presented in new Reporting Form 0403203 used starting from the middle of 2018. The reason for this is the need to use more comprehensive indicators. Nevertheless, such data are substantiated and verified by the data from Form 0409258.

In 2019, the value of all EPM transactions executed without the authorisation of customers amounted to ₽5,723.5 million. The number of such transactions is 571,957.

EPM transactions not authorised by customers can by grouped into three categories:

- transactions executed using ATMs, payment terminals and imprinters
- payments for goods and services on the internet (CNP transactions)
- RBS transactions.

It is of note that most transactions not authorised by customers (individuals) are executed by malefactors gaining unauthorised direct access to electronic

[1] *In the past year, FinCERT used the 'unauthorised transaction' indicator, which remains in Reporting form 0409258.*

means of payment or persuading the owners of the funds to make a transfer in favour of the malefactor by deceit or abuse of trust (using social engineering techniques).

THE SHARE OF TRANSACTIONS NOT AUTHORISED BY CUSTOMERS IN THE TOTAL VALUE OF PAYMENT CARD TRANSACTIONS

In 2019, the share of transactions not authorised by customers in the total value of payment card transactions amounted to 0.0023% (0.0018% in 2018). These figures do not exceed the threshold established by the Bank of Russia for the share of unauthorised transactions in the total value of payment card transactions. This threshold is established at 0.005%.

The downward trend fluctuations detected in 2015–2017, as well as materially higher data presented in operating reports, demonstrate the real need for increasing the transparency of data provided by banks and confirms the appropriateness of the development and adoption by market participants and the Bank of Russia of measures to mitigate the risk of transactions not authorised by customers, as well as the need for the further development of such measures.

GROUPING BY CONDITIONS OF EXECUTING TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

According to the rules for completing the reporting forms submitted to the Bank of Russia, transactions not authorised by customers (individuals) are grouped by conditions in which they were executed:

- RBS transactions
- via ATMs, payment terminals, imprinters
- CNP transactions.

As a year earlier, CNP transactions account for the bulk of such transactions in terms of both value and number.

In 2019, 40,000 uses of payment cards (excluding pre-paid) at ATMs or payment terminals without the permission of the card holders were detected. Almost a quarter of them (22.4%) occurred due to malefactors' use of social engineering techniques. The total amount of damages caused by thefts through ATMs and payment terminals amounted to more than ₽525 million, and banks returned more than 10% (₽54.4 million) of funds stolen to the affected customers.

Payment for goods and services on the internet (CNP transactions) amounted for the majority of transactions not authorised by customers (individuals). In the past year, bank customers reported 371,100 transactions of this type; 2/3 of the transactions (243,300) resulted from the use of social engineering techniques. The damages caused amounted to ₽2,971.3 million, and banks indemnified to their customers approximately one in five rubles stolen (a total of ₽653.2 million).

After the adoption of the Federal Law 'On Amending the Federal Law "On Information, Information Technologies and Information Protection" and the

Civil Code of the Russian Federation' (Draft Law 605945-7), the Bank of Russia will be authorised to block phishing websites 'extrajudicially' by interacting with Roskomnadzor to include the websites in question in the register of information, the dissemination of which is prohibited in the Russian Federation.

The said draft law also provides for the implementation of a judicial mechanism for blocking websites disseminating malware. The Bank of Russia will be granted the right to apply to court for the protection of the rights, liberties and legal interests of an indefinite range of persons due to the publication of such information in information and telecommunication networks, including the internet.

Malefactors committed 160,800 offences through remote banking systems, and the share of social engineering in the total number of such offences is the highest at around 88.9%. This results from the target-oriented nature of such attacks, which is a result of the chance for malefactors to 'earn' more (the balance on an RBS account may considerably exceed the value of an average internet transaction). The volume of thefts amounted to around ₽2,227 million; banks indemnified to their customers a total of ₽162.3 million (i.e., one in 14 rubles).

Countering mobile fraud also requires the development of additional regulatory documents. The Bank of Russia contributes amendments to Federal Law No. 115FZ, dated 7 August 2001, 'On Countering the Legalisation (Laundering) of Criminally Obtained Incomes and the Financing of Terrorism' to provide for the creation of a single channel for exchanging mobile device and subscriber data between communication operators and banks.

