Банк России
Центральный банк Российской Федерации

BANK OF RUSSIA STANDARD

STO BR BFBO-1.5-2018

SECURITY OF FINANCIAL (BANKING) OPERATIONS INFORMATION SECURITY INCIDENT MANAGEMENT

ON THE FORMS AND TIMEFRAMES OF THE BANK OF RUSSIA'S INTERACTION WITH INFORMATION EXCHANGE PARTICIPANTS
IN THE EVENT OF DETECTION OF INCIDENTS RELATED TO VIOLATIONS OF DATA PROTECTION REQUIREMENTS

Effective date: 1 November 2018

Official edition

Moscow 2018

Preface

APPROVED AND IMPLEMENTED by Bank of Russia Order No. OD-2403, dated 14 September 2018.

Contents

Introduction....4
1. Scope....8
2. Regulatory references....8
3. Terms and definitions....9
4. Designations and abbreviations....12
5. The data submission form used by information exchange participants for registration with the Bank of Russia....13
6. Data submission form used by information exchange participants to inform the Bank of Russia about incidents related to violations of data protection requirements and the timeframes for their submission to the Bank of Russia....32
7. The form of the Bank of Russia's request to the information exchange participant serving the payee....114
8. The data submission form used by information exchange participants to provide a response to the Bank of Russia's request to the information exchange participant servicing the payee and the timeframes for their submission to the Bank of Russia....124
9. The form of information message of the Bank of Russia to the information exchange participant serving the payer....140
10. The form for submitting a request to the Bank of Russia from information request participants who are not structural units of the Bank of Russia using the express and non-rapid money transfer platforms, about imposing (or lifting) restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban to debit funds upon detecting incidents related to violations of data protection requirements during money transfer....155
11. The form of an information message of the Bank of Russia on imposing (or lifting) the restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban to debit fundsсредств....160
12. The form of distribution by the Bank of Russia among information exchange participants of data on the detected incidents associated with violations of data protection requirements....164
13. The form of data submission used by information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violations of data protection requirements and timeframes for their submission to the Bank of Russia....196
14. Conditions for information exchange participants to submit to the Bank of Russia data on detected incidents related to a violation of data protection requirements 201
15. Description of the technology for preparing and sending electronic messages during information exchange with the Bank of Russia....208

Annex 1. Schemes of interaction between an information exchange participant and the Bank of Russia..... 210
Annex 2. Schemes of interaction between the Bank of Russia and an information exchange participant.....245
Annex 3. Diagrams of processes of interaction between an information exchange participant and the Bank of Russia.....259
Bibliography.....264

Introduction

This standard defines the following aspects of the Bank of Russia's interaction with credit institutions, non-bank financial institutions, and entities of the national payment system (hereinafter, information exchange participants) when incidents related to violation of data protection requirements are detected:

- the data submission form used by information exchange participants for registration with the Bank of Russia;
- the data submission form used by information exchange participants to inform the Bank of Russia about incidents related to violations of data protection requirements and the timeframes for their submission to the Bank of Russia;
- the form of the Bank of Russia's request to the information exchange participant serving the payee;
- the data submission form used by information exchange participants to provide a response to the Bank of Russia's request to the information exchange participant servicing the payee and the timeframes for their submission to the Bank of Russia;
- the form of information message of the Bank of Russia to the information exchange participant serving the payer;
- the data submission form used by information exchange participants to submit a request to the Bank of Russia to impose (or lift) a restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to violation of data protection requirements;
- the form of a Bank of Russia information message on imposing or lifting restrictions in the form of a ban on debiting funds on bank (correspondent) accounts (sub-accounts) of information exchange participants upon detecting incidents related to violation of data protection requirements;
- the form of distribution by the Bank of Russia to information exchange participants of data on detected incidents related to violation of data protection requirements;
- the form of data submission used by information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violation of data protection requirements and the timeframes for their submission to the Bank of Russia;
- conditions for information exchange participants to submit to the Bank of Russia data on identified incidents related to violation of data protection requirements;
- description of the technology for preparing and sending electronic messages during information exchange with the Bank of Russia.

The data submission form used by information exchange participants to inform the Bank of Russia about incidents related to violations of data protection requirements shall be used in the following cases:

- when money transfer operators and payment infrastructure service providers inform the Bank of Russia about the detected incidents related to the violation of data protection requirements

when making money transfers, in accordance with the Bank of Russia's requirements [3];

- when money transfer operators and payment infrastructure service providers inform the Bank of Russia about all cases and (or) attempts to make money transfers without the customer's consent in accordance with the requirements of the Bank of Russia [4];
- when credit institutions inform the Bank of Russia about the revealed incidents related to the violation of the requirements for ensuring information protection in the course of banking activities, in accordance with the requirements of the Bank of Russia [5];
- when non-bank financial institutions inform the Bank of Russia about the detected incidents related to the violation of the requirements for ensuring the protection of information in the course of activities in financial markets, in accordance with the requirements of the Bank of Russia [6];
- when money transfer operators inform the Bank of Russia about the suspension of funds crediting to the payee's bank account or the increase in the balance of the payee's electronic funds in accordance with the Bank of Russia's requirements [20];

The form of the Bank of Russia's request to an information exchange participant serving the payee shall apply:

- when requesting from the money transfer operator servicing the payee, including the e-money operator, information identifying the payee, in accordance with the requirements of the Bank of Russia [4];
- when sending a notice of suspension of the transfer of funds to the payee's bank account or an increase in the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20].
- The data submission form used by information exchange participants to provide a response to the Bank of Russia's request to an information exchange participant serving the payee shall be used:
- when the money transfer operator serving the payee, including the electronic funds operator, informs the Bank of Russia about a specific payee in accordance with the requirements of the Bank of Russia [4];
- when sending a notification about the successful suspension of the money transfer to the bank account of the payee or an increase in the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20];
- when sending a notification about the impossibility to suspend the money transfer to the payee's bank account or increasing the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20].

The form of the Bank of Russia’s information message to an information exchange participant serving the payer shall be used:

- when sending a notification about the successful suspension of the money transfer to the bank account of the payee or an increase in the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20];
- when sending a notification about the impossibility to suspend the money transfer to the payee's bank account or increasing the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20].

The data submission form used by information exchange participants to send a request to the Bank of Russia on imposing (or lifting) the restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to violation of data protection requirements shall apply as follows:

- when exchange participants using speedy and non-speedy money transfer services and which are not Bank of Russia structural units;

  inform the Bank of Russia about imposing restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to violations of data protection requirements during money transfers at the information infrastructure facilities of information exchange participants in accordance with requirements of the Bank of Russia [21];

- when exchange participants using the speedy and non-speedy money transfer services and which are not Bank of Russia structural units inform the Bank of Russia about lifting restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to violations of data protection requirements during money transfers at the information infrastructure facilities of information exchange participants in accordance with requirements of the Bank of Russia [21].

The form of a Bank of Russia information notice about imposing or lifting a restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds shall be used as follows:

- when sending a notification to an information exchange participant in case of achieving a positive result of integrity control and acceptance of requests for imposing or lifting restrictions in the form of a ban on debiting funds in accordance with the requirements of the Bank of Russia [21];

- when sending a notification to an information exchange participant in case of achieving a negative result of integrity control and non-acceptance for execution of requests for imposing or lifting restrictions in the form of a ban on debiting funds in accordance with the requirements of the Bank of Russia [21].

The form for distribution by the Bank of Russia of data on detected incidents related to violation of data protection requirements among information exchange participants shall be used when sending information contained in the database on cases and attempts to make money transfers without the customer's consent in accordance with the requirements of the Bank of Russia [4].

The data submission form for information exchange participants to send information to the Bank of Russia on planned measures for disclosing information on identified incidents related to violation of data protection requirements shall be used to inform the Bank of Russia by money transfer operators and payment infrastructure service providers about the above measures in accordance with the requirements of the Bank of Russia [3].

The data submission form for information exchange participants to send information to the Bank of Russia on planned measures for disclosing information on identified incidents related to violations of information protection requirements in the course of banking activities shall be used to inform the

Bank of Russia about the above-mentioned measures in accordance with the Bank of Russia's requirements [5].

The data submission form for information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violation of information protection requirements in the course of financial market activities shall be used to inform non-bank financial institutions of the above-mentioned measures in accordance with the Bank of Russia's requirements [6].

STO BR BFBO-1.5-2018

BANK OF RUSSIA STANDARD

SECURITY OF FINANCIAL (BANKING) OPERATIONS INFORMATION SECURITY INCIDENT MANAGEMENT

ON THE FORMS AND TIMEFRAMES OF THE BANK OF RUSSIA'S INTERACTION WITH INFORMATION EXCHANGE PARTICIPANTS IN THE EVENT OF INCIDENTS RELATED TO VIOLATIONS OF THE DATA PROTECTION REQUIREMENTS

Effective date: 1 November 2018

1. Scope

This standard establishes the form and timeframes for the Bank of Russia's interaction with information exchange participants to identify incidents related to violations of data protection requirements.

This standard is recommended for use by including references hereto and/or direct use of the provisions hereof in the internal documentation of information exchange participants, as well as in agreements.

The mandatory application of this standard by other organisations may be defined by an agreement on cooperation with the Bank of Russia on countering computer attacks.

2. Regulatory references

This standard shall refer to the following documents:

Federal Law No. 86-FZ, dated 10 July 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)' [1];

Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System' [2];

Bank of Russia Regulation No. 382-P, dated 9 June 2012, 'On Requirements to Protect Information Related to Funds Transfers and on the Procedure for the Bank of Russia to Control the Compliance with Requirements to Protect Information Related to Funds Transfers' [3];

the Bank of Russia's regulation establishing the forms and procedure for sending information by money transfer operators, payment system operators and payment infrastructure service providers to the Bank of Russia on all cases and attempts to make money transfers without the customer's

consent and receiving information from the Bank of Russia, contained in the database on cases and attempts to make money transfers without the customer's consent, and the procedure for taking measures by money transfer operators, payment system operators, and payment infrastructure service providers to prevent money transfers without the customer's consent [4];

the Bank of Russia's regulation establishing mandatory requirements for credit institutions to ensure data protection in the course of banking activities [5];

the Bank of Russia's regulation establishing mandatory requirements for non-bank financial institutions to ensure data protection in financial markets [6];

the Bank of Russia's regulation establishing the forms and procedure for money transfer operators to send notifications about suspending money transfers to the payee's bank account or increasing the payee's electronic money balance, as well as about the impossibility of suspending money transfers to the bank account of the payee or suspending the increase in the electronic money balance of the payee [20];

the Bank of Russia's regulation establishing requirements for ensuring data protection in the Bank of Russia payment system [21].

3. Terms and definitions

This standard uses the terms defined in the following documents:

Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System' [2];

Bank of Russia Regulation No. 382-P, dated 9 June 2012, 'On Requirements to Protect Information Related to Funds Transfers and on the Procedures for the Bank of Russia to Control the Compliance with Requirements to Protect Information Related to Funds Transfers' [3];

The Bank of Russia's regulation establishing the forms and procedure for money transfer operators, payment system operators, and payment infrastructure service providers to send information to the Bank of Russia on all cases and attempts to make money transfers without the customer's consent and for receiving information from the Bank of Russia contained in the database of cases and attempts to make money transfers without the customer's consent, and the procedure for money transfer operators, payment system operators, payment infrastructure service providers to take measures to prevent money transfers without the customer's consent [4];

The Bank of Russia's regulation establishing mandatory requirements for credit institutions to ensure data protection in the course of banking activities [5];

The Bank of Russia's regulation establishing mandatory requirements for non-bank financial institutions to ensure data protection in financial markets [6];

National Standard of the Russian Federation GOST R ISO/IEC 15 408-3-2013 'Information Technology. Security Methods and Tools. Criteria for Assessing Information Technology Security. Part 3. Security Confidence Components' [19];

The Bank of Russia's regulation establishing the forms and procedure for money transfer operators to send notifications about suspending money transfers to the payee's bank account or increasing the payee's electronic money balance, as well as about the impossibility of suspending money transfers to the bank account of the payee or suspending the increase in the electronic money balance of the payee [20];

The Bank of Russia's regulation establishing requirements for ensuring data protection in the Bank of Russia payment system [21].

3.1. Incidents associated with violations of data protection requirements include:

– incidents associated with violations of data protection requirements when making money transfers;
– incidents associated with violations of data protection requirements in the course of banking activities;
– incidents associated with violations of data protection requirements in financial markets;
– incidents associated with a failure to provide money transfer services or their untimely provision;
– incidents associated with a failure to provide financial (banking) services or their untimely provision.

3.2. For the purposes of this standard, an incident involving a violation of data protection requirements shall mean one or a series of related undesirable or unexpected data protection events that may result or have already resulted in the following negative consequences:

– transferring funds without the customer's consent;
– conducting a financial (banking) operation without the customer's consent;
– a failure to provide money transfer services or their untimely provision;
– a failure to provide financial (banking) services or their untimely provision.
– Data protection shall include the following events:

a) receiving notifications by information exchange participants, including:

- upon receiving by the money transfer operator servicing the payer, including the e-money operator, of notifications in the form provided for by the relevant contract from customers, including individuals, legal entities, individual entrepreneurs, or persons engaged in private businesses, about actual and (or) attempted money transfers without the customer's consent and the use of electronic payment instruments;
- when the money transfer operator servicing the payee, including the e-money operator, identifies transactions with signs of a money transfer without the customer's consent established by the Bank of Russia and posted on the Bank of Russia website;
- receiving by the payment system settlement centre of notifications from payment system participants about funds debiting from their correspondent accounts without their consent and (or) using distorted information contained in the orders of payment clearing centres or payment system participants;

- receiving notifications from individual customers, and (or) individual entrepreneurs, and (or) persons engaged in private businesses in accordance with the procedure established by Russian laws, and (or) legal entities on conducting financial (banking) operations without their consent;

b) the identified occurrence and (or) a change in the condition of an aggregate of access objects and resources, information processing facilities and systems, including automated systems (hereinafter, AS) used to provide IT support to business processes and (or) technological processes of information exchange participants, which may have the following consequences:

- identification by the money transfer operator servicing the payer, including the electronic money operator, of money transfer and cash receipt transactions resulted from unauthorised access to the information infrastructure of the money transfer operator, including when the balance of electronic funds, excluding virtual payment cards, is reduced;
- conducting financial (banking) operations as a result of unauthorised access to information infrastructure facilities of a non-bank financial institution;
- unauthorised withdrawal of funds of the money transfer operator at ATMs;
- unauthorised withdrawal of funds of the electronic money operator at ATMs;
- a failure to provide money transfer services or their untimely provision by the money transfer operator;
- a failure to provide by settlement services or their untimely provision by the settlement centre of an important payment system;
- a failure to provide payment clearing services or their untimely provision by the payment clearing centre of an important payment system;
- a failure to provide operational services or their untimely provision by the operational centre of an important payment system;
- a failure to provide financial (banking) services or their untimely provision;
- identification by the money transfer operator, including the electronic money operator and (or) the payment infrastructure service provider, of attacks which, if launched, may result in actual and attempted money transfers without the customer's consent.

4. Designations and abbreviations

DDoS (Distributed Denial of Service) is a distributed ‘denial of service’ attack with a simultaneous use of a large number of attacking computers as a rule aimed at partial disrupting of the nominal functionality of the information structure of an organisation

IPv4 – Internet Protocol version 4

URL – Uniform Resource Locator

AS – Automated system(s)

BIN – Bank Identification Number is a part of the payment card number used to identify the issuing bank within the card payment system during authorisation, processing and clearing operations

Botnet is a computer network consisting of nodes running the same type of centrally managed malware

MC – Malicious Code

MCSE – Malicious Code Side Effect(s)

CII – Critical Information Infrastructure

OGRN – Primary State Registration Number

OKOPF – All-Russian Classifier of Organisational and Legal Forms

OKTMO - All-Russian Classifier of Municipal Territories

OS – operating system

Internet – Internet Telecommunications Network

CIPF – Cryptographic Information Protection Facility

SNILS – individual insurance account number of the insured in the customised account system of the Pension Fund of the Russian Federation

5. The data submission form used by information exchange participants for registration with the Bank of Russia

5.1. Mandatory conditions and time characteristics of information provision

Mandatory information conditions:

[O] – information of the data block (field) shall be provided as required;

[N] [N] – information of the data block (field) shall be provided in the case of technical capability.

Time characteristics of information provision (stages of information provision):

[1] – information of the data block (field) shall be provided within the registration of an information exchange participant;

[2] – information of the data block (field) shall be provided as part of the change in registration data of an information exchange participant.