GROUPING BY REASON OF EXECUTING TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

As in the previous year, according to the reporting operators, the absolute majority of thefts were committed through social engineering. As of 2019, its share amounted to approximately 69% of cases (97% in 2018).

First and foremost, such decrease can be explained by a change in the methods of base indicator calculation and also by an increase in the level of the population's cyber literacy resulting from the activities of reporting operators (under Subclause 2.12.3 of Regulation No. 382-P) and the Bank of Russia aimed to increase bank customer awareness of the risks related to the use of EMP.

It is of note that reporting operators indicate the cause of transactions not authorised by customers (individuals) based on the data provided by customers in their statements, which is an important source of information for gaining understanding of the type of unauthorised transactions.

In addition, operators should improve the quality of their work aimed to raise customer awareness about the possible risks of using EMP and the allocation of liability between the bank and customer if payment card data are compromised. Operators must perform these activities on an ongoing basis in accordance with the legislation of the Russian Federation.

GROUPING OF THE NUMBER AND VALUE OF FUNDS TRANSFERS NOT AUTHORISED BY CUSTOMERS, BY PLACE OF TRANSFER

Figure 3 demonstrates the grouping of transactions not authorised by customers by the place of such transactions. Only data on ATM (payment terminal or imprinter) and CNP transactions involving the use of payment cards issued in the Russian Federation are taken into account (excluding Moscow Region, which accounts for 339,522 transactions not authorised by customers—that is, a total of ₽2,594 million). One feature of the distribution of such transactions is their concentration in the Central Federal District. This is due to the fact that the majority of credit institutions servicing individuals are located in the Central Federal District.

Credit institutions in the regions specified in Table 1 should pay special attention to the fulfilment of Subclause 2.12.3 of Bank of Russia Regulation No. 382-P, which obliges credit institutions to carry out activities to increase the awareness of employees and customers about information security methods and risks of unauthorised access to EMP.

Figure 3
Number and value of funds transfers not authorised by customers (excluding Moscow Region)

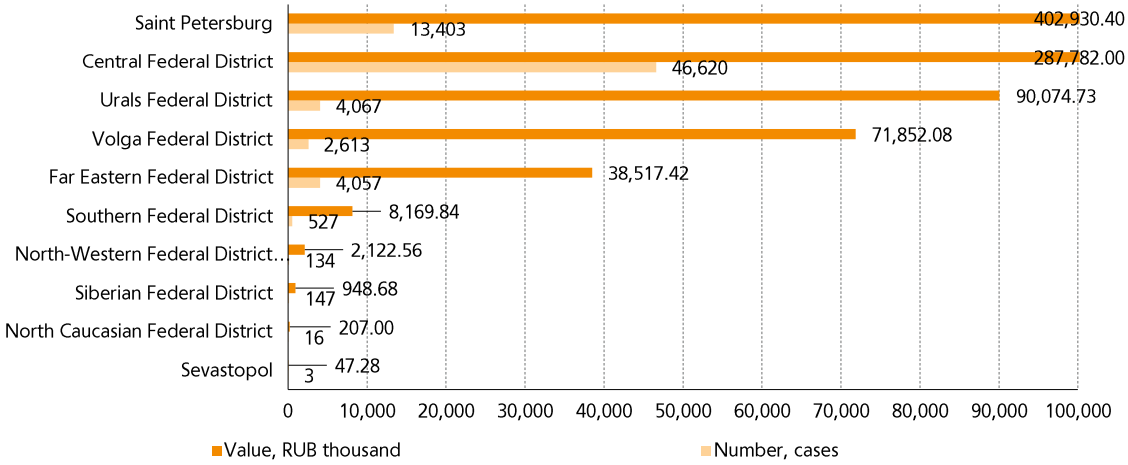


Table 1
Number and value of funds transfers not authorised by customers, broken down by place of transfer

	Number, cases	Value, RUB thousand
Moscow	339,522	2,593,875
Saint Petersburg	13,403	402,930.4
Kostroma Region	46,353	285,878.2
Sverdlovsk Region	1,920	70,744.69
Ulyanovsk Region	2	31,575.86
Amur Region	2,627	25,328.57
Republic of Tatarstan	1,547	19,837.44

	Number, cases	Value, RUB thousand
Tyumen Region	1,605	13,726.22
Primorye Territory	1,384	10,812.21
Udmurt Republic	170	7,222.28
Krasnodar Territory	390	5,794.73
Chelyabinsk Region	542	5,603.82
Kirov Region	526	5,069.36
Nizhny Novgorod Region	137	3,920.63
Sakha Republic (Yakutia)	40	2,298.87
Orenburg Region	86	2,283.89
Rostov Region	115	1,884.27
Perm Territory	66	1,438
Vologda Region	89	1,386.97
Kursk Region	121	599.99
Novosibirsk Region	85	567.55
Kaliningrad Region	32	537.57
Kaluga Region	22	521
Republic of Crimea	21	474.88
Moscow Region	63	406.75
Samara Region	46	237.65
Republic of Mordovia	22	207.87
Stavropol Territory	16	207
Novgorod Region	12	197.95
Lipetsk Region	38	158.73
Krasnoyarsk Territory	41	151.79
Tomsk Region	4	125.14
Tula Region	7	95.14
Republic of Khakassia	9	85.2
Sakhalin Region	6	77.77
Ivanovo Region	10	73.42
Sevastopol	3	47.28
Saratov Region	6	44.55
Ryazan Region	4	29.77
Astrakhan Region	1	15.96
Chuvash Republic	5	14.55
Vladimir Region	1	10
Omsk Region	1	9.59
Yaroslavl Region	1	9
Irkutsk Region	2	6.95
Kemerovo Region	5	2.46
Republic of Komi	1	0.07

Transactions not authorised by customers and executed outside the Russian Federation account for 42.5% of the total number and 29.3% of the total value of unauthorised transactions (in 2018, these indicators totalled 44% and 40.7%, respectively).

Figure 4
Value of payment card transactions not authorised by customers, broken down by geography (%)

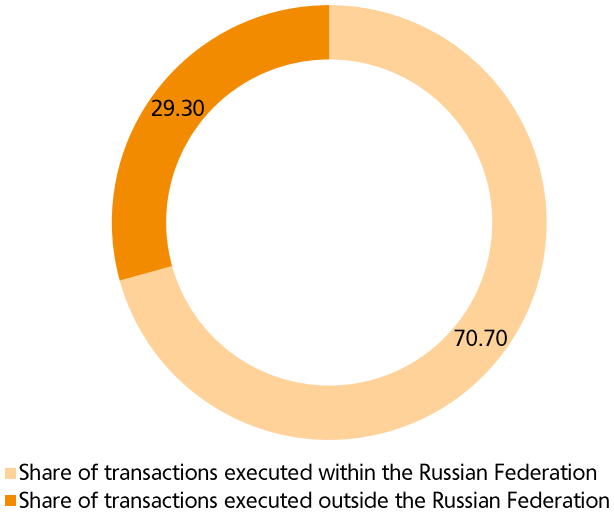
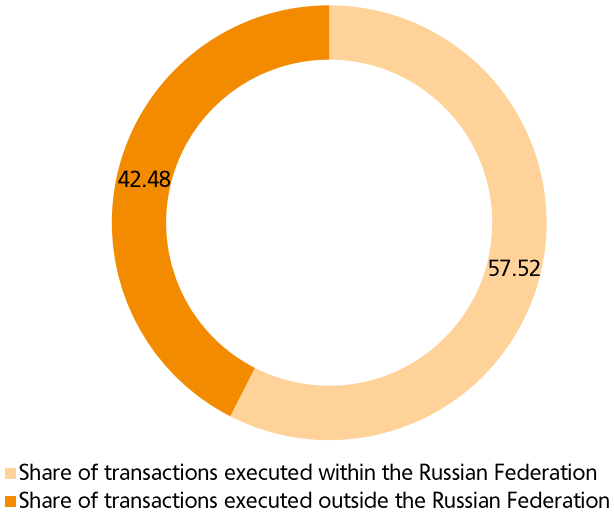


Figure 5
Number of unauthorised payment card transactions, broken down by geography (%)



As in the previous year, this indicates the need for credit institutions to inform their customers about possible risks when making cross-border funds transfer transactions. The attributes of funds transfers not authorised by customers published by the Bank of Russia help operators improve the performance of antifraud systems as regards detecting cross-border transactions not authorised by customers.