5.2. Registration data of an information exchange participant. Data block **[HEADER]**

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
1.1	'schemaType' (data field)	type of electronic message	Specify the value of [**PARTICIPANT**] – information exchange participant	{ 'header': { 'schemaType': 'participant', 'schemaVersion': '1', 'version': '1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z', 'modifiedAt': '2002-10-02T15:00:00.05Z' },	[O]	[1], [2]
1.2	'schemaVersion' (data field)	version of electronic message type scheme	Textarea (text field)		[O]	[1], [2]
1.3	'version' (data field)	version number of electronic message during information exchange	numeric value (int)		[O]	[1], [2]
1.4	'memberId' (data field)	identifier of an information exchange participant assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia		[O]	[2]
1.5	'sourceId'	Identifier	128-bit identifier		[O]	[1], [2]

	(data field)	assigned by an information exchange participant	(GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant			
1.6	'publishedAt' (data field)	date and time of registration of an information exchange participant	data provision format in accordance with Specification RFC 3339 [11]		[O]	[1], [2]
1.7	'modifiedAt' (data field)	date and time of a change in the registration data of an information exchange participant	data provision format in accordance with Specification RFC 3339 [11]		[O]	[2]

5.3. Registration data of an information exchange participant. Data Block [**PARTICIPANT**]

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
2.1	'orgId' (data field)	information exchange participant identifier	It is determined by the type of an information exchange participant: • an information exchange participant operating as a money transfer operator – the number of the licence issued by the Bank of Russia; • an information exchange participant operating as a payment infrastructure service provider – the payment infrastructure service operator's registration number	'participant': { 'orgId': 'information exchange participant identifier' 'orgBrand': 'brand name of an information exchange participant', 'orgShortName': 'short name of an information exchange participant', 'orgFullName': 'full name of an information exchange participant', 'orgE-mails':['qwerty1@example.ru','qwerty2@example.ru'], 'orgIncomingEmail': 'requestsFromfincert@example.ru', 'orgBik': '123456789', 'orgLegalEntityForm': '12345', 'orgBin': ['123456', '123456'], 'orgInn': '1234567890', 'orgKpp': '123456789',	[O]	[1], [2]

			of payment infrastructure;
			• an information exchange participant operating as a payment system operator – the payment system operator's registration number;
			• an information exchange participant operating as a professional securities market participant – the number of the licence issued by the Bank of Russia;
			• an information exchange participant operating as the management company of an investment fund, a unit investment fund and a non-governmental pension fund – the number of the licence issued by the Bank of Russia;
			• an information exchange participant operating as a specialised depository of an investment fund, a unit investment fund and a non-governmental pension fund – the number of the licence issued by the Bank of Russia;
			• an information exchange participant operating as a
				'orgOgrn': '1234567890000',
				'isp': [{
				'name': 'telecom operator name,
				'ipAddress': ['192.168.1.0',
				'192.168.2.0']
				}],
				'software': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'type': 'type of software/hardware of an information exchange participant',
				'name': 'name of software/hardware',
				'version': 'software/hardware version used',
				'description': 'additional description of software/hardware'
				}],
				'persons': [{
				'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c',
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'lastName': 'surname',
				'middleName': 'middle name',
				'firstName': 'name',
				'landlineNumber': '1234567890000',
				'mobileNumber': '1234567890000', 'email': 'qwerty1@example.ru',
				'position': 'position',
				'active': 'availability of access to the personal account of an information exchange participant',
				'category': 'category of the structural unit of the responsible person of an information exchange participant'
				}],
				'id_cii': 'CII object identifier',
				'orgType': 'information exchange participant type',
				'legalAddress': {
				'oktmo': '12345678',
				'postalCode': 'postal code','country': 'three-letter country code',
				'federalDistrict': 'federal district code',		

			joint-stock investment fund – the number of the licence issued by the Bank of Russia;
			• an information exchange participant engaged in clearing activities – the number of a licence issued by the Bank of Russia;
			• an information exchange participant performing functions of the central counterparty – registration number from the register of state registration of credit institutions;
			• an information exchange participant operating as a trade organiser – the number of a licence issued by the Bank of Russia (directory of financial market participants);
			• an information exchange participant performing activities of the central depository – OGRN;
			• an information exchange participant engaged in repository activities – number of the licence issued by the Bank of Russia;
			• an information exchange
				'subjectOfFederation': '00',
				'fiasId': 'e6668cfd-ae08-4b02-a385-88179dfb1097',
				'district': 'district',
				'city': 'city',
				'cityDistrict': 'inner city district', 'locality': 'residential area',
				'street': 'street', 'house': 'house number',
				'building': 'block/building', 'room' 'room/office',
				'additionalInformation': 'additional information'
				},
				'postAddress': {
				'oktmo': '12345678',
				'postalCode': 'postal code','country': 'three-letter country code',
				'federalDistrict': 'federal district code',
				'subjectOfFederation': '00',
				'fiasId': '8abe47a7-24dd-4951-ae16-f2781eba9d93',
				'district': 'district',
				'city': 'city',
				'cityDistrict': 'inner city district', 'locality': 'residential area',
				'street': 'street', 'house': 'house number',
				'building': 'block/building', 'room' 'room/office',
				'additionalInformation': 'additional information'
				},
				'physicalAddress': [{
				'oktmo': '12345678',
				'postalCode': 'postal code','country': 'three-letter country code',
				'federalDistrict': 'federal district code',
				'subjectOfFederation': '00',
				'fiasId': '8661e93f-6c6a-4b19-b485-14e27e564169',		

			participant operating as an insurance entity - the number of the licence issued by the Bank of Russia; • an information exchange participant operating as a non-governmental pension fund - the number of the licence issued by the Bank of Russia (a directory of financial market participants); • an information exchange participant operating as a microfinance organisation - the registration number of the record in the state register of microfinance organisations; • an information exchange participant operating as a consumer credit cooperative, – OGRN; • an information exchange participant operating as a housing savings cooperative – OGRN; • an information exchange participant operating as a credit history bureau – the number in the state register of credit history bureaus; • an information	'district': 'district', 'city': 'city', 'cityDistrict': 'inner city district', 'locality': 'residential area', 'street': 'street', 'house': 'house number', 'building': 'block/building', 'room' 'room/office', 'additionalInformation': 'additional information' }] } }		

			exchange participant operating as an insurance entity - the number of the licence issued by the Bank of Russia; • an information exchange participant operating as a non-governmental pension fund - the number of the licence issued by the Bank of Russia (a directory of financial market participants); • an information exchange participant operating as a microfinance organisation - the registration number of the record in the state register of microfinance organisations; • an information exchange participant operating as a consumer credit cooperative, – OGRN; • an information exchange participant operating as a housing savings cooperative – OGRN; • an information exchange participant operating as a credit history bureau – the number in the state	'district': 'district', 'city': 'city', 'cityDistrict': 'inner city district', 'locality': 'residential area', 'street': 'street', 'house': 'house number', 'building': 'block/building', 'room' 'room/office', 'additionalInformation': 'additional information' }] } }		

			register of credit history bureaus; • an information exchange participant operating as an actuary – the registration number of the record on entering information in the unified register of responsible actuaries; • an information exchange participant operating as a credit rating agency - number of the issued form of the certificate of entry of information about the legal entity in the register of credit rating agencies; • an information exchange participant operating as an agricultural consumer credit cooperative – number in the state register of agricultural consumer credit cooperatives; • an information exchange participant operating as a pawnshop – number in the state register of pawnshops; • information exchange participant (state authorities, foreign organisations,			

			providers, software developers, centres of competence for countering cyber threats) – full name of the organisation			
2.2	‘orgBrand’ (data field)	name of the information exchange participant's brand -	textarea (text field)		[N]	[1], [2]
2.3	‘orgShortName’ (data field)	short name of the information exchange participant	textarea (text field)		[N]	[1], [2]
2.4	‘orgFullName’ (data field)	full name of an information exchange participant	textarea (text field)		[O]	[1], [2]
2.5	‘orgEmails’ (data field)	addresses of group mailboxes of an information exchange participant	Addresses of electronic mailboxes of an information exchange participant shall be submitted in the format in accordance with Specification RFC 5322 [18]		[O]	[1], [2]
2.6	‘orgIncomingEmail (data field)	the information exchange participant's mailbox address for receiving messages from the Bank of Russia	The e-mail address for receiving messages from the Bank of Russia shall be submitted in the format in accordance with Specification RFC 5322 [18]		[O]	[1], [2]
2.7	‘orgBik’ (data field)	BIC of the information exchange participant	in the **AAAAAAAAA** format		[O1]	[1], [2]

1 Mandatory notification is established only for credit institutions.

2.8	‘orgLegalEntityFor m’ (data field)	OKOPF code of the information exchange participant	in the five-digit format – **XXXXX**		[O]	[1], [2]
2.9	‘orgBin’ (data field)	BIN of the information exchange participant	in the six-digit format – **XXXXXX**		[N]	[1], [2]
2.10	‘orgInn’ (data field)	TIN of the information exchange participant	in the **XXXXXXXXXX** format		[O]	[1], [2]
2.11	‘orgKpp’ (data field)	KPP (tax registration reason code) of the exchange participant	in the nine-digit code format – **NNNNPPXXX**		[O]	[1], [2]
2.12	‘orgOgrn’ (data field)	OGRN of the information exchange	in the 13-digit format **СГГКККННХХХХХЧ**		[O]	[1], [2]
2.13	‘Isp’(data block)	telecom operator’s identifier	If it is necessary to specify several values of data fields (name, ipAddress), specify one or several objects in the data block ‘isp’		[O]	[1], [2]
2.13.1	‘name’ (data field)	telecom operator name	textarea (text field)		[O]	[1], [2]
2.13.2	‘ipAddress’ (data field)	external IP addresses of the information exchange participant	Logical addresses of type IPv4 shall comply with Specification RFC 791 [12]		[O]	[1], [2]
2.14	‘software’ (data block)	composition of software/hardware used	If it is necessary to specify several data field values (sourceId, type, name, version, description), specify one or several objects in the ‘software” data block		[N]	[1], [2]

2.14.1	'sourceId' (data field)	identifier assigned by the information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant		[N]	[1], [2]
2.14.2	'type' (data field)	type of software/hardware of the information exchange participant	One code is selected from the limited set of possible values: 1) system levels: • **[hw]** – hardware, • **[net]** – network equipment, • **[net _ s]** – network applications and services, • **[hw _ s]** – server components of virtualisation, software infrastructure services, • **[os]** – operating systems, database management systems, application servers; 2) the level of AS and applications used to provide services within the framework of business or technological processes of an information exchange participant: • **[rbs]** – remote banking system, • **[front-office]** – transaction processing system,		[N]	[1], [2]

			conducted by using payment cards, • **[web]** – information resources of the Internet, • **[abs]** – automated banking system, • **[back-office]** – system for post-transaction servicing of payment card transactions, • **[int-services]** – internal information infrastructure for supporting business processes of an information exchange participant (mail servers, file servers); • **[participant_w]** – terminal equipment (AWS) used by employees of an information exchange participant.			
2.14.3	'name' (data field)	name of software/ hardware used	textarea (text field)		[N]	[1], [2]
2.14.4	'version' (data field)	software/hardware version used	textarea (text field)		[N]	[1], [2]

2.14.5	‘description’ (data field)	additional description of software/hardware used	textarea (text field)		[N]	[1], [2]
2.15	‘persons’ (data block)	responsible person identifiers	If it is required to indicate several values of data fields (memberId, sourceId, lastName, middleName, firstName, landlineNumber, mobileNumber, email, position, active) one or several objects shall be specified in the ‘persons” data block		[O]	[1], [2]
2.15.1	‘memberId’ (data field)	identifier of the responsible person of an information exchange participant assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia		[O]	[2]
2.15.2	‘sourceId’ (data field)	identifier of the responsible person in the information exchange participant system	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant		[O]	[1], [2]
2.15.3	‘lastName’ (data field)	surname	textarea (text field)		[O]	[1], [2]
2.15.4	‘middleName’	middle name	textarea (text field)		[O]	[1], [2]

	(data field)					
2.15.5	'firstName' (data field)	name	textarea (text field)		[O]	[1], [2]
2.15.6	'landlineNumber' (data field)	stationary telephone	textarea (text field)		[O]	[1], [2]
2.15.7	'mobileNumber' (data field)	mobile telephone	textarea (text field)		[O]	[1], [2]
2.15.8	'email' (data field)	e-mail address	textarea (text field)		[O]	[1], [2]
2.15.9	'position' (data field)	position	textarea (text field)		[O]	[1], [2]
2.15.10	'active' (data field)	availability of access to the personal account of an information exchange participant	One code shall be selected from the limited set of possible values: • **[ACT]** – access to the personal account of an information exchange participant is activated; • **[DIS]** – access to the personal account of an information exchange participant is not activated		[O]	[2]
2.15.11	'category' (data field)	category of the structural division of the responsible person of an information exchange participant	One code shall be selected from the limited set of possible values: • **[MANAGEMENT] –** top management; • **[SECURITY]** – information security units; • **[IT]** – IT units; • **[RISKS]** – risk management units; • **[PAYMENT]** - operational units; • **[OTHER]** - other structural units		[O]	[1], [2]

2.16	'ID_CII' (data field)	identifier of a CII object	textarea (text field)		[N]	[1], [2]
2.17	'orgType' (data field)	type of an information exchange participant	One code shall be selected from the limited set of possible values: • **[PSP]** is an information exchange participant engaged in the money transfer operator's activity; • **[SOPI]** is an information exchange participant engaged in the payment infrastructure service provider's activity; • **[PS]** is an information exchange participant engaged in the payment system operator's activity. <u>Non-bank financial institutions:</u> • **[PSB]** is an information exchange participant engaged in the activity of a professional securities market participant; • **[MOF]** is an information exchange participant operating as the management company of an investment fund, a unit investment fund and a non-governmental pension fund;		[O]	[1], [2]

			• **[SDIF]** is an information exchange participant operating as a specialised depository of an investment fund, a unit investment fund and a non-governmental pension fund; • **[IncIF]** is an information exchange participant operating as a joint-stock investment fund; • **[CC]** is an information exchange participant engaged in clearing activities; • **[CCOUNT]** is an information exchange participant performing the functions of a central counterparty; • **[TDO]** is an information exchange participant engaged in the activity of a trade organiser; • **[CD]** is an information exchange participant operating as a central depository; • **[RO]** is an information exchange participant engaged in repository activities; • **[SIB]** is an information exchange participant			

			operating as an insurance entity; • **[NGPF]** is an information exchange participant operating as a non-governmental pension fund; • **[MFO]** is an information exchange participant operating as a microfinance organisation; • **[CCC]** is an information exchange participant operating as a consumer credit cooperative; • **[HCCC]** is an information exchange participant operating as a housing savings cooperative; • **[CHB]** is an information exchange participant operating as a credit history bureau; • **[AA]** is an information exchange participant engaged in actuarial activities; • **[CRA]** is an information exchange participant operating as a credit rating agency;			

			• **[ACCC]** is an information exchange participant operating as an agricultural consumer credit cooperative; • **[PWS]** is an information exchange participant operating as a pawnshop. <u>Public authorities:</u> • **[FED]** is an information exchange participant who is a federal executive authority; • **[REG]** is an information exchange participant who is an executive authority of a constituent entity of the Russian Federation; • **[localGov]** is an information exchange participant who is a local government; • **[LEA]** is a law enforcement agency. <u>Telecom operators:</u> • **[MO]** is an information exchange participant who is a cellular mobile operator; • **[ISP]** is an information exchange participant who is an Internet provider; <u>Software developers:</u> • **[devBANK]** is an information exchange participant – a eveloper of application software			

			for financial (banking) activities; • **[devVIRUS]** is an information exchange participant – a developer of anti-malware tools (hereinafter, AMW tools); • **[devOTHER]** is an information exchange participant -– an other software developer. Foreign organisations: • **[FNB]** is an information exchange participant who is a foreign central (national) bank; • **[FB]** is an information exchange participant -– a foreign bank; • **[FOTHER]** is an information exchange participant -– other foreign organisation. Centres of competence for countering cyber threats: • **[CERTRUS]** is an information exchange participant – a Russian cyber threat prevention centre; • **[CERTINT]** is an information exchange participant – a foreign centre for countering			

			cyber threats; • **[OTHER]** is an information exchange participant – other organisation			
2.18	'legalAddress' (block)	legal address of the Information exchange participant	text fields (textarea)		[O]	[1], [2]
2.19	'postAddress' (data block)	postal address of the information exchange participant	text fields (textarea)		[O]	[1], [2]
2.20	'physicalAddress' (data block)	actual address of the information exchange participant	text fields (textarea)		[O]	[1], [2]

6. The data submission form used by information exchange participants to inform the Bank of Russia about incidents related to violation of data protection requirements and deadlines for data submission to the Bank of Russia

6.1. Mandatory conditions and time characteristics of information

Mandatory information conditions:
[O] – data block (field) information shall be provided as required;
[N] – data block (field) information shall be provided if it is technically feasible.
Time characteristics of information provision (stages of information provision):
[1] – data block (field) information shall be provided as part of the initial notification (for important entities of the critical information infrastructure, the information shall be sent to the Bank of Russia within three hours from the moment of incident detection, for other information exchange participants within 24 hours from the moment of incident detection);
[2] – data block (field) information shall be provided as part of an interim notification (for important entities of the critical information infrastructure, the information shall be sent to the Bank of Russia within three hours after the incident is detected, for other information exchange participants within two business days after the initial notification or the previous interim notification);
[3] – data block (field) information shall be provided as part of the final notification of the results of the incident closure (within three business days from the moment of the incident closure by an information exchange participant).
[*] – data block (field) information shall be provided promptly upon receiving from an information exchange participant's client who is a legal entity the notification specified in Part 11 of Article 9 of Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System'.

6.2. Incident identification data. Data block **[HEADER]**

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
1 .1	'schemaType' (data field)	type of electronic message	Specify the value of [INCIDENT] - incident	{ 'header': { 'schemaType': 'incident', 'schemaVersion': '1', 'version': '1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z', 'modifiedAt': '2002-10-02T15:00:00.05Z'	[O]	[1], [2], [3], [*]
1.2	'schemaVersion' (data field)	version of electronic message version	textarea (text field)		[O]	[1], [2], [3], [*]
1.3	'version' (data field)	version number of electronic	numeric value (int)		[O]	[1], [2], [3], [*]

		message during information exchange		},		
1.4	‘memberId’ (data field)	information exchange participant identifier assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia		[O]	[1], [2], [3], [*]
1.5	‘sourceId’ (data field)	incident identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant		[O]	[1], [2], [3], [*]
1.6	‘publishedAt’ (data field)	date and time of initial provision of information	data provision format in accordance with Specification RFC 3339 [11]		[O]	[1], [2], [3], [*]
1.7	‘modifiedAt’ (data field)	date and time of interim or final notification	data provision format in accordance with Specification RFC 3339 [11]		[O]	[2], [3]

6.3. Incident description Data Block **[INCIDENT]**

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

2.1	‘fincertId’ (data field)	Incident identifier assigned by the Bank of Russia	textarea (text field)	‘incident’: {
				‘fincertId’: ‘20180324215113’, ‘fixationAt’: ‘2002-10-02T15:00:00.05Z’,
				‘description’: ‘incident description’,
				‘lawEnforcementRequest’: {
					[O]	[2], [3]

2.2	‘fixationAt’	date and time of	data provision format	‘addressed’: information exchange participant's appeal to	[O]	[1], [2], [3], [*]

	(data field)	incident registration by an information exchange participant	in accordance with Specification RFC 3339 [11]	law enforcement agencies',
				'request': 'information on the fact of an information exchange participant's appeal to the police',
				'number': '123123',
				'numberTicket': '1234567890', 'dateTimeAt': '2002-10-02T15:00:00.05Z'
				},
				'assistance': 'identifier of the need to support an information exchange participant by the Bank of Russia',
				'vectorCode': 'computer attack vector identifier',
				'serviceType': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985av6d91c',
				'type': 'type of attacked object',
				'name': 'name of software /hardware',
				'version': 'software/hardware version',
				'description': 'additional description of the type of the object under attack'
				}],
				'registration': {
				'department': 'the structural (organisational) unit of an information exchange participant where the incident was registered (detected)',
				'technicalDevice': 'technical tools of incident registration'
				},
				'typeOfAttack': 'computer attack type code',
				'measuresAndRecomendations': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'dateTimeAt': '2018-03-22T08:14:38Z',
				'action': 'actions taken to eliminate the incident',
				'text': 'the text of measures taken or recommendations received',
				-
				'attachment': {
				'sourceId': 'f34030ef-358a-445c-8567-		

2.3	'description' (data field)	incident description	textarea (text field)		[O]	[1], [2], [3], [*]
2.4	'lawEnforcement Request' (data block)	an information exchange participant's appeal to law enforcement agencies			[O]	[2], [3]
2.4.1	'addressed' (data field)	an entity who applied to law enforcement agencies	One code shall be selected from the limited set of possible values: • **[PIE]** - information exchange participant; • **[CIE]** - client of an information exchange participant		[O]	[2], [3]
2.4.2	'request' (data field)	information on the fact of an information exchange participant's appeal to law enforcement agencies	One code shall be selected from the limited set of possible values: • **[POL]** - an appeal to law enforcement agencies; • **[NPL]** - no appeal to law enforcement agencies		[O]	[2], [3]
2.4.3	'number' (data field)	application number from the register of crime reports	numeric value (int)		[O]	[2], [3]
2.4.4	'numberTicket' (data field)	number of the ticket for accepting and registering	numeric value (int)		[O]	[2], [3]

		applications		25985ce6d91c’,
				‘comment’: 'description of the attachment', 'dateTimeAt': ‘2018-03-22T08:14:38Z’,
				‘file’: {
				‘name’: 'file name',
				‘size’: 'file size in bytes',
				‘base64’: 'attachment in base64 format'
				},
				‘fileLink’: ‘http://domain.com/archive.rar’
				}
				}],		