In this regard, we predict the continuation of the trend in which the share of the value and number of transactions not authorised by customers and executed within the Russian Federation in the total value and number of all unauthorised transactions amounts to more than 50%.

2. INFORMATION ON CORPORATE ACCOUNT TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

NUMBER AND VALUE OF TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

In this review, corporate account transactions not authorised by customers shall be understood as incidents with regard to which customers reported the theft of funds as a result of unauthorised access to the RBS systems (means) of legal entities, individual entrepreneurs and persons involved in private practice, including systems (means) used for funds transfers using the correspondent accounts of legal entities.

In 2019, legal entities reported to banks 4,609 transactions not authorised by customers, totalling ₽701 million.

Around 10% of the funds stolen (₽65 million) was indemnified or refunded to the affected entities.

GROUPING BY REASON OF EXECUTING TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

The data submitted by reporting operators indicate that 16% of transactions not authorised by customers (legal entities) were executed through social engineering techniques (723 thefts). First and foremost, such cases include incidents where malefactors gain access to RBS systems using malware designed to hack desktop PC software. We believe this issue will remain pressing in 2020. The recommendations should include the need to improve the quality of reporting operator operations in the area of increasing cyber literacy among customers.

GROUPING OF THE NUMBER AND VALUE OF FUNDS TRANSFERS NOT AUTHORISED BY CUSTOMERS, BY PLACE OF TRANSFER

The provided data on the geographical distribution of corporate account transactions not authorised by customers include data on the place where a legal entity reports such incident upon its detection—that is, where the entity's account is maintained. As in 2018, the Central Federal District accounts for the majority of corporate account transactions not authorised by customers and executed using RBS systems. This trend results from the high concentration of legal entities in the Central Federal District, which attracts malefactors.

Credit institutions in the regions specified in Table 2 should pay special attention to the fulfilment of Subclause 2.12.3 of Bank of Russia Regulation No. 382-P, which obliges credit institutions to carry out activities to increase the awareness of their employees and customers about information security methods and the risks of unauthorised access to EMP.

Figure 6
Number and value of funds transfers not authorised by customers (excluding Moscow Region)

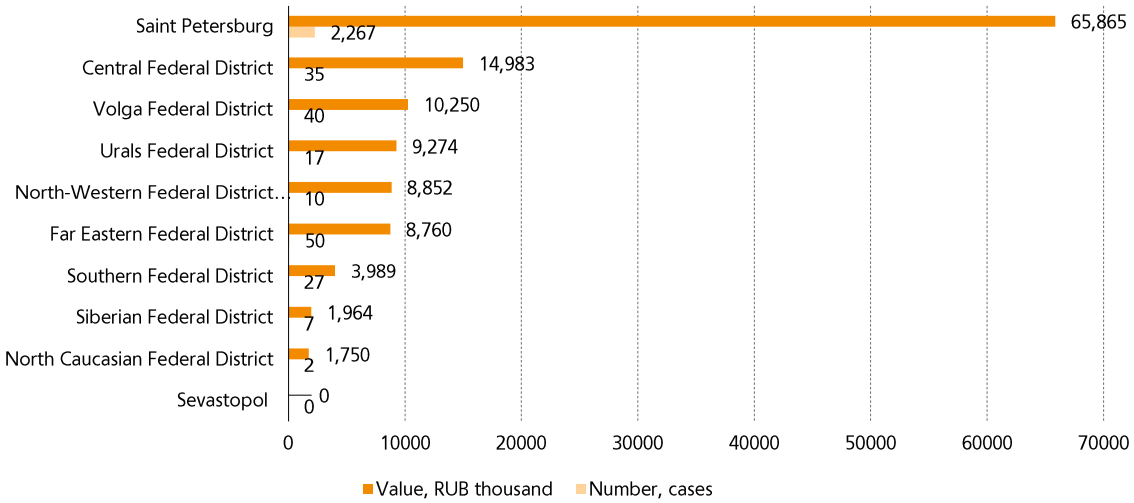


Table 2
Number and value of funds transfers not authorised by customers, broken down by place of transfer