2.4.5	'dateTimeAt' (data field)	date and time of the application acceptance	data provision format in accordance with Specification RFC 3339 [11]		[O]	[2], [3]
2.5	'assistance' (data field)	identifier of the need to support an information exchange participant by the Bank of Russia	One code shall be selected from the limited set of possible values: • **[HLP]** - support from the Bank of Russia is needed; • **[NND]** - no support required from the Bank of Russia		[O]	[1], [2], [3], [*]
2.6	'vectorCode' (data field)	computer attack vector identifier	One code shall be selected from the limited set of possible values: • **[INT]** – vector aimed at the information exchange participant infrastructure; • **[EXT]** – vector aimed at an information exchange participant's client		[O]	[1], [2], [3], [*]
2.7	'serviceType'(data block)	information infrastructure object identifier	If it is necessary to specify several data field values (sourceId, type, name, version, description), one or several objects in the data block 'serviceType' should be specified		[O]	[1], [2], [3], [*]
2.7.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange		[O]	[1], [2], [3], [*]

			participant			
2.7.2	'type' (data field)	type of the object under attack	One code shall be selected from the limited set of possible values: 1) system levels: • **[hw]** - hardware, • **[net]** - network equipment, • **[net _ s]** – network applications and services, • **[hw _ s]** – server components of virtualisation, software infrastructure services, • **[os]** - operating systems, database management systems, application servers; 2) the level of AS and applications used to provide services within the framework of business or technological processes of an information exchange participant: • **[rbs**] – remote banking system, • **[front-office]** - payment card transaction processing system, • **[web]** - information resources of the		[O]	[1], [2], [3], [*]

			Internet, • **[abs]** – automated banking system, • **[back-office]** - a system of post-transaction servicing of operations conducted using payment cards; • **[int-services]** – internal information infrastructure for supporting business processes of an information exchange participant (mail servers, file servers); • **[participant _ w]** - terminal equipment (AWS) used by employees of an information exchange participant; 3) the level of the AS and applications operated by an information exchange participant's client: • **[cfs]** - file server, • **[crbs]** – remote banking system, • **[ecs]** - e-mail server; • **[client _ w]** - automated systems used by employees of an information			

			exchange participant's client; 4) other system: • **[oth]** - other system			
2.7.3	'name' (data field)	'name of software hardware -	textarea (text field)		[O]	[1], [2], [3], [*]
2.7.4	'version' (data field)	software/ hardware version	textarea (text field)		[O]	[1], [2], [3], [*]
2.7.5	'description' (data field)	additional description of the type of an attacked object	textarea (text field)		[O]	[1], [2], [3], [*]
2.8	'registration' (data block)	incident localisation identifier			[O]	[1], [2], [3], [*]
2.8.1	'department' (data field)	the attacked structural (organisational) unit of an information exchange participant where an incident was registered (detected)	textarea (text field)		[O]	[1], [2], [3], [*]
2.8.2	'technicalDevice' (data field)	technical tools of incident registration	textarea (text field)		[O]	[1], [2], [3], [*]
2.9	'typeOfAttack' (data field)	Computer attack type identifier	One code shall be selected from the limited set of possible values:		[O]	[1], [2], [3], [*]

			• **[trafficHijackAttacks]** – computer attacks related to changes in route and address information; • **[malware]** – computer attacks related to the use of malicious software in relation to information infrastructure objects of information exchange participants and their clients; • **[socialEngineering]** – computer attacks launched after inducing customers to make money transfers by deceit or breach of trust; • **[ddosAttacks]** – denial-of-service computer attacks (DDoS attacks) in relation to the information infrastructure of information exchange participants; • **[atmAttacks]** – computer attacks related to unauthorised access to ATMs and payment terminals of information exchange participants;			

			• **[vulnerabilities]** – computer attacks related to the full use of vulnerabilities (exploiting vulnerabilities) of the information infrastructure of information exchange participants and their clients for the benefit of an attacker; • **[bruteForces]** – computer attacks related to searching (hacking) and compromising authentication data (login details); • **[spams]** – computer attacks related to spamming information exchange participants and their customers; • **[controlCenters]** – computer attacks related to the detection of interaction of information infrastructure objects of information exchange participants with Botnet command centres; • **[sim]** – computer attacks associated with the change (substitution) of the mobile subscriber identifier (IMSI) of the SIM card number, as well as with the replacement of the mobile equipment identifier (IMEI); • **[phishingAttacks]** –			

			computer attacks associated with data that are deceptive for information exchange participants and their clients, as well as other persons interacting with them, regarding the ownership of information distributed via the Internet due to the similarity of domain names, design or content; • **[prohibitedContents]** – computer attacks associated with the distribution of information regarding the offer and/or provision of financial services in the Russian Federation by persons not entitled to provide them in accordance with the legislation of the Russian Federation. Posting of prohibited content on the Internet; • **[maliciousResources]** – computer attacks associated with the placement on the Internet of information enabling illegal access to information systems of information exchange participants and their customers used in the provision (receipt) of			

			financial services, including through illegal access to confidential customer information. Placement of a malicious resource on the Internet; • **[changeContent]** – computer attacks related to a change in content; • **[scanPorts]** – computer attacks related to scanning software ports of information infrastructure objects of information exchange participants by persons who do not have the relevant authority; • **[other]** – other computer attacks directed to information infrastructure objects of information exchange participants and their clients			
2.10	'measuresAndRe-comendations' (data block)	actions taken to eliminate an incident	If it is necessary to specify several data field values (sourceId, dateTimeAt, action, text), one or several objects in the data block 'measuresAndRecomend ations' are to be specified		[N]	[1], [2], [3]
2.10.1	'sourceId'	Identifier	128-bit identifier		[N]	[1], [2], [3]

	(data field)	assigned by an information exchange participant	(GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant			
2.10.2	'dateTimeAt' (data field)	date and time of actions taken to eliminate an incident	data provision format in accordance with Specification RFC 3339 [11]		[N]	[1], [2], [3]
2.10.3	'action' (data field)	actions taken to eliminate an incident	One code shall be selected from the limited set of possible values: • **[measures]** – the measures taken; • **[recommendations]** – recommendations		[N]	[1], [2], [3]
2.10.4	'text' (data field)	measures taken or recommendations followed	textarea (text field)		[N]	[1], [2], [3]
2.10.5	'attachment' (data block)	additional data on the measures taken to eliminate an incident			[N]	[1], [2], [3]
2.10.5.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant		[N]	[1], [2], [3]
2.10.5.2	'comment' (data field)	description of the attachment	textarea (text field)		[N]	[1], [2], [3]
2.10.5.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[1], [2], [3]

2.10.5.4	'file' (data block)	data file	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[N]	[1], [2], [3]
2.10.5.5	'fileLink' (data field)	reference link for obtaining (downloading) the data file	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]		[N]	[1], [2], [3]

6.4. Incident classification. Data Block **[INCIDENT]**

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

3.1	'location' (data block)	identifier of the geographical location of the incident		‘location’: {
				‘subjectOfFederation’: ‘00’,
				‘locality’: 'residential area name'
				},
				‘classification’: {
				‘typeOfIncident’: 'incident type,
				'ext': [{
				‘events’: 'data protection events'
				‘method’: 'method of preparing and transferring operational instructions enabling financial transactions'
				}],
				‘int’: [{
				‘events’: 'data protection events',
				‘typeOfIntruder’: 'intruder type'
				}],
				‘damage’: {
				‘operating’: 'assessment of operational expenses of an information exchange participant at the moment of providing data on the occurrence of an incident (INT vector)',
					[O]	[1], [2], [3], [*]

3.1.1	‘subjectOfFederation’ (data field)	upper-level OKTMO code	textarea (text field)		[O]	[1], [2], [3], [*]
3.1.2	'locality' (data field)	name of a residential area	textarea (text field)		[O]	[1], [2], [3], [*]
3.2	‘classification’ (data block)	incident classification			[O]	[1], [2], [3], [*]
3.2.1	'typeOfIncident' (data field)	incident type	One code shall be selected from the limited set of possible values: • **[MTR]** – an incident involving a violation of the information protection requirements when making money transfers; when making		[O]	[1], [2], [3], [*]

			money transfers;
			• **[BAC]** – an incident involving a violation of the information protection requirements in the course of banking activities;
			• **[FMA**] – an incident involving a violation of the information protection requirements in financial markets;
			• **[DT _ MTR]** – an incident involving the non-provision or untimely provision of money transfer services;
			• **[DT _ FS]** – an incident related to a failure to provide financial services or their untimely provision
				'relative': 'relative (qualitative) assessment of the scale (severity of consequences) of an incident (INT vector
				)',
				'schemaConclusion': 'description of a money withdrawal scheme',
				'attachments': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'comment': 'description of the attachment', 'dateTimeAt': '2018-03-22T08:14:38Z',
				'file': {
				'name': 'file name',
				'size': 'file size in bytes',
				'base64': 'attachment in base64 format'
				},
				'fileLink': 'http://domain.com/archive.rar'
				}]
				},		

3.2.2.	'ext' (data subblock)	occurrence of an incident involving an information exchange participant's client	If it is necessary to specify several data field values (events, method), specify one or several objects in the 'ext' data sub-block		[O]	[1], [2], [3], [*]
3.2.2.1	'events' (data field)	data protection events	One code shall be selected from the limited set of possible values: • **[MTR _ WC]** – receipt by the money transfer operator servicing the payer, including the electronic money operator, of notifications in the form stipulated by the agreement from		[O]	[1], [2], [3], [*]

			customers – individuals, legal entities, individual entrepreneurs, or individuals engaged in private business, about cases and (or) attempts to transfer funds without their client's consent, including the use of electronic payment instruments; • **[A _ SC]** – receipt by the payment system settlement centre of notifications from payment system participants on the debiting of funds from their correspondent accounts without their consent and/or using distorted information contained in the orders of payment clearing centres or payment system participants; • **[UO _ WC]** – identification by the money transfer operator servicing the payer, including the electronic money operator, of transactions with signs of a money transfer without the customer's consent as established by the Bank of Russia and described on			

			the Bank of Russia website; • **[FMA _ WC]** – receipt of notifications from customers: individuals, and (or) individual entrepreneurs, and (or) individuals engaged in private business in accordance with the procedure established by the legislation of the Russian Federation, and (or) legal entities about conducting a financial (banking) transaction without their consent; • **[OTH]** – other events the consequences or identification of which may lead to incidents specified in codes **[MTR], [BAC], [FMA], [DT _ MTR], [DT_FS]**			
3.2.2.2	'method' (data field)	a method of creating and transferring operational instructions enabling a financial transaction	One code shall be selected from the limited set of possible values: • **[SMS]** is a remote service technology where information is exchanged between an information exchange participant and its client using short text messages from the telephone number specified in the bank account agreement;		[O]	[1], [2], [3], [*]

			• **[MBB]** is a remote service technology which helps exchange information between an information exchange participant and its client using software developed for mobile operating systems (e.g., iOS, Android); • **[BRW]** is a remote service technology which helps exchange information between an information exchange participant and its client using an internet browser without installing additional software; • **[PCW]** is a remote service technology which helps exchange information between an information exchange participant and its client from a personal computer using additional software provided by the information exchange participant; • **[ATM]** is an ATM;			

			• **[CIN]** is an ATM capable to accept cash; • **[REC]** is an ATM with a recycling function; • **[POS]** is a POS terminal; • **[SST]** is a payment terminal; • **[CNP]** is making transfers using payment cards without their direct use (CNP transactions); • **[OTH]** is another method of creating and transferring transaction instructions enabling a financial transaction			
3.2.3	'int' (data subblock)	an incident in the information infrastructure of an information exchange participant	If it is necessary to specify several data field values (events, method), one or several objects in the 'int' data sub-block shall be specified		[O]	[1], [2], [3], [*]
3.2.3.1	'events' (data field)	data protection events	One code shall be selected from the limited set of possible values: • **[MTR _ UA]** – identification by the money transfer operator servicing the payer, including		[O]	[1], [2], [3], [*]

			the electronic money operator, of money transfer operations and cash receipts as a result of unauthorised access to the information infrastructure of the money transfer operator, including when the balance of electronic funds is reduced, except for virtual payment cards; • **[FMS _ UA]** – conducting financial (banking) operations as a result of unauthorised access to information infrastructure facilities of a non-bank financial institution; • **[UPT _ PSP]** – unauthorised withdrawal of funds of the money transfer operator from ATMs; • **[UPT _ EMP]** – unauthorised withdrawal of funds of the electronic money operator from ATMs;			

			• **[DT _ ALL]** – failure to provide services of the money transfer operator for a period of more than two hours in general for all constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) remote banking systems (funds); • **[DT _ SELECTED]** – failure to provide services of the money transfer operator for a period of more than two hours in general for individual constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) a remote banking system (s); • **[DT _ SC]** – failure of the settlement centre to provide settlement services for a period of more than one operational day; • **[DTPT _ SC]** – failure by a settlement centre to make payments during an operational day			

			according to orders of a payment clearing centre or payment system participants accepted for execution; • **[DT _ CC]** – suspension by a clearing centre of the provision of payment clearing services for the period of more than one operational day; • **[DTPT _ CC]** – failure of a clearing centre to perform payment clearing subject to the accepted orders of the payment system participants during one operational day; • **[DT _ OC]** – suspension by an operational centre of the provision of operational services for a period of more than two hours; • **[DT _ FS _ ALL]** – non-provision of services by a non-bank financial institution for a period of more than two hours in total for all constituent territories of the Russian Federation where this non-bank financial institution provides financial (banking) services; • **[DT _ FS _ SEL]** – non-provision of services by a			

			non-bank financial institution for a period of more than two hours in total for individual constituent territories of the Russian Federation where this non-bank financial institution provides financial (banking) services; • **[PSP _ CMTR]** – detection by a money transfer operator, including an electronic money operator, and/or a payment infrastructure service provider of attacks the consequences of which may lead to events and attempts of making money transfers without their customer's consent; • **[CO _ CFS]** – detection by a credit institution of computer attacks, the consequences of which may lead to events and attempts to carry out a financial (banking) transaction without its customer's consent; • **[NCFI _ CFS]** – detection by a non-bank financial institution of computer attacks, the consequences of which may lead to events and attempts to conduct an operation in the			

			financial market without its customer's consent; • **[OTH]** – other events the consequences or detection of which may lead to incidents specified in codes [**MTR], [BAC], [FMA], [DT _ MTR], [DT_FS]**			
3.2.3.2	'typeOfIntruder' (data field)	intruder/violato type	One code shall be selected from the limited set of possible values: • **[INT _ ORG]** – unauthorised access of employees of an information exchange participant or other persons with the authority to access information infrastructure facilities of an information exchange participant (actions of an internal violator); • **[EXT _ ORG]** – computer attacks or unauthorised access of persons who do not have the authority to access information infrastructure facilities of an information exchange participant (actions of an external violator)		[O]	[1], [2], [3], [*]
3.3	'damage' (data block)	identification of damages from			[O]	[2], [3]

		unauthorised operations				
3.3.1	'operating' (data field)	assessment of operational expenses of an information exchange participant at the moment of reporting the incident occurrence (INT vector)	textarea (text field)		[N]	[2], [3]
3.3.2	'relative' (data field)	relative (qualitative) assessment of the scale (severity of consequences) of the incident occurrence (INT vector)	One code (pursuant to Section 14 hereof) is to be selected from the limited set of possible values: • **[MOD]** – moderate influence; • **[ESS]** – essential impact; • **[CRIT]** – critical impact		[O]	[2], [3]
3.4	'schema Conclusion' (data field)	description of a money withdrawal scheme	textarea (text field)		[O[1]]	[2], [3]
3.5	'attachments' (data block)	additional data for incident identification	If it is necessary to specify several data field values (sourceId, comment, dateTimeAt, file, fileLink), one or several objects in the 'attachments' data block should be specified		[N]	[1], [2], [3]

[1] *Reporting is mandatory only for non-bank financial institutions.*

3.5.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant		[N]	[1], [2], [3]
3.5.2	'comment' (data field)	attachment description	textarea (text field)		[N]	[1], [2], [3]
3.5.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[1], [2], [3]
3.5.4	'file' (data block)	data file	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[N]	[1], [2], [3]
3.5.5	'fileLink' (data field)	link for obtaining (downloading) the data file	it is required to specify URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]		[N]	[1], [2], [3]

6.5. 'Antifraud' Data Block **[ANTIFRAUD]**

The 'antifraud' data block is used by information exchange participants in the following cases:

when money transfer operators, payment system operators, and payment infrastructure service providers inform the Bank of Russia of all events and attempts to transfer funds without their customer's consent [4];

when money transfer operators inform the Bank of Russia of the suspension of funds crediting to a payee's bank account or of the increase in the balance of a payee's electronic funds [20].

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

4.1	'antifraud' (data block)		If it is necessary to specify several data block values (payerIdentifier, payer, payee, additionalStatus), one or more objects in the 'antifraud' data block shall be specified	'antifraud': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'victim': 'information on the legal status of the payer'
				'payerIdentifier': {
				'hash': 'E25059612A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9A8FA441E44',
				'hashSnils': 'C49337884A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A9A8FA441E44'
				},
				'payer': {
				'bik': '123456789',
				'inn': '123456789000',
				'payerName': 'name of the organisation that is the payer',
				'payerTransferId': {
				'transferType': 'money transfer method type',
				'paymentCard': {
				'number': '123412341234123412',
				'sum': 'amount of a money transfer transaction using
					[O]	[1], [2], [3], [*]

4.1.1	'sourceId' (data field)	identifier assigned by an information exchange participant being the payer	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant		[O]	[1], [2], [3], [*]
4.1.2	'victim' (data field)	'information on the legal status of the payer	One code shall be selected from the limited set of possible values: • **[person]** – an individual; • **[entity]** – a legal entity		[O]	[1], [2], [3], [*]

4.2	‘payerIdentifier’ (data block)	identification data defining a particular payer		payment cards',
				‘currency’:'currency of money transfers',
				‘dateTimeAt’: ‘2018-01-13T09:14:38Z’,
				‘rrn’: 'the number generated for a money transfer transaction during its authorisation'
				},
				‘settlement’: {
				‘number’: ‘12345123451234512345’,
				‘sum’: 'amount of funds to be transferred',
				‘currency’:'currency of money transfers',
				‘dateTimeAt’: ‘2018-01-13T09:14:38Z’,
				},
				‘phoneNumber’: {
				‘number’: ‘1212312345678’,
				‘sum’: 'transaction amount',
				‘currency’:'transaction currency',
				‘dateTimeAt’: ‘2018-01-13T09:14:38Z’
				},
				‘idNumber’: {
				‘number’: ‘1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT’,
				‘sum’: 'transaction amount',
				‘currency’:'transaction currency',
				‘dateTimeAt’: ‘2018-01-13T09:14:38Z’
				}
				},
				‘device’: {
					[O]	[1], [2], [3], [*]

4.2.1	'hash' (data field)	the result of calculating the hashing function of the number of an identification document in order to identify the person – the payer who sent the notification about events and (or) attempts to transfer funds without its client's consent, including the use of electronic means of payment	The sequence of symbols obtained as a result of the calculation of the SHA-256 hash function from the identification document's series and number. The series and number of the identification document are to be provided for calculating a hash function: without spaces (_), number sign (N), letters (if any) in upper case (ABC). For a Russian passport, this is **XXXXYYYYY**, where: **XXXX** is the four-digit passport series number; **YYYYYY** is the six-digit passport number. Source text encoding (before hash) – Windows-1251; Hash text encoding - Windows-1251.		[O]	[1], [2], [3], [*]
4.2.2	'hash' (data field)	the result of the calculation of	The sequence of symbols received as a result of		[O]	[1], [2], [3], [*]

		the insurance number hashing function of an individual personal account of the insured person in the personal accounting system of the Pension Fund of the Russian Federation (hereinafter, SNILS) of the payer who sent a notification of events and (or) attempts of transferring funds without their clients' consent, including the use of electronic means of payment, if any	the calculation of the SHA-256 hash function from a SNILS payer.
			
			SNILS is provided for calculating the hash function: without spaces (_) and separation marks (-).
			SNILS type:
			XXXXXXXXXXX
			
			Source text encoding (before hash)
			– Windows-1251; Hash text encoding – Windows-1251.
				'ip': '127.0.0.1',
				'imsi': 'international mobile subscriber identifier (individual subscriber number)',
				'imei': 'international mobile equipment identifier',
				'aiic': 'Acquiring institution identification code (32 field ISO 8583)',
				'cati': 'Card acceptor terminal identification (41 field ISO 8583)',
				'caic': 'Card acceptor identification code (42 field ISO 8583)',
				}
				},
				'payee': {
				'bik': '123456789',
				'inn': '123456789000',
				'payeeName': 'the name of an organisation that is the payee',
				'payeeTransferId': {
				'transferType': 'money transfer method type',
				'paymentCard': {
				'number': '123412341234123412'
				},
				'settlement': {
				'number': '12345123451234512345'
				},
				'phoneNumber': {
				'number': '1212312345678'
				},
				'idNumber': {
				'number': '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT'
				}
				}
				},
				'additionalStatus': {
				'crossBorder': 'cross-border banking		

4.3	'payer' (data block)	Information identifying the payer			[O]	[1], [2], [3], [*]

				Identifier’, ‘additionalTransactionApprove’: ['identifier of additional confirmation of a transaction'] } }],		
4.3.1	'bik' (data field)	BIC of the money transfer operator, including the e-money operator serving the payer	in the **AAAAAAAAA** format		[O]	[1], [2], [3], [*]
4.3.2	'inn' (data field)	TIN of the payer who is a legal entity and/or an individual entrepreneur, and/or a person engaged in private business	in the **XXXXXXXXXX** format for legal entities, in x**XXXXXXXXXX** or **XXXXXXXXXXXX** formats – for individual entrepreneurs and (or) individuals engaged in private business in accordance with the procedure established by the legislation of the Russian Federation		[O]	[1], [2], [3], [*]
4.3.3	'payerName' (data field)	organisation name that is the payer	textarea		[O]	[1], [2], [3], [*]
4.3.4	'payerTransferId' (data subblock)	identification data depending on the money			[O]	[1], [2], [3], [*]

		transfer method				
4.3.4.1	'transferType' (data field)	'money transfer method type',	One code shall be selected from the limited set of possible values: • **[paymentCard]** – when making money transfers using payment cards; • **[settelment]** – when making money transfers to bank accounts; • **[phoneNumber]** – when making money transfers by telephone number; • **[idNumber]** – if the balance of electronic funds changes		[O]	[1], [2], [3], [*]
4.3.4.2	'paymentCard' (data subblock)	when making money transfers using payment cards			[O]	[1], [2], [3], [*]
4.3.4.2.1	'number' (data field)	the number of the payer's payment card issued to him/her and (or) the person authorised by the payer	in the **XXXXXXXXXXXXXXXXXX** format the payment card number shall be provided without spaces (_) and		[O]	[1], [2], [3], [*]

		and the money transfer operator by the issuer	separation marks (-).			
4.3.4.2.2	'sum' (data field)	the amount of a money transfer transaction using payment cards	transaction amount – field 'F004' of ISO 8583 Financial Messaging Standard [7], [8], [9]		[O]	[1], [2], [3], [*]
4.3.4.2.3	'currency' (data field)	currency of a money transfer transaction	transaction currency – field 'F049' of ISO 8583 Financial Messaging Standard [7], [8], [9]		[O]	[1], [2], [3], [*]
4.3.4.2.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]		[O]	[1], [2], [3], [*]
4.3.4.2.5	'rrn' (data field)	the number generated for a money transfer transaction during its authorisation	the number generated for a money transfer transaction during its authorisation – field 'F037' < * > of ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of field 'F037' (Retrieval Reference Number) should be generated by		[O]	[1], [2], [3], [*]

			the acquiring bank host according to the following rule: **YJJJXXNNNNNN**, where: **Y** is the last figure of a year; **JJJ** - a Julian date; **XX** is the identifier assigned to the acquiring bank's host by the operator; **NNNNNN** - the transaction sequence number during a day			
4.3.4.3	'settlement' (data subblock)	when making money transfers in bank accounts by debiting funds from payers' bank accounts			[O]	[1], [2], [3], [*]
4.3.4.3.1	'number' (data field)	the number of the payer's bank account opened with the money transfer operator serving the payer	in the **XXXXXXXXXXXXXXXXXXXX** format bank account number is to be provided without spaces (_) and separation marks (-).		[O]	[1], [2], [3], [*]

4.3.4.3.2	'sum' (data field)	the amount of a money transfer transaction	textarea (text field)		[O]	[1], [2], [3], [*]
4.3.4.3.3	'currency' (data field)	money transfer transaction currency	textarea (text field)		[O]	[1], [2], [3], [*]
4.3.4.3.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]		[O]	[1], [2], [3], [*]
4.3.4.4	'phoneNumber' (data subblock)	when making money transfers by telephone number			[O]	[1], [2], [3], [*]
4.3.4.4.1	'number' (data field)	the payer's telephone number specified in a bank account agreement and/or an agreement on the use of electronic payment instruments concluded with the payer	in the **KKKXXXNNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number is to be provided without a plus sign (+), spaces (_) and separation signs (-).		[O]	[1], [2], [3], [*]

4.3.4.4.2	'sum' (data field)	transaction amount	textarea (text field)		[O]	[1], [2], [3], [*]
4.3.4.4.3	'currency' (data field)	transaction currency	textarea (text field)		[O]	[1], [2], [3], [*]
4.3.4.4.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]		[O]	[1], [2], [3], [*]
4.3.4.5	'idNumber' (data subblock)	if the balance of electronic funds changes			[O]	[1], [2], [3], [*]
4.3.4.5.1	'number' (data field)	the payer's identification number, in particular, the number of the payer's electronic wallet used by him/her on the basis of a bank account agreement and (or) an agreement on the use of electronic payment instruments concluded with the money transfer operator	textarea (text field)		[O]	[1], [2], [3], [*]

4.3.4.5.2	'sum' (data field)	'transaction amount', -	textarea (text field)		[O]	[1], [2], [3], [*]
4.3.4.5.3	'currency' (data field)	transaction -	textarea (text field)		[O]	[1], [2], [3], [*]
4.3.4.5.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]		[O]	[1], [2], [3], [*]
4.3.5	'device' (data subblock)	parameters of the device used to access the automated system and software for the purpose of money transfer without the customer's consent			[N]	[1], [2], [3]
4.3.5.1	'ip' (data field)	network address of a computer and/or a communication device (router) (IP)	The IPv4 network address shall comply with Specification RFC 791 [12]		[N]	[1], [2], [3]

4.3.5.2	'imsi' (data field)	International Mobile Subscriber Identity (IMSI) means the international Identifier of a mobile subscriber (individual number of a subscriber (customer – individual) by which the system recognises a mobile communication user using GSM and UMTS standards	the number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**		[N]	[1], [2], [3]
4.3.5.3	'imei' (data field)	International Mobile Equipment Identity (IMEI) means the international Identifier of a mobile equipment (a mobile device of an individual customer)	the number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**		[N]	[1], [2], [3]

4.3.5.4	'aiic' (data field)	identifier of the participant who is an acquiring bank when transferring funds using payment cards	identifier of the participant who is an acquiring bank in the course of money transfer operations using payment cards (Acquiring institution identification code) - field 'F032' of ISO 8583 [7], [8], [9]		[N]	[1], [2], [3]
4.3.5.5	'cati' (data field)	identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn	identifier of the ATM and/or the electronic terminal where the funds are transferred and/or withdrawn (Card acceptor terminal identification) - field 'F041'* of the ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of the terminal identifier shall be aligned to the left and supplemented with spaces on the right with up to 8 characters		[N]	[1], [2], [3]
4.3.5.6	'caic' (data field)	identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn by its geographical location	identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) - field 'F042'* of ISO 8583 Financial Messaging Standard [7], [8], [9] *The value of the service point identifier shall be aligned to the left and supplemented with spaces on the right with up to 15 characters		[N]	[1], [2], [3]

4.4	‘payee’ (data block)	information determining the payee			[O]	[1], [2], [3], [*]
4.4.1	'bik' (data field)	BIC of the money transfer operator serving the payee	in the **AAAAAAAAA** format		[O]	[1], [2], [3], [*]
4.4.2	'inn' (data field)	TIN of the payee - a legal entity, and (or) an individual entrepreneur, and (or) a person engaged in private business	in the **XXXXXXXXXX** format for legal entities, in X**XXXXXXXXXX** or **XXXXXXXXXXXX** formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation		[O]	[1], [2], [3], [*]

4.4.3	'payeeName' (data field)	name of the organisation that is the payee	textarea (text field)		[O]	[1], [2], [3], [*]
4.4.4	'payeeTransferId' (data subblock)	identification data depending on the money transfer method			[O]	[1], [2], [3], [*]
4.4.4.1	'transferType' (data field)	money transfer method type	One code shall be selected from the limited set of possible values: • **[paymentCard]** – when transferring funds using payment cards; • **[settelment]** – when transferring funds in bank accounts; • **[phoneNumber]** – when transferring funds by telephone number;		[O]	[1], [2], [3], [*]

			• **[idNumber]** - if the balance of electronic funds changes			
4.4.4.2	'paymentCard' (data subblock)	when transferring funds using payment cards			[O]	[1], [2], [3], [*]
4.4.4.2.1	'number' (data field)	the payment card number format of the payee issued to him/her and (or) the person authorised by the payee, the money transfer operator - the issuer	in the format **XXXXXXXXXXXXXXXXXX** payment card number shall be provided without spaces (_) and separation marks (-).		[O]	[1], [2], [3], [*]
4.4.4.3	'settlement' (data subblock)	when making money transfers in bank accounts by debiting funds from payers 'bank accounts			[O]	[1], [2], [3], [*]

4.4.4.3.1	'number' (data field)	the settlement account number of the payee opened with the money transfer operator serving the payee	in the **XXXXXXXXXXXXXXXXXXX** format bank account number is to be provided without spaces (_) and separation marks (-).		[O]	[1], [2], [3], [*]
4.4.4.4	'phoneNumber' (data subblock)	when making money transfers by telephone number			[N]	[1], [2], [3], [*]
4.4.4.4.1	'number' (data field)	the payee's phone number	in the **KKKXXXNNNNNNN** format, where: **KKK** - a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number is to be provided without a plus sign (+), spaces (_) and separation signs (-).		[N]	[1], [2], [3], [*]
4.4.4.5	'idNumber'				[O]	[1], [2], [3], [*]

	(data subblock)	if the balance of electronic funds changes				
4.4.4.5.1	'number' (data field)	identification number of the payee, in particular, the number of the electronic wallet of the payee used by him/her on the basis of a bank account agreement and (or) an agreement on the use of the electronic means of payment concluded with the money transfer operator	textarea (text field)		[O]	[1], [2], [3], [*]
4.5	'additionalStatus' (data block)	additional statuses of unauthorised transaction			[O]	[1], [2], [3], [*]
4.5.1	'crossBorder'	identifier of cross-border banking			[O]	[1], [2], [3], [*]

	(data field)		One code is selected from the limited set of possible values: • **[CRB]** – cross-border transfers; • **[DOM]** – domestic transfers -			
4.5.2	'additionalTransactionApprove' (data field)	identifier of additional confirmation of a transaction	One or more codes are to be selected from the limited set of possible values: • **[3DS]** – an operation was confirmed using 3D Secure; • **[DCS]** – implementation of technological measures to use separate technologies [3]; • **[NAA]** – an operation without confirmation; • **[SMS]** – an operation was confirmed using short text messages (SMS messages); • **[LTR]** – an operation was performed in accordance with the list of trusted payees; • **[TEL]** – an operation was confirmed by telephone; • **[OAA]** – other method of approval		[O]	[1], [2], [3], [*]

6.6. Information on technical data describing computer attacks against information infrastructure facilities of information exchange participants and their customers, as well as relevant forms of electronic messages. Data Block **[IMPACTS]**

6.6.1. Computer attacks related to changes in route and address information **[trafficHijackAttacks]** (for vector [INT], [EXT])

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
1.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange	'impacts': { 'trafficHijackAttacks': [{ 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'legalAsPath': 'legal AS-Path', 'wrongAsPath': 'wrong AS-Path', 'lookingGlass': reference link to Looking Glass used to verify AS-Path', 'legalPrefix': 'legal prefix', 'wrongPrefix: 'wrong prefix' }],	[N]	[2], [3]
1.2	'legalAsPath' (data field)	legal AS-Path	textarea (text field)		[N]	[2], [3]
1.3	'wrongAsPath' (data field)	wrong AS-Path	textarea (text field)		[N]	[2], [3]
1.4	'lookingGlass' (data field)	reference link to Looking Glass used to verify AS-Path	textarea (text field)		[N]	[2], [3]
1.5	'legalPrefix' (data field)	legal prefix	textarea (text field)		[N]	[2], [3]
1.6	'wrongPrefix' (data field)	wrong prefix	textarea (text field)		[N]	[2], [3]

6.6.2. Computer attacks related to the use of malicious software for information infrastructure facilities of information exchange participants and their customers **[malware]** (for [INT], [EXT] vector)

Data block (field) number	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
2	'sourceId'	identifier	128-bit identifier	'malware': [{	[N]	[2], [3]

	(data field)	assigned by an information exchange participant	GUID) generated in accordance with Specification RFC4122 [16] assigned by an information exchange participant			
2.1	‘target’ (data block)	identifier of the attacked object			[N]	[2], [3]
2.1.1	'ip' (data field)	IP address	The logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
2.2	‘sources’ (data block)	identifiers of sources of malicious resources on the Internet with which the attacked object interacts	If it is necessary to specify several data field values (ip, domain, url), one or several objects in the data block ‘sources’ should be specified		[N]	[2], [3]
2.2.1	'ip' (data field)	IP address	The logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
2.2.2	'domain' (data field)	domain name	Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13]		[N]	[2], [3]
2.2.3	‘url’ (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
2.3	'classifications' (data block)	MC classification	If it is necessary to specify several data field values (vendorName, vendorVerdict), one or several objects in the data block 'classifications' should be specified		[N]	[2], [3]
2.3.1	'vendorName' (data field)	name of the MCSE tool used by an information exchange participant	textarea (text field)		[N]	[2], [3]


```
‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
‘target’: {
    ‘ip’: ‘127.0.0.1’
},
‘sources’: [{
    ‘ip’: ‘127.0.0.1’,
    ‘domain’: ‘example.com’,
    ‘url’:’http://example.com’
}],
‘classifications’: [{
    ‘vendorName’: 'name of the AMW tool',
    ‘vendorVerdict’: 'MC classification'
-
}],
‘malwareSamples’: [{
    ‘hash’: {
        ‘md5’: ‘4BA5139A444538479D9D750E2E2779BF’,
        ‘sha1’: ‘D2B063763378A8CB38B192B2F71E78BC13783EFE’,
        ‘sha256’: ‘E25059612A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A
E48FA441E44’
    },
    ‘attachment’: {
        ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
        ‘comment’: 'description of the attachment',
        ‘dateTimeAt’: ‘2018-03-22T08:14:38Z’,
        ‘file’: {
            ‘name’: 'file name',
            ‘size’: 'file size in bytes',
            ‘base64’: 'attachment in base64 format'
        },
```

				'fileLink': 'http://domain.com/archive.rar' } }], 'malwareMessageSenders': [{ 'email': 'qwer-ty@example.ru', 'server': '127.0.0.1' }], 'malwareMessageAttachment': { 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'comment': 'comment to the attachment', 'dateTimeAt': '2018-03-22T08:14:38Z', 'file': { 'name': 'file name', 'size': 'file size in bytes', 'base64': 'attachment in in base64 format' }, 'fileLink': 'http://domain.com/archive.rar' }, 'harmfulResourceAddress': [{ 'ip': '127.0.0.1', 'domain': 'example.com', 'url': 'http://example.com' }], 'iocs': [{ 'net': [{ 'impact': 'type of the detected compromising identifier', 'comment': 'additional description' }], 'fil': [{ 'impact': 'type of the detected		
2.3.2	'vendorVerdict' (data field)	MC class in accordance with the MCSE tool of an information exchange participant	textarea (text field)		[N]	[2], [3]
2.4	'malwareSamples' (data block)	it is required to specify MC samples that may be characterised by the hash function or an attachment	If it is necessary to specify several data field values (hash, attachment), one or several objects in the data block 'malwareSamples' should be specified		[N]	[2], [3]
2.4.1	'hash' (data subblock)	MC sample in the form of hash functions (MD5, SHA-1, SHA-256 function is calculated for each MC sample)			[N]	[2], [3]
2.4.1.1	'md5' (data field)	MC sample in the form of MD5 hash function	sequence of characters obtained as a result of MD5 hash function calculation		[N]	[2], [3]
2.4.1.2	'sha1' (data field)	MC sample in the form of the SHA-1 hash function	sequence of characters obtained as a result of the SHA-1 hash function calculation		[N]	[2], [3]
2.4.1.3	'sha256' (data field)	MC sample in the form of SHA- 256	sequence of characters obtained as a result of the SHA-256 hash function calculation		[N]	[2], [3]