	Number, cases	Value, RUB thousand
Moscow	2,154	575,306.4
Saint Petersburg	2,267	65,865.42
Chelyabinsk Region	10	7,197.28
Moscow Region	12	6,873.44
Vologda Region	3	5,691.67
Primorye Territory	4	5,649.24
Amur Region	46	3,111
Kostroma Region	11	2,998.76
Krasnodar Territory	7	2,821.64
Republic of Tatarstan	9	2,594.59
Kirov Region	13	2,432.34
Republic of Komi	4	2,283.09
Vladimir Region	3	2,234.4
Sverdlovsk Region	5	2,076.51

	Number, cases	Value, RUB thousand
Nizhny Novgorod Region	5	2,063.4
Kaluga Region	3	1,591.85
Republic of Dagestan	1	1,500
Novosibirsk Region	3	1,237.5
Udmurt Republic	3	1,223.8
Republic of Crimea	20	1,166.97
Republic of Karelia	1	756.49
Saratov Region	2	697.07
Orenburg Region	1	500
Ivanovo Region	1	440
Tver Region	1	418.67
Irkutsk Region	2	411.28
Perm Territory	3	369
Kemerovo Region	1	300
Stavropol Territory	1	250
Penza Region	1	230.5
Ryazan Region	3	227.59
Kursk Region	1	198.5
Samara Region	1	139.6
Kaliningrad Region	1	95
Pskov Region	1	26
Tomsk Region	1	15
Chuvash Republic	2	0
Tyumen Region	2	0

3. INFORMATION ON INCIDENTS THAT OCCURRED DURING THE OPERATION OF INFORMATION INFRASTRUCTURE FACILITIES BY REPORTING FUNDS TRANSFER OPERATORS AND PAYMENT INFRASTRUCTURE SERVICE OPERATORS

In 2019, reporting operators submitted data to the Bank of Russia about 973 incidents related to unauthorised access to their information infrastructure, totalling ₽103.8 million.

As many as 877 incidents related to the transfer of operator or customer funds without their consent were caused by the unauthorised access of employees or third parties to information infrastructure facilities, automated banking systems or account information. Damages from such thefts amounted to around ₽24.5 million.

The number of detected thefts resulting from computer attacks or unauthorised access to automated banking systems (account information) was smaller by a factor of 15, or 58 incidents; the total amount of such thefts was ₽23.2 million.

The unauthorised access of employees or other persons with access to the information infrastructure facilities of a funds transfer operator, ATMs and e-terminal hardware and software resulted in 14 thefts for a total of around ₽13.5 million, while the number of thefts due to computer attacks and unauthorised access was as small as 8 (totalling around ₽10.6 million).

Moreover, in 2019, 15 computer attacks and 2 cases of unauthorised access to ATM software and hardware resulted in the unauthorised withdrawal of cash from the ATMs of a funds transfer operators for a total of ₽32.2 million and ₽0.9 million respectively.

The total operating expenses of funds transfer operators incurred due to withdrawals (debiting) resulting from unauthorised access to operator information infrastructure is ₽27.4 million.

The stated funds theft amounts indicate a relatively low efficiency of malefactor attacks on credit institutions. This may be due to the increased attention of operators toward information security, including their work in this area, or the result of actions taken by the Bank of Russia in the area of information security with regards to funds transfers.

The Bank of Russia plans to pay sufficient attention to matters related to information security in financial sector institutions to reduce the number of attacks on them.

4. INFORMATION ON MEASURES TAKEN BY THE BANK OF RUSSIA TO MITIGATE THE RISK OF TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

The measures taken by the Bank of Russia to mitigate the risk of transactions not authorised by customers and incidents related to breaches of information security during the use of information infrastructures by reporting operators are as follows:

- improving the Russian laws on information security of financial institutions
- improving Bank of Russia regulations on information security of financial institutions
- improving the financial literacy of the population with regard to securing the information and payment technology used
- organising FinCERT-based information sharing for prompt and continuous mutual communication of threats to information security
- organising FinCERT-based information sharing for prompt and continuous mutual communication of transactions not authorised by customers.