				Compromising identifier', 'comment': 'additional description' }], 'reg': [{ 'impact': 'type of the detected compromising identifier', 'comment': 'additional description' }], 'prc': [{ 'impact': 'type of the detected compromising identifier', 'comment': 'additional description' }], 'oth': [{ 'impact': 'type of the detected compromising identifier', 'comment': 'additional description' }] }], 'infectionMethods': [{ 'type': 'type of the suggested infection method', 'comment': 'additional description' }] }],		
2.4.2	'attachment' (data subblock)	MC sample in the file form of a file			[N]	[2], [3]
2.4.2.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant		[N]	[2], [3]
2.4.2.2	'comment' (data field)	description of the attachment	text field (textarea)		[N]	[2], [3]
2.4.2.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
2.4.2.4.1	'file' (data subblock)	additional materials containing MC samples	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[N]	[2], [3]
2.4.2.5	'fileLink' (data field)	additional materials containing MC samples	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
2.5	'malwareMessageSenders' (data block)	identifiers of electronic mailboxes from which the letter with the attached MC was received	If it is necessary to specify several data field values (email, server), specify one or several objects in the data block 'malwareMessage'		[N]	[2], [3]
2.5.1	'email' (data field)	sender's e-mail address	The sender's e-mail address shall be submitted in the format in accordance with RFC 5322 specification [18]		[N]	[2], [3]
2.5.2	'server' (data field)	IP address of the last mail server	The logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]

2.6	"malwareMessage Attachment" (data subblock)	a file with the initial code of an electronic letter (if MC was sent to the e-mail box)			[N]	[2], [3]
2.6.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by the information exchange participant		[N]	[2], [3]
2.6.2	"comment" (data field)	attachment description	text field (textarea)		[N]	[2], [3]
2.6.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
2.6.4.1	"file" (data block)	data file containing a MC sample	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[N]	[2], [3]
2.6.4	'fileLink' (data field)	link for obtaining (downloading) a data file containing MC samples	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with RFC 3986 specification [15]		[N]	[2], [3]
2.7	"harmfulResource-Address" (data block)	identifiers of malicious resources from which a MC was loaded	If it is necessary to specify several data field values (ip, domain, url), specify one or several objects in the data block "harmfulResourceAddress"		[N]	[2], [3]
2.7.1	"ip" (data field)	IP address	Logical IPv4 address should comply with Specification RFC 791 [12]		[N]	[2], [3]

2.7.2	'domain' (data field)	domain name	Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13]		[N]	[2], [3]
2.7.3	'url' (data field)	URL-address	URL in accordance with RFC 3986 specification [15]		[N]	[2], [3]
2.8	'iocs' (data block)	identified compromise indicators	If it is necessary to specify several values of data fields (net, fil, reg, prc, oth), specify one or more objects in the 'iocs' data block		[N]	[2], [3]
2.8.1	'net' (data subblock)	network indicators	If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the 'net' data block		[N]	[2], [3]
2.8.1.1	'impact' (data field)	type of the compromising identifier detected	One code shall be selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion		[N]	[2], [3]
2.8.1.2	'comment' (data field)	additional description	textarea (text field)		[N]	[2], [3]
2.8.2	'fil' (data subblock)	file indicators	If it is necessary to specify several data field values (impact, comment), specify one or several objects in the 'fil' data block		[N]	[2], [3]
2.8.2.1	'impact' (data field)	type of the compromising identifier detected	One code shall be selected from the limited set of possible values:		[N]	[2], [3]

			• **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion			
2.8.2.2	'comment' (data field)	additional description	textarea (text field)		[N]	[2], [3]
2.8.3	'reg' (data subblock)	OS register indicators	If it is necessary to specify several data field values (impact, comment), specify one or several objects in the 'reg' data block		[N]	[2], [3]
2.8.3.1	'impact' (data field)	type of the compromising identifier detected	One code shall be selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion		[N]	[2], [3]
2.8.3.2	'comment' (data field)	additional description	textarea (text field)		[N]	[2], [3]
2.8.4	'prc' (data subblock)	indicators of OS processes	If it is necessary to specify several data field values (impact, comment), specify one or several objects in the 'prc' data block		[N]	[2], [3]
2.8.4.1	'impact' (data field)	type of the compromising identifier detected	One code shall be selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion		[N]	[2], [3]

2.8.4.2	‘comment’ (data field)	additional description	textarea (text field)		[N]	[2], [3]
2.8.5	'oth' (data subblock)	indicators not included in (2.8.1 – 2.8.4.2)	If it is necessary to specify several data field values (impact, comment), specify one or several objects in the ‘oth’ data block		[N]	[2], [3]
2.8.5.1	'impact' (data field)	type of the compromising identifier detected	One code shall be selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion		[N]	[2], [3]
2.8.5.2	‘comment’ (data field)	additional description	textarea (text field)		[N]	[2], [3]
2.9	'infectionMethods (data block)	identifiers of assumed infection methods	If it is necessary to specify several data field values (impact, comment), specify one or several objects in the 'infectionMethods' data block		[N]	[2], [3]
2.9.1	‘type’ (data field)	type of the suspected infection method	One code shall be selected from the limited set of possible values: • **[EML]** – via e-mails; • **[DSD]** – from a data storage device; • **[LCL]** – distribution via a local network; • **[OTH]** – other method		[N]	[2], [3]
2.9.2	'comment' (data field)	comment to the selected type	textarea (text field)		[N]	[2], [3]

6.6.3. Computer attacks that have been launched as a result of inducing clients to conduct money transfer transactions through deception or abuse of trust **[socialEngineering]** (for [EXT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

3	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	'socialEngineering': {
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'soiTypes': ('identifiers of social engineering methods']
				'soiSenders': [{
				'phoneNumber': '1212312345678',
				'email': 'qwerty@example.ru',
				'server': '127.0.0.1'
				}],
				'messageAttachment': {
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'comment': 'comment to the attachment',
				'dateTimeAt': '2018-03-22T08:14:38Z',
				'file': {
				'name': 'file name',
				'size': 'file size in bytes',
				'base64': 'attachment in base64 format'
				},
				'fileLink': 'http://domain.com/archive.rar '
				},
				'description': 'additional description'
				},
					[N]	[2], [3]

3.1	'soiTypes' (data field)	identifiers of social engineering methods	One or more codes should to be selected from the limited set of possible values: • **[MOB]** – a call from a mobile telephone; • **[TPH]** – a call from a telephone number starting with 8-800; • **[SMS]** – an SMS message; • **[SNW]** – social engineering using social networks; • **[MSG]** – social engineering using instant messaging tools; • **[OTH]** – other method of implementing social engineering methods		[N]	[2], [3]
3.2	'soiSenders' (data block)	social engineering implementation identifiers	If it is necessary to specify several data field values (phoneNumber, email, server), specify one or several objects in the data block 'soiSenders'		[N]	[2], [3]

3.2.1	'phoneNumber' (data field)	telephone number	in the **KKKXXXNNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number is to be provided without a plus sign (+), spaces (_) and separation signs (-).		[N]	[2], [3]
3.2.2	'email' (data field)	e-mail address	The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18]		[N]	[2], [3]
3.2.3	'server' (data field)	IP address of the last mail server	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
3.3	'message Attach-ment' (data block)	data files describing the social engineering method			[N]	[2], [3]
3.3.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant		[N]	[2], [3]
3.3.2	'comment' (data field)	description of the attachment	textarea (text field)		[N]	[2], [3]
3.3.3	'dateTimeAt'	date and time	data provision format		[N]	[2], [3]

	(data field)	when the file was added	in accordance with Specification RFC 3339 [11]			
3.3.4.1	'file' (data subblock)	data files describing the social engineering method	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[N]	[2], [3]
3.3.5	'fileLink' (data field)	data files describing the social engineering method	Specify URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
3.4	'description' (data field)	additional description	textarea (text field)		[N]	[2], [3]

6.6.4. Denial of service computer attacks (DDoS attacks) in relation to the information infrastructure of information exchange participants [ddosAttacks] (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

4	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	'ddosAttacks': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'target': {
				'ip': '127.0.0.1',
				'domain': 'example.com',
				'url': 'http://example.com',
				'assignment': 'purpose of the object under attack',
				'serviceType': 'information service type',
				'network': 'network address'
				},
				'attackType': {
				'type': 'attack type (by OSI levels)',
				'comment': 'additional description'
				-
					[N]	[2], [3]

4.1	'target' (data block)	attacked object identifiers			[N]	[2], [3]
4.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
4.1.2	'domain' (data field)	domain name	Domain name as per Specification RFC 1034 [14], as well as the international hierarchy of domain zones as per Specification RFC 5890 [13]		[N]	[2], [3]

					}, ‘sources’: [{ ‘ip’: ‘127.0.0.1’ }],		
4.1.3	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	per	‘power’: { ‘pps’: 'number of packets in	[N]	[2], [3]
4.1.4	'assignment' (data field)	purpose of the attacked object	purpose of the attacked object in the information infrastructure of an information exchange participant (server, data storage system, telecom, personal computer, firewall, etc.)	second', per second,' per second'	'mps'': 'number of megabits in 'rps'': 'number of requests in }, ‘startTimeAt’: ‘2018-03-22T08:14:38Z’, ‘endTimeAt’: ‘2018-03-22T09:15:44Z’, ‘negativeImpact’: { ‘type’: ‘- ‘comment’:	[N]	[2], [3]
4.1.5	'serviceTyp' (data field)	information service type	textarea			[N]	[2], [3]
4.1.6	'network' (data field)	network address	Logical IPv4 address in accordance with Specification RFC 791 [12] specifying the network mask (Subnet Mask) in accordance with Specification RFC 997 [17] [17]	’ selected type’	'comment to } }],	[N]	[2], [3]
4.2	'attackType' (data block)	attack type				[N]	[2], [3]
4.2.1	‘type’ (data field)	type of attack (by OSI levels)	One code shall be selected from the limited set of possible values: **[1]** – ‘L2/3: ICMP-flood’, **[2]** – ‘L2/3: NTP-amplification’, **[3]** – ‘L2/3: TFTP-amplification’, **[4]** – ‘L2/3: SENTINEL-			[N]	[2], [3]

			amplification', **[5]** – 'L2/3: DNS-amplification', **[6]** – 'L2/3: SNMP-amplification', **[7]** – 'L2/3: SSDP-amplification', **[8]** – 'L2/3: CHARGEN-amplification', **[9]** – 'L2/3: RIPv1-amplification', **[10]** – 'L2/3: BitTorrent-amplification', **[11]** – 'L2/3: QTPD-amplification', **[12]** – 'L2/3: Quake-amplification', **[13]** – 'L2/3: LDAP-amplification', **[14]** – 'L2/3: 49ad34-amplification', **[15]** – 'L2/3: Portmap-amplification', **[16]** – 'L2/3: Kad-amplification', **[17]** – 'L2/3: NetBIOS-amplification', **[18]** – 'L2/3: Steam-amplification', **[19]** – 'L3: DPI-attack', **[20]** – 'L4: LAND-attack', **[21]** – 'L4: TCP-SYN- attack', **[22]** – 'L4: TCP-ACK-		

			attack', **[23]** – 'L4: Smurf-attack', **[24]** – 'L4: ICMP/UDP-frag', **[25]** – 'L4: TCP-frag', **[26]** – 'L6: SSL-attack', **[27]** – 'L7: DNS Water Tor- ture Attack', **[28]** – 'L7: Wordpress Pingback DDoS', **[29]** – 'L7: DNS-flood', **[30]** – 'L7: HTTP/S-flood', **[31]** – 'L7: FTP-flood', **[32]** – 'L7: SMTP-flood', **[33]** – 'L7: VoIP/SIP-attack', **[34]** – 'L7: POP3-flood', **[35]** – 'L7: SlowRate- attack,' **[36]** – 'other'			
4.2.2	'comment' (data field)	additional description	textarea (text field)		[N]	[2], [3]
4.3	'sources' (data block)	identification of attack sources	If it is necessary to specify several values of the data field (ip), specify one or several objects in the data block 'sources'		[N]	[2], [3]
4.3.1	'ip' (data field)	IP address of the attack source (in case of a large number of computer attack sources in the block	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]

		- specify the top 100 IP addresses of the attackers, with the complete list attached in a text file)				
4.4	'power' (data block)	attack power			[N]	[2], [3]
4.4.1	'pps' (data field)	number of packets per second	Packets per second		[N]	[2], [3]
4.4.2	'mps' (data field)	number of megabits per second	Megabits per second		[N]	[2], [3]
4.4.3	'rps' (data field)	number of requests per second	Requests per second		[N]	[2], [3]
4.5	'startTimeAt' (data field)	attack start time	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
4.6	'end time' (data field)	attack end time	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
4.7	'negativeImpact' (data block)	attack negative impact -			[N]	[2], [3]
4.7.1.	'type' (data field)	negative impact type	One code shall be selected from the limited set of possible values: • **[NAW]** – service availability interruption; • **[OTH]** – service degradation;		[N]	[2], [3]

			• **[NCQ]** – service was not adversely affected			
4.7.2.	‘comment’ (data field)	additional description	textarea (text field)		[N]	[2], [3]

6.6.5. Computer attacks related to unauthorised access to ATMs and payment terminals of information exchange participants **[atmAttacks]** (for vector [INT])

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
5	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	‘atmAttacks’: { ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,	[N]	[2], [3]
5.1	‘target’ (data block)	identifier of the attacked object		‘target’: { ‘type’: 'attacked object type','description': 'additional description' },	[N]	[2], [3]
5.1.1	‘type’ (data field)	attacked object type	One code shall be selected from the limited set of possible values: • **[ATM]** is an ATM; • **[CIN]** is an ATM capable to accept funds; • **[REC]** is an ATM with a recycling function; • **[POS]** is a POS terminal; • **[SST]** is a payment terminal; • **[OTH]** is other facility	‘attackType’: [{ ‘type’: attack type depending on the target ‘description’: 'additional description' }], ‘attackImage’: { ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘comment’: 'comment to the attachment', ‘dateTimeAt’: ‘2018-03-22T08:14:38Z’, ‘file’: { ‘name’: 'file name', 'size': 'file size in bytes', ‘base64’: 'attachment in base64 format' },	[N]	[2], [3]
5.1.2	‘description’ (data field)	additional description	textarea (text field)		[N]	[2], [3]

5.2	'attackType' (data block)	attack type	If it is necessary to specify several values of data fields (type, description), specify one or several objects in the data block 'sources'	'fileLink': 'http://domain.com/archive.rar ' } },	[N]	[2], [3]
5.2.1	'type' (data field)	type of attack depending on the target	One code shall be selected from the limited set of possible values: • **[BBX]** – blackbox attacks; • **[DSP]** – direct dispense attacks and their variations; • **[SKM]** – skimming; • **[OTH]** – other method		[N]	[2], [3]
5.2.2	'description' (data field)	additional description	textarea (text field)		[N]	[2], [3]
5.3	'attackImage' (data block)	additional materials of attack events			[N]	[2], [3]
5.3.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant		[N]	[2], [3]
5.3.2	'comment' (data field)	description of the attachment	textarea (text field)		[N]	[2], [3]
5.3.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
5.3.4.1	'file' (data subblock)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[N]	[2], [3]

5.3.5	'fileLink' (data field)	reference link for obtaining (downloading) a data file containing additional materials	Specify the URL-address for downloading a file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]		[N]	[2], [3]

6.6.6. Computer attacks related to exploiting information infrastructure vulnerabilities of information exchange participants and their clients **[vulnerabilities]** (for vector [INT], [EXT])

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

6	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	'vulnerabilities': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'target': {
				'ip': '127.0.0.1',
				'domain': 'example.com', 'url': 'http://example.com',
				'serviceType': 'information service type',
				},
				'sources': [{
				'ip': '127.0.0.1',
				'url': 'http://example.com'
				}],
				'identifier': 'vulnerability identifier',
				'cvss': 'CVSS metrics',
				'idCustom': {
				'description': 'vulnerability description',
				'swName': 'software name'.
				программного обеспечения',
				'swVer': 'software version',
				'cweType': 'CWE error type',
					[N]	[2], [3]

6.1	'target' (data block)	attacked object identifiers			[N]	[2], [3]
6.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
6.1.2	'domain' (data field)	domain name	Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13]		[N]	[2], [3]
6.1.3	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]

6.1.4	'serviceType' (data field)	type of information service	textarea (text field)	'class': 'vulnerability class', 'osName': 'operating system that controls software with detected vulnerabilities', 'detectedAt': date and time of vulnerability detection', 'baseCVSS': 'baseline vector of vulnerability', 'danger': 'severity level of detected vulnerability', 'measures': 'potential measures to eliminate vulnerability', 'status': 'vulnerability status', 'exploit': 'exploit availability', 'recommendation': 'information on vulnerability elimination', 'link': 'links to sources of information on the elimination of vulnerability', 'manufacturer': 'a company (organisation) that manufactures (develops) software in which vulnerabilities have been detected' } }],	[N]	[2], [3]
6.2	'sources' (data block)	identifiers of sources from which vulnerability was detected	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block 'sources'		[N]	[2], [3]
6.2.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
6.2.2	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
6.3	'identifier' (data field)	vulnerability identifier	If a vulnerability is detected, its type is to be specified in accordance with the classification of the FSTEC of Russia, CVE: • FSTEC of Russia - https://bdu.fstec.ru/vul; • Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org/data/downloads/allitems.html		[N]	[2], [3]
6.4	'cvss' (data field)	CVSS metrics	Specify CVSS v 3.0 Metrics (the Common Vulnerability Scoring System (CVSS) if * is defined. Specify the maximum possible number of metrics listed as follows: basic metrics, temporary metrics, context metrics, and environment metrics. (* If no metrics are defined,		[N]	[2], [3]

			use the FSTEC of Russia calculator -– https://bdu.fstec.ru/cvss3)			
6.5	'idCustom' (data block)	generating a vulnerability identifier			[N]	[2], [3]
6.5.1	‘description’ (data field)	vulnerability description	textarea (text field)		[N]	[2], [3]
6.5.2	'swName' (data field)	software name	textarea (text field)		[N]	[2], [3]
6.5.3	'swVer' (data field)	software version	textarea (text field)		[N]	[2], [3]
6.5.4	'sweType' (data field)	type of error established in accordance with the general list of CWE errors	in accordance with Common Weakness Enumeration (CWE) (https://cwe.mitre.org/)		[N]	[2], [3]
6.5.5	'class' (data field)	vulnerability class	One code shall be selected from the limited set of possible values: • **[COD]** – code vulnerability - a vulnerability resulting from software development, excluding data security requirements; • **[ARH]** – architecture vulnerability - a vulnerability resulting from the choice and composition of software components containing vulnerabilities;		[N]	[2], [3]

			• **[MULT]** – multiple-factor vulnerability (caused by various classes of vulnerabilities in the software)			
6.5.6	'osName' (data field)	an operating system that controls software with detected vulnerabilities	Textarea (text field)		[N]	[2], [3]
6.5.7	'dateTimeAt' (data field)	date and time when vulnerability was detected	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
6.5.8	'baseCVSS' (data field)	baseline vulnerability vector	in accordance with CVSS 3.0 (https://bdu.fstec.ru/cvss3		[N]	[2], [3]
6.5.9	'danger' (data field)	severity level of identified vulnerability	One code is to be selected from the limited set of possible values in accordance with the results of the baseline vulnerability vector: • **[LL]** – low level, if 0.0 < = V < = 3.9; • **[ML]** – mean level, if 4.0 < = V < = 6.9; • **[HL]** – high level, if 7.0 < = V < = 9.9; • **[CL]** – critical level, if V = 10.0		[N]	[2], [3]
6.5.10	'measures' (data field)	possible measures to	textarea (text field)		[N]	[2], [3]

		eliminate vulnerability				
6.5.11	'status' (data field)	vulnerability status	One code shall be selected from the limited set of possible values: • **[APR_M]** – 'confirmed by the manufacturer' – if a vulnerability was confirmed by the manufacturer (developer) of software containing a vulnerability; • **[APR_M]** – 'confirmed in the course of research' - if a vulnerability was detected and confirmed by a researcher (organisation) who is not the software manufacturer (developer); • **[Potential]** – 'potential vulnerability' – in all other cases		[N]	[2], [3]
6.5.12	'exploit' (data field)	existence of exploit	Textarea (text field)		[N]	[2], [3]
6.5.13	'recommendation' (data field)	information on the elimination of vulnerability	Textarea (text field)		[N]	[2], [3]
6.5.14	'link' (data field)	reference links to sources of information on the elimination of vulnerability	Textarea (text field)		[N]	[2], [3]
6.5.15	'manufacturer' (data field)	a company (organisation) that is the manufacturer (developer	Textarea (text field)		[N]	[2], [3]

		of software in which a vulnerability has been detected				

6.6.7. Computer attacks related to searching (hacking) and compromising authentication data (login) data **[bruteForces]** (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

7	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	'bruteForces': [{
				'sourceId': 'f34030ef-358a-445c-8567-
				25985ce6d91c',
				'target': {
				'ip': '127.0.0.1',
				'url': 'http://example.com',
				'serviceType': 'service type'
				},
				'sources': [{
				'ip': '127.0.0.1'
				}],
				'accountOs': {
				'name': 'account name',
				'privileges': 'account (privilege) level'
				}
				}],
					[N]	[2], [3]

7.1	'target' (data block)	attacked object attacked object			[N]	[2], [3]
7.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
7.1.2	'domain' (data field)	domain name	Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13]		[N]	[2], [3]
7.1.3	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
7.1.4	'serviceTyp' (data field)	type of information service	Textarea (text field)		[N]	[2], [3]
7.2	'sources' (data block)	identifiers of attack source	If it is necessary to specify several values of the data field (ip), specify one or several objects in the data block 'sources'		[N]	[2], [3]

7.2.1	'ip' (data field)	IP address of the source of attack (in the case of a large number of computer attack sources, the sources data block shall contain the top 100 IP addresses of the attackers with the complete list attached in a text file) -	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
7.3	'accountOs' (data block)	compromised account identiriers			[N]	[2], [3]
7.3.1	‘name’ (data field)	account name	Textarea (text field)		[N]	[2], [3]
7.3.2	'privileges' (data field)	account level (privileges)	Textarea (text field)		[N]	[2], [3]

6.6.8. Computer attacks related to spam mailings to information exchange participants and their clients **[spams]** (for [INT], [EXT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

8	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	'spams': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'receivedAt': '2018-03 22T08:14:38Z',
				'targets': [{
				'email': 'qwerty@example.ru'
				}],
				'sources': [{
				'ip': '127.0.0.1',
				'domain': 'example.com',
				'email': 'qwerty@example.ru'
				}],
				'spamImages': {
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'comment': 'attachment description',
				'dateTimeAt': '2018-03-22T08:14:38Z ',
				'file': {
				'name': 'file name',
				'size': 'file size in bytes',
				'base64': 'attachment in in base64 format'
				},
				'fileLink': 'http://domain.com/archive.rar'
				}
				}],
					[N]	[2], [3]

8.1	'receivedAt' (data field)	date and time when a spam message is received	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
8.2	'target' (data block)	attacked object identifiers (recipients of spam messages)	If it is necessary to specify several values of the data field (email), specify one or several objects in the 'targets' data block		[N]	[2], [3]
8.2.1	'email' (data field)	spam message recipient's email address	The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18]		[N]	[2], [3]
8.3	'sources' (data block)	attack source identifiers (spam sender)	If it is necessary to specify several data field values (ip, domain, email), specify one or several objects in the data block 'sources'		[N]	[2], [3]
8.3.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]

8.3.2	'domain' (data field)	domain name	Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13]		[N]	[2], [3]
8.3.3	‘email’ (data field)	spam message sender's e-mail address	The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18]		[N]	[2], [3]
8.4	‘spamImage’ (data block)	spam message example			[N]	[2], [3]
8.4.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant		[N]	[2], [3]
8.4.2	‘comment’ (data field)	description of the attachment	Textarea (text field)		[N]	[2], [3]
8.4.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
8.4.4.1	'file' (data block)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[N]	[2], [3]
8.4.5	'fileLink' (data field)	reference link for obtaining (downloading) a data file containing additional materials	Specify the URL-address for downloading a file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]		[N]	[2], [3]

6.6.9. Computer attacks related to detecting an interaction of information infrastructure facilities of information exchange participants with Botnet command centres **[controlCenters]** (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

9	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant	‘controlCenters’: [{
				‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
				‘target’: {
				‘ip’: ‘127.0.0.1’,
				‘url’: ‘http://example.com’
				},
				‘hostUrl’: ‘http://example.com’,
				‘intruderIp’: ‘1.1.1.1’,
				‘intruderActions’: 'what preceded the incident',
				‘description’: 'known information about the Botnet Command Centre',
				‘nodes’: [{
				‘ip’: ‘127.0.0.1’,
				‘lastRequestRateTimeAt’: ‘2018-03-22T08:08:49Z’
				}]
				}],
					[N]	[2], [3]

9.1	‘target’ (data block)	attacked object identifiers			[N]	[2], [3]
9.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
9.1.2	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
9.2	'hostUrl' (data field)	URL hosting the Botnet Command Centre	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
9.3	'intruderIp' (data field)	IP address of the attacker who hosted the Botnet Command Centre	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
9.4	'intruderActions' (data field)	description of unauthorised activity in the information infrastructure of an information	Textarea (text field)		[N]	[2], [3]

		exchange participant				
9.5	‘description’ (data field)	additional description of the Botnet command centre	Textarea (text field)		[N]	[2], [3]
9.6	'nodes' (data block)	identifiers of appeals to the Botnet command centre	If it is necessary to specify several data field values (ip, lastRequestRateTimeAt), specify one or several objects in the data block		[N]	[2], [3]
9.6.1	'ip' (data field)	external IP address (information exchange participant)	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
9.6.2	'lastRequest RatetimeAt' (data field)	date and time of the last interaction with the Botnet command centre	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]

6.6.10. Computer attacks related to the change (substitution) of the mobile subscriber identifier (IMSI) of the SIM card number, as well as the replacement of the mobile equipment identifier (IMEI) **[sim]** (for [EXT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
10	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	‘sim’: { ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘mobileOperator’: 'mobile operator name' ‘phoneNumber’: ‘1212312345678’, ‘imsi’: ‘123456789000000’, ‘imsiChangedAt’: ‘2018-03-	[N]	[2], [3]
10.1	‘mobileOperator’	name of a	Textarea (text field)		[N]	[2], [3]

	(data field)	mobile operator		22T08:08:49Z' },		
10.2	'phoneNumber' (data field)	mobile phone number	in the **KKKXXXNNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; NNNNNNN – seven characters of the number. The telephone number is to be provided without a plus sign (+), spaces (_) and separation signs (-).		[N]	[2], [3]
10.3	'imsi' (data field)	unique SIM card number (IMSI number)	in the **XXXXXXXXXXXXXXX** format		[N]	[2], [3]
10.4	'imsiChangedAt' (data field)	date and time when the IMSI change was recorded	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]

6.6.11. Computer attacks related to information that misleads information exchange participants and their clients, as well as other persons interacting with them, about the ownership of the information disseminated via the Internet due to the similarity of domain names, design or content. Phishing [phishingAttacks] (for [EXT], [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

11	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange	'phishingAttacks': [{
				'sourceId': 'f34030ef-358a-445c-8567-
				25985ce6d91c',
				'target': {
				'ip': '127.0.0.1',
				'domain': 'example.com'
					[N]	[2], [3]

			participant		},		
11.1	‘target’ (data block)	identifier of the attacked object (legitimate resourse)			‘harmful’: [{ ‘ip’: ‘127.0.0.1’, ‘url’: ‘http://example.com’ }],	[N]	[2], [3]
11.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		‘fixationAt’: ‘2018-03-22T08:08:49Z ‘, ‘messageAttachment’: { ‘sourceId’: ‘f34030ef-358a-	[N]	[2], [3]
11.1.2	'domain' (data field)	domain name	Domain name according to Specification RFC 1034 [14], as well as the international hierarchy of domain zones according to Specification RFC 5890 [13]	445c-8567-25985ce6d91c’, 22T08:08:49Z’, ‘http://domain.com/archive.rar’ }],	‘comment’: ‘attachment description’ dateTimeAt’: ‘2018-03- ‘file’: { ‘name’: 'file name', 'size': 'file size in bytes’ ‘base64’: 'attachment in base64 format’ },	[N]	[2], [3]
11.2	‘harmful’ (data block)	phishing resource source identifiers	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block ‘harmful’		‘fileLink’: }	[N]	[2], [3]
11.2.1	‘ip’ (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]			[N]	[2], [3]
11.2.2	‘url’ (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]			[N]	[2], [3]
11.3	‘fixationAt’ (data field)	date and time of phishing message recording	data presentation format in accordance with RFC 3339 [11]			[N]	[2], [3]
11.4	‘message Attachment’ (data block)	phishing message sample				[N]	[2], [3]
11.4.1	‘sourceId’ (data field)	identifier assigned by an information	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by			[N]	[2], [3]

		exchange participant	an information exchange participant			
11.4.2	‘comment’ (data field)	description of the attachment	Textarea (text field)		[N]	[2], [3]
11.4.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
11.4.4.1	'file' (data block)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform encoding in Base64 formate		[N]	[2], [3]
11.4.5	'fileLink' (data field)	reference link for obtaining (downloading) a data file containing additional materials	Specify the URL-address for downloading a file, if its size exceeds 5 MB, in accordance with RFC Specification 3986 [15]		[N]	[2], [3]

6.6.12. Computer attacks related to the distribution of information related to offers and/or provision of financial services in the Russian Federation by persons not entitled to provide them in accordance with the legislation of the Russian Federation. Posting prohibited content on the Internet **[prohibitedContents]**(for [EXT], [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

12	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	‘prohibitedContents’: [{
				‘sourceId’: ‘f34030ef-358a-445c-8567-
				25985ce6d91c’,
				‘sources’: [{
				‘ip’: ‘127.0.0.1’,
				‘url’: ‘http://example.com’
				}],
				‘type’: 'prohibited content type'
				}],
					[N]	[2], [3]

12.1	'sources' (data block)	identifiers of prohibited content sources	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the ‘target’ data block		[N]	[2], [3]

12.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
12.1.2	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
12.2	‘type’ (data field)	prohibited content type	textarea (text field)		[N]	[2], [3]

6.6.13. Computer attacks related to posting on the Internet information enabling illegal access to information systems of information exchange participants and their customers used for providing (receiving) financial services, including through illegal access to confidential customer information. Posting a malicious resource on the Internet **[maliciousResources]** (for [EXT], [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Mandatory provision of information	Information provision stages
13	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	‘maliciousResources’: [{ ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘sources’: [{ ‘ip’: ‘127.0.0.1’, ‘url’: ‘http://example.com’ }], ‘activityType’: 'description of malicious activity' }],	[N]	[2], [3]
13.1	‘sources’ (data block)	identifiers of malicious resource sources	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the ‘target’ data block		[N]	[2], [3]
13.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
13.1.2	‘url’	URL-address	URL in accordance with		[N]	[2], [3]

	(data field)		Specification RFC 3986 [15]			
13.2	'activityType' (data field)	type of malicious activity	textarea (text field)		[N]	[2], [3]

6.6.14. Computer attacks related to changes in content **[changeContent]** (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

14	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant	'changeContent': [{
				'sourceId': 'f34030ef-358a-445c-8567-
				25985ce6d91c',
				'targets': [{
				'ip': '127.0.0.1',
				'url': 'http://example.com'
				}],
				'type': 'type of content'
				}],
					[N]	[2], [3]

14.1	'targets' (data block)	identifiers of attacked objects which content was modified	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the 'target' data block		[N]	[2], [3]
14.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
14.1.2	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
14.2	'type' (data field)	type of modified content	textarea (text field)		[N]	[2], [3]

6.6.15. Computer attacks related to the scanning of software ports of information infrastructure facilities of information exchange participants by persons not authorised to do so **[scanPorts]** (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
15	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	‘scanPorts’: [{ ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘sources’: [{ ‘ip’: 'IP address' }], ‘ports’: [‘21’], ‘method’: 'information on scanning methods or software used for this purpose', ‘startTimeAt’: ‘2018-03-22T08:08:49Z’, ‘endTimeAt’: ‘2018-03-22T08:09:49Z’ }],	[N]	[2], [3]
15.2	‘sources’ (data block)	malicious activity source identifiers	If it is necessary to specify several values of the data field (email), specify one or several objects in the ‘sources’ data block		[N]	[2], [3]
15.2.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
15.3	'ports' (data field)	port numbers that have been scanned	textarea (text field)		[N]	[2], [3]
15.4	'method' (data field)	information on scanning methods or software used for this purpose	textarea (text field)		[N]	[2], [3]
15.5	'startTimeAt' (data field)	scanning start time	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]

15.6	'end time' (data field)	scanning end time	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]

6.6.16. Other computer attacks against information infrastructure facilities of information exchange participants and their clients **[other]** (for [INT], [EXT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
16	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	‘other’: { ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘description’: 'computer attack description', ‘source’: { ‘ip’: ‘127.0.0.1’, ‘url’: ‘http://example.com’ }, ‘type’: 'other type of prohibited, malicious, altered content', ‘attachment’: { ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘comment’: 'attachment description', ‘dateTimeAt’: ‘2018-03-22T08:08:49Z ‘, ‘file’: { ‘name’: 'file name', 'size': 'file size in bytes', ‘base64’: 'attachment in in base64 format' }, ‘fileLink’: ‘ http://domain.com/archive.rar’ } } },	[N]	[2], [3]
16.1	‘description’ (data field)	computer attack attacked object	textarea (text field)		[N]	[2], [3]
16.2	‘source’ (data block)	identifiers of another source of malicious, prohibited content/ resource			[N]	[2], [3]
16.2.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]		[N]	[2], [3]
16.2.2	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]		[N]	[2], [3]
16.2.3	‘type’ (data field)	other type of prohibited, malicious, modified content	textarea (text field)		[N]	[2], [3]

16.3	'attachment' (data block)	additional data to identify a computer attack			[N]	[2], [3]
16.3.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant		[N]	[2], [3]
16.3.2	'comment' (data field)	attachment description	textarea (text field)		[N]	[2], [3]
16.3.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[2], [3]
16.3.4	'file' (data block)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform encoding in Base64 format		[N]	[2], [3]
16.3.5	'fileLink' (data field)	reference link for obtaining (downloading) a data file containing additional materials	it is required to specify URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]		[N]	[2], [3]

6.7. Information on the results of the completion of an incident and relevant forms of electronic messages

6.7.1. Organisational information **[finalReport]**

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
1.1	'closeDateAt' (data field)	date and time of incident closure	data provision format in accordance with Specification RFC 3339 [11]	'finalReport': { 'closeDateAt': 'date and time of incident closure' 'recovery': 'identifier of recovery after the occurrence of the incident', 'description': 'additional description if recovery is impossible', 'rootCause': 'key causes of the incident', 'mainActions': 'actions taken to prevent incidents in the future',	[O]	[3]
1.2	'recovery' (data field)	identifier of recovery after incident occurrence	One code shall be selected from the limited set of possible values: • **[Full]** – provision of financial (banking) services is fully restored; • **[Not _ Full]** – provision of financial (banking) services is partially restored		[O]	[3]
1.3	'description' (data field)	additional description if recovery is impossible	textarea (text field)		[O]	[3]
1.4	'rootCause' (data field)	key causes of the incident	textarea (text field)		[O]	[3]
1.5	'mainActions' (data field)	actions taken to prevent future incidents	textarea (text field)		[O]	[3]

6.7.2. Technical information describing the signature of computer attacks **[signatures]**

Data block (field) No.	Data block (field) identifier	Content of data block (field)	Data field format	E-mail format	Mandatory provision of information	Information provision stages
2.1	‘signatures’ (data block)	signature	If it is necessary to specify several data field values (identifier, name, source, eventsAmount), specify one or several objects in the data block ‘signatures’	‘signatures’: [{ ‘identifier’: ‘signature identifier’ - ‘name’: ‘detection tool’, ‘source’: ‘signature source’, ‘eventsAmount’: ‘number of signature responses’ }], ‘snort’: [‘rule1’,’rule2’], ‘attachment’: { ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘comment’: 'description of the attachment', 'dateTimeAt': ‘2018-03-22T08:14:38Z’, ‘file’: { ‘name’: 'file name', ‘size’: 'file size in bytes', ‘base64’: ‘attachment in base64 format’ }, ‘fileLink’: ‘http://domain.com/archive.rar’ } } } }	[N]	[3]
2.2	'identifier' (data field)	unique identifier of the signature	sequence of symbols obtained as a result of MD5 hash function calculation		[N]	[3]
2.3	‘name’ (data field)	detection tool	textarea (text field)		[N]	[3]
2.4	‘source’ (data field)	source of signature receipt	textarea (text field)		[N]	[3]
2.5	‘eventsAmount’ (data field)	number of signature responses	textarea (text field)		[N]	[3]
2.6	‘snort’ (data field)	Snort-rules	submission format in the form of: <Action> <Protocol> <Sender IP addresses> <Sender ports> <Destination operator> <Recipient IP addresses> <Recipient ports> (key_1: value_1; key_2: value_2;.. key_n: value_n;)		[N]	[3]

2.7	'attachment' (data block)	additional data upon completion of an incident			[N]	[3]
2.7.1	‘sourceId’ (data field)	identifier assigned by an informatio n exchange participant	128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant		[N]	[3]
2.7.2	'comment' (data field)	attachment description	textarea (text field)		[N]	[3]
2.7.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339[11]		[N]	[3]
2.7.4	'file' (data block)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[N]	[3]
2.7.5	'fileLink' (data field)	link for obtaining (downloadi ng) a data file containing additional materials	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with the RFC 3986 specification [15]		[N]	[3]

7. The form of the Bank of Russia's request to an information exchange participant servicing the payee

If the Bank of Russia receives information in accordance with Chapter 6 of Section 6.5 hereof from an information exchange participant serving the payer in order to verify a particular payee, it shall send a request to the information exchange participant servicing the payee, as well as a notice of the suspension of the crediting of funds to the payee's bank account or an increase in the balance of the payee's electronic funds.