ORGANISING FINCERT-BASED INFORMATION SHARING FOR THE PROMPT AND CONTINUOUS MUTUAL COMMUNICATION OF TRANSACTIONS NOT AUTHORISED BY CUSTOMERS

Currently, Russian laws on the national payment system establish the obligation for funds transfer operators to check funds transfer transactions for attributes of transactions not authorised by customers before crediting sender accounts. If such attributes are discovered, the funds transfer operator is obliged to suspend the transaction, block the EMP and contact its customer to establish whether the transaction was made by the legal account holder.

According to Bank of Russia Order No. OD-2525, the attributes of operations not authorised by customers can be grouped into two categories: a clear match with information about recipient and device parameters kept in the database of the Bank of Russia and a deviation from the amount, time, place of payment etc typical for the customer.

Such verification significantly reduces the risk of transfers not authorised by the customer. However, the risk of such transaction still remains. If a customer reports a detection of an unauthorised transaction pursuant to the form established in their contract, the funds transfer operator receiving such report must notify the Bank of Russia of such transaction no later than within one business day. For this purpose, the Bank of Russia has deployed a prototype of Feed-Antifraud AS on the basis of FinCERT AIPS. The system allows participants (participating institutions supervised by the Bank of Russia, which ensures trust as part of information exchange), including funds transfer operators, to submit

reports both through a web interface, in manual and semi-automated modes, and through an automated upload interface. The interface is currently being tested and is available for testing by participants. The format of transmitted data is established by Bank of Russia standard STO BR IBBS 1.5, while the description of the automated upload interface is available on the FinCERT AIPS portal.

When the Bank of Russia receives an automated notice from a funds transfer operator, the funds transfer operator serving the recipient is determined, after which a notice of the transaction not authorised by the customer is submitted to the relevant institution through the automated system. If the sender is a legal entity, the funds transfer operator, upon receipt of such notice, must suspend the transfer of funds to the settlement account of the recipient and request documents confirming the validity of the payment in accordance with the law. If the payment is already credited, the status of the transfer is returned. Regardless of the type of applicant, for each query of the Bank of Russia regarding an unauthorised transaction, the receiving funds transfer operator is obliged (according to the regulatory document of the Bank of Russia) to submit information about the recipient (e.g., the encrypted passport number) using FinCERT AIPS.

Since FinCERT AIPS is automated, information about transactions can be sent and routed correctly regardless of the day of the week.

In addition, for each unauthorised transaction in the frame of preliminary notification, the funds transfer operator serving the sender can send information on the number of the customer's police report to the Bank of Russia based on the information provided by the customer. Hence, if citizens show adequate activity protecting their rights and reporting to law enforcement agencies, the possibility of correlating citizen reports of unauthorised transactions submitted to law enforcement agencies with information about transactions and their recipients is forming in the Bank of Russia. As part of interdepartmental cooperation, the Bank of Russia can send this information to the Ministry of Internal Affairs of Russia to increase the crime detection rate when funds transferred as a result of a transaction not authorised by a customer are withdrawn by a recipient.

It should be noted that the exchange of information on transactions not authorised by customers is a relatively new area of activity for the Bank of Russia. In terms of results, the Bank of Russia aims to establish interaction between the participants of information exchange, reduce the number and value of transactions not authorised by customers and improve the quality of data provided for such transactions. Informing operators about transactions not authorised by customers via FinCERT AIPS is a real-time notification channel, unlike the data provided by operators as part of regular reporting to the Bank of Russia.

5. CONCLUSION

The value and number of transactions not authorised by customers involving payment cards issued by Russian banks are constantly increasing in the Russian Federation and abroad. The systematic development of remote payment services and the improvement of the National Payment System using modern technologies are expanding the availability of payment services and the sphere of cashless payments. The collaboration between the Bank of Russia, market participants and law enforcement agencies carried out in 2018 and 2019 after the introduction of new Reporting Form 0403203, the entry into force of Federal Law No.167-FZ, and the launch of FinCERT AIPS and the Feed-Antifraud AS made it possible to increase the rate detection of unauthorised transactions. The implementation of these measures has led to changes in a number of theft trends observed in previous years. During the reporting period, the number of such transactions amounted to 571,957, and in 2019 the 2018 trend towards the increase in the total number of thefts remained unchanged. In 2019, the value of EMP transactions not authorised by customers amounted to ₽5,723.5 million. In 2019, the share of transactions not authorised by customers in the total value of payment card transactions amounted to 0.0023% (0.0018% in 2018). Given the further growth expected in the number and value of non-cash payments, the Bank of Russia aims to reduce the share of transactions not authorised by customers (individuals) in the total value of payment card transactions to below 0.005%.