7.1. Identification data of the Bank of Russia's request. Data block **[HEADER]**

Data block (field) No.	Data block (field) identifier	Data block (field) content	Data field format	E-mail format
1.1	'schemaType' (data field)	type of electronic message	Specify the value **[antifraudRequest]** - an additional request to an information exchange participant - 'the payee' in an unauthorised transaction	{ 'header': { 'schemaType': 'antifraudRequest', 'schemaVersion': '1', 'version': '1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'publishedAt': '2002-10-02T15:00:00.05Z' },
1.2	'schemaVersion' (data field)	electronic message type scheme	textarea (text field)	
1.3	'version' (data field)	electronic message version number during information exchange	numeric value (int)	
1.4	'memberId' (data field)	identifier of an information exchange participant assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia	
1.5	'publishedAt' (data field)	date and time of initial provision of information	data submission format in accordance with Specification RFC 3339 [11]	

7.2. Description of the Bank of Russia's request form. Data block **[antifraudRequest]**

The form of Bank of Russia's request to the information exchange participant servicing the payee shall apply:

when requesting from the money transfer operator serving the payee, including the electronic funds operator, information identifying the payee [4];

when sending a notification of the suspension of funds crediting to the payee's bank account or an increase in the balance of the payee's electronic funds [20].

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format

1	‘antifraudRequest (data block)		If it is necessary to specify several values of data blocks (payer, payee), specify one or several objects in the data block ‘antifraudRequest’	‘antifraudRequest’: [{
				‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
				‘victim’: ‘information on the subject status of the payer’,
				‘payer’: {
				‘bik’: ‘123456789’,
				‘inn’: ‘123456789000’,
				‘namePayer’: ‘name of the organisation that is the payer’,
				‘payerTransferId’: {
				‘transferType’: ‘type of funds transfer method’,
				‘paymentCard’: {
				‘number’: ‘123412341234123412’,
				‘sum’: ‘the amount of a payment card money transfer transaction’,
				‘currency’: ‘currency of a money transfer transaction’,
				‘dateTimeAt’: ‘2018-01-13T09:14:38Z’,
				‘rrn’: ‘the number generated for a money transfer transaction during its authorisation’
				},
				‘settlement’: {
				‘number’: ‘12345123451234512345’,
				‘sum’: ‘money transfer amount’
				-
				‘currency’: ‘currency of a money transfer transaction’
				-
				‘dateTimeAt’: ‘2018-01-13T09:14:38Z’
				},
				‘phoneNumber’: {
				‘number’: ‘1212312345678’,

1.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant who is the payer	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant	
1.2	'victim' (data field)	information on the legal status of the payer	One code is selected from the limited set of possible values: • **[person]** – an individual; • **[entity]** – a legal entity	
1.2	‘payer’ (data block)	information identifying the payer		
1.2.1	'bik' (data field)	BIC of the money transfer operator serving the payer	in the **AAAAAAAAA** format	
1.2.2	'inn' (data field)	TIN of the payer - a legal entity, and/or an individual entrepreneur, and/or a person engaged in private business	in the **XXXXXXXXXX** format – for legal entities, in **XXXXXXXXXX** or **XXXXXXXXX** formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation	

1.2.3	'payerName' (data field)	organisation name that is the payer	textarea	
1.2.4	'payerTransferId' (data subblock)	identification data depending on the money transfer method		
	'transferType' (data field)	type of money transfer method	One code is selected from the limited set of possible values: • **[paymentCard]** – when transferring funds using payment cards; • **[settlement]** – when transferring funds to bank accounts; • **[phoneNumber]** – when transferring funds by telephone number; • **[idNumber]** – if the balance of electronic funds changes	
1.2.4.1	'paymentCard' (data subblock)	when transferring funds using payment cards		
1.2.4.1.1	'number' (data field)	number of the payer's payment card issued to him/her and (or) the person authorised by the payer and the money transfer operator by the issuer	in the **XXXXXXXXXXXXXXXXXX** format payment card number shall be provided without spaces (_) and separation marks (-).	
1.2.4.1.2	'sum' (data field)	amount of money transferred using payment cards	transaction amount - field 'F004' of ISO 8583 Financial Messages Standard [7], [8], [9]	

```
                    'sum': 'transaction amount',
                    'currency': 'transaction currency',
                    'dateTimeAt': '2018-01-13T09:14:38Z'
                },
                'idNumber': {
                    'number': '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT',
                    'sum': 'transaction amount',
                    'currency': 'transaction currency',
                    'dateTimeAt': '2018-01-13T09:14:38Z'
                }
            },
            'device': {
                'ip': '127.0.0.1',
                'imsi': 'international mobile subscriber identifier (individual subscriber number)',
                'imei': 'international mobile equipment identifier',
                'aiic': 'Acquiring institution identification code (32 field ISO 8583)',
                'cati': 'Card acceptor terminal identification (41 field ISO 8583)',
                'caic': 'Card acceptor identification code (42 field ISO 8583)'
            }
        },
        'payee': {
            'bik': '123456789',
            'inn': '123456789000',
            'payeeName': 'name of the organisation that is the payee',
            'payeeTransferId': {
                'transferType': 'type of funds transfer method',
                'paymentCard': {
                    'number': '123412341234123412'
                },
                'settlement': {
                    'number': '12345123451234512345'
                },
                'phoneNumber': {
```

				'number': '1212312345678'
				},
				'idNumber': {
				'number':
				'1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT'
				}
				}
				}
				}]
				}

1.2.4.1.3	'currency' (data field)	currency of a money transfer transaction	transaction currency - field 'F049' of ISO 8583 Financial Messaging Standard [7], [8], [9]	
1.2.4.1.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339[11]	
1.2.4.1.5	'rrn' (data field)	number generated for a money transfer transaction during its authorisation	number generated for a money transfer transaction during its authorisation - field 'F037' < * > of ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of field 'F037' (Retrieval Reference Number) shall be generated by the acquiring bank host according to the following rule: **YJJJXXNNNNNN**, where: **Y** is the last figure of a year; **JJJ** is a Julian date; **XX** is the identifier assigned to the acquiring bank host by the operator; **NNNNNN** is the transaction sequence number during a day	
1.2.4.2	'settlement' (d subblock)	when transferring funds in bank accounts by debiting money from payers' bank accounts		
1.2.4.2.1	'number' (data field)	the number of the payer's bank account opened with the money transfer operator serving the payer	in the **XXXXXXXXXXXXXXXXXXXX** format bank account number shall be provided without spaces (_) and	

			separation marks (-).	
1.2.4.2.2	‘sum’ (data field)	amount of a fund transfer transaction	textarea (text field)	
1.2.4.2.3	‘currency’ (data field)	currency of funds transfer transaction	textarea (text field)	
1.2.4.2.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339[11]	
1.2.4.3	'phoneNumber' (data subblock)	when making money transfers by telephone number		
1.2.4.3.1	'number' (data field)	the payer's telephone number specified in a bank account agreement and/or a agreement on the use of electronic payment instruments concluded with the payer	in the **KKKXXXNNNNNNNN** format, where: **KKK** – from one to three characters of the country code; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-).	
1.2.4.3.2	‘sum’ (data field)	transaction amount	textarea (text field)	
1.2.4.3.3	‘currency’ (data field)	transaction currency	textarea (text field)	
1.2.4.3.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339[11]	
1.2.4.4	‘idNumber’ (data subblock)	if the balance of electronic funds changes		
1.2.4.4.1	'number' (data field)	the payer's identification number, in particular, the number of the payer's electronic wallet used by him/her on the basis of a bank account agreement	textarea (text field)	

		and (or) an agreement on the use of the electronic payment instruments concluded with the money transfer operator		
1.2.4.4.2	‘sum’ (data field)	transaction amount	textarea (text field)	
1.2.4.4.3	'currency' (data field)	transaction currency	textarea (text field)	
1.2.4.4.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]	
1.2.5	'device' (data subblock)	parameters of the device used to access an automated system and software for the purpose of money transfer without the customer's consent		
1.2.5.1	'ip' (data field)	network address of a computer and/or a communication device (router) (IP)	The IPv4 network address shall comply with RFC 791 specification [12]	
1.2.5.2	'imsi' (data field)	International Mobile Subscriber Identity (IMSI) means the international identifier of a mobile subscriber (individual number of a subscriber (an individual customer) by which the system recognises a mobile communication user using GSM and UMTS standards	number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**	
1.2.5.3	‘imei’ (data field)	International Mobile Equipment Identity (IMEI)	number (15-bit in decimal)	

		international identifier of mobile equipment (mobile device of an individual customer)	**AA-BBBBBB-CCCCCC- EE**	
1.2.5.4	‘aiic’ (data field)	identifier of the participant who is an acquiring bank when transferring funds using payment cards	identifier of the participant who is an acquiring bank in the course of money transfer operations using payment cards (Acquiring institution identification code) - field ‘F032’ of ISO 8583 [7], [8], [9]	
1.2.5.5	‘cati’ (data field)	identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn	identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn (Card acceptor terminal identification) - field ‘F041’* of the ISO 8583 Financial Messaging Standard [7], [8], [9] * The terminal identifier value should be aligned to the left and supplemented with spaces on the right with up to 8 characters	
1.2.5.6	‘caic’ (data field)	identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn by its geographical location	identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) - field ‘F042’* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of the service point identifier shall be aligned to the left and supplemented with spaces	

			on the right with up to 15 characters	
1.3	‘payee’ (data block)	information identifying the payee		
1.3.1	'bik' (data field)	BIC of the money transfer operator serving the payee	in the **AAAAAAAAA** format	
1.3.2	'inn' (data field)	TIN of the payee – a legal entity, and (or) an individual entrepreneur, and (or) a person engaged in private business	in the **XXXXXXXXXX** format - for legal entities, in **XXXXXXXXXX** or **XXXXXXXXX** formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation	
1.3.3	‘namePayee’ (data field)	name of the organisation that is the payee	textarea (text field)	
1.3.4	'payeeTransferId' (data subblock)	identification data depending on the method of a money transfer		
	'transferType' (data field)	type of money transfer method	One code is selected from the limited set of possible values: • **[paymentCard]** – when transferring funds using payment cards; • **[settlement]** – when transferring funds to bank accounts; • **[phoneNumber]** – when transferring funds by telephone number; • **[idNumber]** – if the balance of electronic funds changes	

1.3.4.1	'paymentCard' (data subblock)	when transferring funds using payment cards		
1.3.4.1.1	'number' (data field)	number of the payment card of the payee issued to him and (or) the person authorised by the payee, the money transfer operator – the issuer	в the **XXXXXXXXXXXXXXXXXX** format payment card number shall be provided without spaces (_) and separation marks (-).	
1.3.4.2	'settlement' (d subblock)	when making money transfers in bank accounts by debiting funds from payers' bank accounts		
1.3.4.2.1	'number' (data field)	the settlement account number of the payee opened with the money transfer operator serving the payee	in the **XXXXXXXXXXXXXXXXXXX** format bank account number shall be provided without spaces (_) and separation marks (-).	
1.3.4.3	'phoneNumber' (data subblock)	when making money transfers by telephone number		
1.3.4.3.1	'number' (data field)	the payee's phone number	in the **KKKXXXNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number.	

			The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-).	
1.3.4.4	'idNumber' (data subblock)	if the balance of electronic funds changes		
1.3.4.4.1	'number' (data field)	identification number of the payee, in particular, the number of the electronic wallet of the payee used by him/her on the basis of a bank account agreement and (or) an agreement on the use of electronic payment instruments concluded with the money transfer operator	textarea (text field)	

8. The data submission form used by information exchange participants to provide a response to the Bank of Russia's request to the information exchange participant serving the payee and the timeframes for their submission to the Bank of Russia

In response to the Bank of Russia's request for verification of a particular payee specified in Chapter 7 hereof, the information shall be sent to the Bank of Russia as soon as possible, but no later than the day following the date of receipt by the information exchange participant serving the payee of the corresponding request of the Bank of Russia.

The information in response to the Bank of Russia's request regarding the suspension (impossibility to suspend) of funds crediting to the payee's bank account or the increase in the balance of the payee's electronic funds specified in Chapter 7 hereof shall be sent promptly upon receipt of the relevant request from the Bank of Russia.

8.1. Identification data of the response to the Bank of Russia's request. Data block **[HEADER]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format	Obligation of informing
1.1	'schemaType' (data field)	type of electronic message	Specify the value of **[anifraudResponse]** – a response of the 'payee' of an unauthorised transaction to the Bank of Russia	{ 'header': { 'schemaType': 'anifraudResponse', 'schemaVersion': '1', 'version': '1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z' },	[O]
1.2	'schemaVersion' (data field)	electronic message type scheme	textarea (text field)		[O]
1.3	'version' (data field)	electronic message version number during information exchange	numeric value (int)		[O]
1.4	'memberId' (data field)	identifier of an information exchange participant assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] and assigned by the Bank of Russia		[O]
1.5	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification		[N]

			RFC 4122 [16] assigned by an information exchange participant		
1.6	‘publishedAt’ (data field)	date and time when the response to the Bank of Russia's request was submitted	data presentation format in accordance with Specification RFC 3339 [11]		[O]

8.2. Description of the response form to the Bank of Russia's request. Data block **[anifraudResponse]**

The data submission form for information exchange participants to provide a response to the Bank of Russia's request sent to the information exchange participant serving the payee shall be used:

when the money transfer operator serving the payee, including the electronic money operator, informs the Bank of Russia about a particular payee [4];

when sending a notification of the successful suspension of funds crediting to the payee's bank account or an increase in the balance of the payee's electronic funds [20];

when sending a notification of the impossibility to suspend funds crediting to the bank account of the payee or an increase in the balance of the payee's electronic funds [20].

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of information provision

1	‘antifraudResponse (data block)		If it necessary to indicate several values of blocks of data (payer, payee, additionalStatus) one or several objects in the block of data ‘antifraud’ should be specified	‘anifraudResponse’: [{
				‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘victim’: ‘information on the legal status of the payer’,
				-
				‘recipient’: ‘information on the legal status of the payee’,
				‘payeeIdentifier’: {
				‘hash’: ‘P79969612A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9A8FA441E11’,
				‘hashSnils’: ‘B49087832A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9A8FA441E44’
				},
				‘payer’: {
				‘bik’: ‘123456789’,
				‘inn’: ‘123456789000’,
				‘payerName’: ‘name of the organisation
					[O]

1.2	‘sourceId’ (data field)	identifier assigned by an information exchange participant being the payer	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] and assigned by the information exchange participant		[O]
1.3	'victim' (data field)	information on the legal status of the payer	One code shall be selected from the limited set of possible values: • **[person]** - an individual; • **[entity]** - a legal		[O]

			entity	that is the payer',
				'payerTransferId': {
				'transferType': 'type of money transfer method',
				'paymentCard': {
				'number': '123412341234123412',
				'sum': 'the amount of a money transfer transaction using payment cards'.
				'currency': 'currency of money transfers',
				'dateTimeAt': '2018-01-13T09:14:38Z',
				'rrn': 'the number generated for a money transfer transaction during its authorisation'
				},
				'settlement': {
				'number': '12345123451234512345',
				'sum': 'amount of a money transfer transaction',
				'currency': 'currency of a funds transfer transaction',
				'dateTimeAt': '2018-01-13T09:14:38Z'
				},
				'phoneNumber': {
				'number': '1212312345678',
				'sum': 'transaction amount',
				'currency': 'transaction currency', 'dateTimeAt': '2018-01-13T09:14:38Z'
				},
				'idNumber': {
				'number': '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT',
				'sum': 'transaction amount',
				'currency': 'transaction currency',
				'dateTimeAt':'2018-01-	

1.4	'recipient' (data field)	information on the legal status of the payee	One code shall be selected from the limited set of possible values: • **[person]** – an individual; • **[entity]** – a legal entity		[O]
1.5	'payeeIdentifier' (data block)	identification data of a particular payee			[O]
1.5.1	'hash' (data field)	information on the result of calculating a hash function of the identification document number in order to identify the applicant(s) authorised to dispose of the funds of the payee(s)	The sequence of symbols obtained as a result of the calculation of the SHA-256 hash function from the series and number of the identification document. The series and number of the identification document are provided for calculating the hash function: without spaces (_), the number sign (N), letters (if any) in upper case (ABC). For a Russian passport, this is **XXXXYYYYY**, where: **XXXX** – four-digit passport series; **YYYYYY** is the six-digit passport number. Source text encoding (before hash) – Windows-1251;		[O]

			Hash text encoding – Windows-1251.	13T09:14:38Z’
				}
				},
				‘device’: {
				‘ip’: ‘127.0.0.1’,
				‘imsi’: ‘international mobile subscriber identifier (individual subscriber number)’,
				‘imei’: ‘international mobile equipment identifier’,
				‘aiic’: ‘Acquiring institution identification code (32 поле ISO 8583)’,
				‘cati’: ‘Card acceptor terminal identifica-tion (41 поле ISO 8583)’,
				‘caic’: ‘Card acceptor identification code (42 поле ISO 8583)’
				}	

1.5.2	'hashSnils' (data field)	information on the result of the calculation of the SNILS hashing function of the payee (s) who is (are) the person(s) authorised to dispose of the funds of the payee(s)	The sequence of symbols obtained as a result of calculating the SHA-256 hash function from the payer’s SNILS. SNILS is provided for calculating the hash function: without spaces (_) and separation marks (-). SNILS type: **XXXXXXXXXXX** Source text encoding (before hash) - Windows-1251; Hash text encoding – Windows-1251.	}	[O]

1.6	‘payer’ (data block)	information identifying the payer		‘payee’: {
				‘bik’: ‘123456789’,
				‘inn’: ‘123456789000’,
				‘payeeName’: ‘name of the organisation that is the payee’,
				‘payeeTransferId’: {
				‘transferType’: ‘type of money transfer method’,
				‘paymentCard’: {
				‘number’: ‘123412341234123412’,
				‘sum’: ‘the amount of a money transfer transaction using payment cards’.
				‘currency’: ‘the amount of a money transfer transaction using payment cards’,
				‘status1’: {
				‘enrollment’: ‘transaction suspension identifier’,
				‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’
				}
				},
					[O]

1.6.1	'bik' (data field)	BIC of the money transfer operator serving the payer	in the **AAAAAAAAA** format		[O]
1.6.2	'inn' (data field)	TIN of the payer who is a legal entity, and/or an individual entrepreneur, and/or a person engaged in private business	in the **XXXXXXXXX** format - for legal entities, in **XXXXXXXXX** or **XXXXXXXXX** formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation.		[O]
1.6.3	'payerName' (data field)	organisation name that is the payer	textarea (text field)		[O]