CNP transactions remain the largest group of transactions not authorised by customers (individuals): in 2019 their share in the total number of transactions was 65%, or 52% in the total value of transactions. They are followed (28% and 39% respectively) by individuals' RBS transactions not authorised by customers. However, while the average total of a CNP transaction is around ₽8,000, one RBS theft leads to average damages of ₽14,000. The remaining 7% of the number and 9% of the value of individuals' account transactions not authorised by customers were executed through ATMs and payment terminals (average amount: ₽13,000).

Among the causes of the majority of transactions not authorised by customers (69%), reporting operators mentioned the use of EMP without the consent of customers as a result of illegal activities and the loss or breach of confidentiality of authenticating information. Malware and the persuasion, by fraud or abuse of trust, of EMP owners to independently execute transactions may be considered the basis for a significant part of such transactions.

Moscow Region accounts for 82% (in terms of the number) and 74% (in terms of the value) of payment card transactions not authorised by customers. In terms of the number of such transactions, it is followed by the Central Federal District at 11.3%, and in terms of value, by Saint Petersburg (11.5%). Transactions executed outside the Russian Federation and not authorised by customers account for 42.5% (in terms of number) and 29.3% (in terms of value) of the total number and value of transactions not authorised by customers executed in 2019.

In 2019, the Bank of Russia received reports on 4,609 corporate account transactions not authorised by customers and executed through the RBS system for a total value of ₽701 million. The majority of such transactions belongs to the ₽100,000 to ₽10 million segment, with an average value of ₽152,000. Almost half (49.2%) of the transactions were executed in Saint Petersburg, while Moscow Region banks leave other regions far behind in terms of the value of thefts (82% of the total value in Russia). They also come in second in terms of the number of thefts.

Within the reporting period, reporting operators submitted to the Bank of Russia reports of 956 unauthorised transfers of funds owned by them or available on the correspondent accounts of their customers for a total of ₽71.5 million. Another ₽32.3 million in funds of banks and their customers was withdrawn from ATMs as a result of 17 incidents related to the unauthorised access of funds transfer operator employees or other persons with the authority to access the information infrastructures of funds transfer operators and ATM software and hardware or computer attacks.

The increasing availability of payment services offered on the internet is leading to a shift in the interest of attackers (gradually following the vector of interests of the clients of credit institutions) from ATMs and retail outlets toward CNP transactions and RBS channels. Taking into account the development of cardless financial services performed on the internet, we expect the upward trend in the migration of transactions not authorised by customers into the CNP environment to continue. The technique of phone number substitution, extensively used by malefactors in 2019, will likely remain one of the most popular tools among malefactors.

The main measures required to reduce the risk of thefts include the introduction of technologies related to the confirmation of transactions via alternative communication channels as well as the further development of antifraud systems, including the wider coverage of channels for performing transactions by these systems, including RBS channels and SMS banking. An important factor in combating unauthorised transactions can be the implementation of antivirus software in banking applications installed on customer devices as well as more accurate systems and methods of customer authentication.

Today, the use of antifraud systems is codified in the amendments to Federal Law No. 161FZ introduced by Federal Law No. 167FZ.

Additional measures for countering CNP transactions not authorised by customers should include the collaboration of financial sector institutions with domain name registrars with regard to AIPS reporting of phishing resources (domains used to perpetrate fraudulent activities associated with payment cards).

Banks indemnified to their customers ₽935 million (15%, or every one in seven rubles stolen). The current level of indemnification results from the high share of social engineering among transactions not authorised by customers. Due to deceit or abuse of trust, such transactions violate the respective agreements with credit institutions providing for the obligation to maintain the confidentiality of payment information. In this connection, the Bank of Russia intends to consider the possibility of changing the procedure for refunding (indemnifying) funds stolen from customers.