				‘settlement’: {	
1.6.4	'payerTransferId' (data subblock)	identification data depending on the money transfer method		‘number’: ‘12345123451234512345’, ‘sum’: ‘amount of a money transfer transaction using payment cards’, ‘currency’: 'currency of money transfers', ‘status1’: { ‘enrollment’: ‘transaction suspension identifier’ ‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’ } }, ‘phoneNumber’: { ‘number’: ‘1212312345678’, ‘sum’: ‘transaction amount’, ‘currency’: ‘transaction currency’, ‘status1’: { ‘enrollment’: ‘transaction suspension identifier’ ‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’ } }, ‘idNumber’: { ‘number’: ‘1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT’, ‘sum’: ‘amount of a transaction for changing the balance of funds’, ‘currency’: ‘currency of a transaction for changing the balance of funds’, ‘status1’: { ‘enrollment’: ‘transaction suspension identifier’ ‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’ } } }	[O]
1.6.4.1	'transferType' (data field)	type of money transfer method	One code shall be selected from the limited set of possible values: • **[paymentCard]** – when transferring funds using payment cards; • **[settlement]** – when transferring funds in bank accounts; • **[phoneNumber]** – when transferring funds by telephone number; • **[idNumber]** – when the balance of electronic money changes		[O]
1.6.4.2	'paymentCard' (data subblock)	when transferring funds using payment cards			[O]
1.6.4.2.1	'number' (data field)	the number of a payer's payment card issued to him/her and (or) the person authorised by the payer and the money transfer operator who is the issuer	in the **XXXXXXXXXXXXXXXXXX** format payment card number shall be provided without spaces (_) and separation marks (-).		[O]
1.6.4.2.2	'sum' (data field)	the amount of a money transfer transaction using payment cards	transaction amount - field ‘F004’ of ISO 8583 Financial Messages Standard [7], [8], [9]		[O]

1.6.4.2.3	'currency' (data field)	currency of a money transfer transaction	transaction currency – field 'F049' of ISO 8583 Financial Messages Standard [7], [8], [9]	} }] }	[O]
1.6.4.2.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]		[O]
1.6.4.2.5	'rrn' (data field)	number generated for a money transfer transaction during its authorisation	the number generated for a money transfer transaction during its authorisation - field 'F037'* of ISO 8583 Financial Messages Standard [7], [8], [9] * The value of field 'F037' (Retrieval Reference Number) shall be generated by the acquiring bank host according to the following rule: **YJJJXXNNNNNN**, where: **Y** is the last figure of a year; **JJJ** is a Julian date; **XX** is the identifier assigned to the acquiring bank host by the operator; **NNNNNN** is the transaction sequence number during a day		[O]
1.6.4.3	'settlement' (data subblock)	when transferring funds in bank accounts by debiting money from payers' bank accounts			[O]
1.6.4.3.1	'number' (data field)	bank account number of the payer opened with	in the		[O]

		the money transfer operator serving the payer	**XXXXXXXXXXXXXXXXXXXX** format bank account number shall be provided without spaces (_) and separation marks (-).		
1.6.4.3.2	'sum' (data field)	amount of a fund transfer transaction	textarea (text field)		[O]
1.6.4.3.3	'currency' (data field)	currency of a fund transfer transaction	textarea (text field)		[O]
1.6.4.3.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]		[O]
1.6.4.4	'phoneNumber' (data subblock)	when making money transfers by telephone number			[O]
1.6.4.4.1	'number' (data field)	the payer's telephone number specified in a bank account agreement and/or a agreement on the use of electronic payment instruments concluded with the payer	in the **KKKXXXNNNNNNNN** format, where: **KKK** – from one to three characters of the country code; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-).		[O]
1.6.4.4.2	'sum' (data field)	transaction amount	textarea (text field)		[O]
1.6.4.4.3	'currency' (data field)	transaction currency	textarea (text field)		[O]
1.6.4.4.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]		[O]
1.6.4.5	'idNumber' (data subblock)	if the balance of electronic funds changes			[O]

1.6.4.5.1	'number' (data field)	the payer's identification number, in particular, the number of the payer's electronic wallet used by him/her on the basis of a bank account agreement and (or) an agreement on the use of electronic payment instruments concluded with the money transfer operator	textarea (text field)		[O]
1.6.4.5.2	'sum' (data field)	transaction amount	textarea (text field)		[O]
1.6.4.5.3	'currency' (data field)	transaction currency	textarea (text field)		[O]
1.6.4.5.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]		[O]
1.6.5	'device' (data subblock)	parameters of the device used to access the automated system and software for the purpose of transferring funds without the customer's consent			[N]
1.6.5.1	'ip' (data field)	network address of a computer and/or a communication device (router) (IP)	The IPv4 network address shall comply with Specification RFC 791 [12]		[N]
1.6.5.2	'imsi' (data field)	International Mobile Subscriber Identity (IMSI) means the international identifier of a mobile subscriber (individual number of a subscriber (individual customer) by which the system recognises a mobile communication user using GSM and UMTS standards	number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**		[N]

1.6.5.3	'imei' (data field)	International Mobile Equipment Identity (IMEI) – international identifier of mobile equipment (mobile device of an individual customer)	number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**		[N]
1.6.5.4	'aiic' (data field)	identifier of the participant who is an acquiring bank when it transfers funds using payment cards	identifier of the participant who is an acquiring bank during money transfer transactions using payment cards (Acquiring institution identification code) - field 'F032' of ISO 8583 [7], [8], [9]		[N]
1.6.5.5	'cati' (data field)	identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn	identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn (Card acceptor terminal identification) – field 'F041'* of ISO 8583 Financial Messages Standard [7], [8], [9] * The value of the terminal identifier shall be aligned to the left and supplemented with spaces on the right with up to 8 characters		[N]
1.6.5.6	'caic'	identifier of the ATM	identifier of the ATM and/or		[N]

	(data field)	and/or the electronic terminal funds are transferred and/or withdrawn by its geographical location	the electronic terminal where funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) - field ‘F042’* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of the service point identifier shall be aligned to the left and supplemented with spaces on the right with up to 15 characters		
1.7	‘payee’ (data block)	information identifying the payee			[O]
1.7.1	'bik' (data field)	BIC of the money transfer operator serving the payee	in the **AAAAAAAAA** format		[O]
1.7.2	'inn' (data field)	TIN of the payee – a legal entity, and (or) an individual entrepreneur, and (or) a person engaged in private business	in the **XXXXXXXXX** format - for legal entities, in **XXXXXXXXX** or **XXXXXXXXX** formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation		[O]
1.7.3	'payeeName' (data field)	name of the organisation that is the payee	textarea (text field)		[O]
1.7.4	'payeeTransferId' (data subblock)	identification data depending on the			[O]

		money transfer method			
1.7.4.1	'transferType' (data field)	type of money transfer method	One code shall be selected from the limited set of possible values: • **[paymentCard]** – when transferring funds using payment cards; • **[settlement]** – when transferring funds in bank accounts; • **[phoneNumber]** – when transferring funds by telephone number; • **[idNumber]** – when the balance of electronic money changes		[O]
1.7.4.2	'paymentCard' (data subblock)	when transferring funds using payment cards			[O]
1.7.4.2.1	'number' (data field)	number of the payment card of the payee issued to him/her and (or) the person authorised by the payee, the money transfer operator – the issuer	in the **XXXXXXXXXXXXXXXXXX** format payment card number shall be provided without spaces (_) and separation marks (-).		[O]
1.7.4.2.2	'sum' (data field)	the amount of a money transfer transaction using payment cards	transaction amount - field 'F004' of ISO 8583 Financial Messages Standard [7], [8], [9]		[O]
1.7.4.2.3	'currency' (data field)	currency of a money transfer transaction	transaction currency – field 'F049' of ISO 8583 Financial Messages Standard [7], [8], [9]		[O]

1.7.4.2.4	‘status1’ (data subblock)	transaction suspension status			[O]
1.7.4.2.4.1	‘enrollment’ (data field)	transaction suspension identifier	One code shall be selected from the limited set of possible values: • **[successful]** – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • **[unsuccessful]** – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee's electronic funds		[O]
1.7.4.2.4.2	'dateTimeAt' (data field)	date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) the increase in the balance of the payee's electronic funds	data provision format in accordance with Specification RFC 3339 [11]		[O]
1.7.4.3	'settlement' (data subblock)	when transferring funds in bank accounts by debiting money from payers’ bank accounts			[O]

1.7.4.3.1	'number' (data field)	the settlement account number of the payee opened with the money transfer operator serving the payee	in the **XXXXXXXXXXXXXXXXXXXX** format bank account number shall be provided without spaces (_) and separation marks (-).		[O]
1.7.4.3.2	'sum' (data field)	amount of a transaction to transfer funds	textarea (text field)		[O]
1.7.4.3.3	'currency' (data field)	currency of a fund transfer transaction	textarea (text field)		[O]
1.7.4.3.4	'status1' (data subblock)	transaction suspension status			[O]
1.7.4.3.4.1	'enrollment' (data field)	transaction suspension identifier	One code shall be selected from the limited set of possible values: • **[successful]** – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • **[unsuccessful]** – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee's electronic funds		[O]
1.7.4.3.4.2	'dateTimeAt' (data field)	date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) the increase in the balance of the payee's electronic funds	data provision format in accordance with Specification RFC 3339 [11]		[O]

		- -			
1.7.4.4	'phoneNumber' (data subblock)	when making money transfers by telephone number			[N]
1.7.4.4.1	'number' (data field)	the payee's phone number	in the **KKKXXXNNNNNNNN** format, where: **KKK** – from one to three characters of the country code; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-).		[N]
1.7.4.4.2	'sum' (data field)	'sum' (data field)	transaction amount		[N]
1.7.4.4.3	'currency' (data field)	'currency' (data field)	transaction currency		[N]
1.7.4.4.4	'status1' (data subblock)	transaction suspension status			[N]
1.7.4.4.4.1	'enrollment' (data field)	transaction suspension identifier	One code shall be selected from the limited set of possible values: • **[successful]** – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • **[unsuccessful]** – it is impossible to suspend		[N]

			the crediting of funds to the payee's bank account or to suspend the increase in the balance of the recipient of electronic funds		
1.7.4.4.4.2	'dateTimeAt' (data field)	date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) the increase in the balance of the payee's electronic funds	data provision format in accordance with Specification RFC 3339 [11]		[N]
1.7.4.5	'idNumber' (data subblock)	if the balance of electronic funds changes			[O]
1.7.4.5.1	'number' (data field)	identification number of the payee, in particular, the number of the electronic wallet of the payee used by him/her on the basis of a bank account agreement and (or) an agreement on the use of the electronic payment instruments concluded with the money transfer operator	textarea (text field)		[O]
1.7.4.5.2	'sum' (data field)	transaction amount	textarea (text field)		[O]
1.7.4.5.3	'currency' (data field)	transaction currency	textarea (text field)		[O]
1.7.4.5.4	'status1' (data subblock)	transaction suspension status			[O]

1.7.4.5.4.1	‘enrollment’ (data field)	transaction suspension identifier	One code shall be selected from the limited set of possible values: • **[successful]** – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • **[unsuccessful]** – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee's electronic funds		[O]
1.7.4.5.4.2	'dateTimeAt' (data field)	date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) the increase in the balance of the payee's electronic funds	data provision format in accordance with Specification RFC 3339 [11]		[O]

9. The form of the Bank of Russia's information message to the information exchange participant serving the payer

The form of the Bank of Russia's information message shall apply to the information exchange participant serving the payer as follows:

when sending a notification on the successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds [20];

when sending a notification of the impossibility to suspend funds crediting to the bank account of the payee or increasing the balance of the payee's electronic funds [20];

9.1. Identification data of the Bank of Russia's information message to the information exchange participant serving the payer.

Data block **[HEADER]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format
1.1	'schemaType' (data field)	type of electronic message	Specify value **[antifraudReturn]** – additional request to the information exchange participant who is the 'payee' of an unauthorised transaction	{ 'header': { 'schemaType': 'antifraudReturn', 'schemaVersion': '1', 'version': '1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'publishedAt': '2002-10-02T15:00:00.05Z' },
1.2	'schemaVersion' (data field)	electronic message type scheme version	textarea (text field)	
1.3	'version' (data field)	electronic message version number during information exchange	numeric value (int)	
1.4	'memberId' (data field)	identifier of an information exchange participant assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia	
1.5	'publishedAt' (data field)	date and time of initial provision of information	data submission format in accordance with Specification RFC 3339 [11]	

9.2. Description of the form of the Bank of Russia's information message to the information exchange participant serving the payer.
Data block **[anifraudReturn]**

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format

1	'anifraudReturn' (data block)		If it is necessary to specify several values of data blocks (payer, payee), specify one or several objects in the data block 'antifraudReturn'	'anifraudReturn': [{
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'victim': 'information on the legal status of the payer',
				'recipient': 'information on the legal status of the payee', 'payer': {
				'bik': '123456789',
				'inn': '123456789000',
				'payerName': 'name of the organisation that is the payer',
				'payerTransferId': {
				'transferType': 'type of money transfer method' -
				'paymentCard': {
				'number': '123412341234123412',
				'sum': 'amount of a money transfer transaction using payment cards',
				'currency': 'currency of a transaction to transfer funds',
				'dateTimeAt': '2018-01-13T09:14:38Z',
				'rrn': 'the number generated for a money transfer transaction during its authorisation'
				},
				'settlement': {
				'number': '12345123451234512345',
				'sum': 'amount of a transaction to transfer funds'
				'currency': 'currency of a transaction to transfer funds',
				'dateTimeAt': '2018-01-13T09:14:38Z'
				},
				'phoneNumber': {

1.1	'sourceId' (data field)	identifier assigned by the information exchange participant being the payer	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	
1.2	'victim' (data field)	information on the legal status of the payer	One code should be selected from the limited set of possible values: • **[person]** – an individual; • **[entity]** – a legal entity	
1.3.	'recipient' (data field)	information on the legal status of the payee	One code should be selected from the limited set of possible values: • **[person]** – an individual; • **[entity]** – a legal entity	
1.4	'payer' (data block)	information identifying the payer		
1.4.1	'bik' (data field)	BIC of the money transfer operator serving the payer	in the **AAAAAAAAA** format	
1.4.2	'inn' (data field)	TIN of the payer – a legal	in the **XXXXXXXXXX** format – for legal entities, in **XXXXXXXXXX** or	

		entity, and/or an individual entrepreneur, and/or a person engaged in private business	**XXXXXXXXXX** formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation.	'number': '1212312345678',
				'sum': 'transaction amount',
				'currency': 'transaction currency',
				'dateTimeAt': '2018-01-13T09:14:38Z'
				},
				'idNumber': {
				'number': '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT',
				'sum': 'transaction amount',
				'currency': 'transaction currency',
				'dateTimeAt': '2018-01-13T09:14:38Z'
				}
				},
				'device': {
				'ip': '127.0.0.1',
				'imsi': 'international mobile subscriber identifier (individual subscriber number)',
				'imei': 'international mobile equipment identifier',
				-
				'aiic': 'Acquiring institution identification code (32 поле ISO 8583)',
				'cati': 'Card acceptor terminal identification (41 поле ISO 8583)',
				'caic': 'Card acceptor identification code (42 поле ISO 8583)'
				}
				},
				'payee': {
				'bik': '123456789
				'inn': '123456789000',
				'payeeName': 'name of the organisation that is the payee',
				'payeeTransferId': {
				'transferType': 'type of money transfer method',
				'paymentCard': {
				'number': '123412341234123412',
				'sum': 'amount of a money transfer transaction using payment cards',
				'currency': 'currency of a transaction to transfer funds using payment cards',

1.4.3	'payerName' (data field)	organisation name that is the payer	textarea (text field)	
1.4.4	'payerTransferId' (data subblock)	identification data depending on the method of a money transfer		
1.4.4.1	'transferType' (data field)	type of a money transfer method	One code should be selected from the limited set of possible values: • **[paymentCard]** – when transferring funds using payment cards; • **[settlement]** – when transferring funds in bank accounts; • **[phoneNumber]** – when transferring funds by a subscriber's telephone number; • **[idNumber]** – when the balance of electronic funds changes	
1.4.4.2	'paymentCard' (data subblock)	when transferring funds using payment cards		
1.4.4.2.1	'number' (data field)	the number of the payer's payment card issued to him and (or) a person	в the **XXXXXXXXXXXXXXXXXX** format payment card number shall be provided without spaces (_)	

		authorised by the payer and the money transfer operator by the issuer	and separation marks (-).	- 02T15:00:00.05Z'
1.4.4.2.2	'sum' (data field)	amount of the money transfer transaction using payment cards	transaction amount - field 'F004' of ISO 8583 Financial Messages Standard [7], [8], [9]	transfer transaction',
1.4.4.2.3	'currency' (data field)	currency of the money transfer transaction	transaction currency - field 'F049' of ISO 8583 Financial Messaging Standard [7], [8], [9]	to transfer funds',
1.4.4.2.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339[11]	- 02T15:00:00.05Z'
1.4.4.2.5	'rrn' (data field)	the number generated for a money transfer transaction during its authorisation	number generated for a money transfer transaction during its authorisation – field 'F037'* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of field 'F037' (Retrieval Reference Number) shall be generated by the acquiring bank host according to the following rule: **YJJJXXNNNNNN**, where: **Y** is the last figure of a year; **JJJ** is a Julian date; **XX** is the identifier assigned to the acquiring bank host by the operator; **NNNNNN** is the transaction sequence number during a day	- 02T15:00:00.05Z'
1.4.4.3	'settlement' (data subblock)	when transferring funds in bank accounts		-

'status1': {
'enrollment': 'transaction suspension identifier',
'dateTimeAt':'2002-10-
}
},
'settlement': {
'number': '12345123451234512345',
'sum': 'amount of a fund
'currency': 'currency of a transaction
'status1': {
'enrollment': 'transaction suspension identifier',
'dateTimeAt':'2002-10-
}
},
'phoneNumber': {
'number': '1212312345678',
'sum': 'transaction amount',
'currency': 'transaction currency',
'status1': {
'enrollment': 'transaction suspension identifier',
'dateTimeAt':'2002-10-
}
},
'idNumber': {
'number':
'1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT',
'sum': 'amount of the transaction for changing the balance of funds',
'currency': 'currency of the transaction for changing the balance of funds',
'status1': {
'enrollment': 'transaction suspension identifier',

		by debiting funds from payers' bank accounts		‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’ } } } } }] }
1.4.4.3.1	'number' (data field)	the number of the payer's bank account opened with the money transfer operator serving the payer	In the **XXXXXXXXXXXXXXXXXXXX** format bank account number shall be provided without spaces (_) and separation marks (-).	
1.4.4.3.2	'sum' (data field)	money transfer amount	textarea (text field)	
1.4.4.3.3	'currency' (data field)	money transfer currency	textarea (text field)	
1.4.4.3.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339[11]	
1.4.4.4	'phoneNumber' (data subblock)	when transferring funds by a subscriber's telephone number		
1.4.4.4.1	'number' (data field)	the payer's telephone number specified in the bank account agreement and/or the agreement on the use of the electronic payment instruments concluded with the payer	In the **KKKXXXNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-).	

1.4.4.4.2	‘sum’ (data field)	transaction amount	textarea (text field)	
1.4.4.4.3	‘currency’ (data field)	transaction currency	textarea (text field)	
1.4.4.4.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]	
1.4.4.5	‘idNumber’ (data subblock)	if the balance of electronic funds changes		
1.4.4.5.1	'number' (data field)	the payer's identification number, in particular, the number of the payer's electronic wallet used by him on the basis of a bank account agreement and (or) an agreement on the use of the electronic payment instruments concluded with the money transfer operator	textarea (text field)	
1.4.4.5.2	'sum' (data field)	transaction amount	textarea (text field)	
1.4.4.5.3	‘currency’ (data field)	transaction currency	textarea (text field)	
1.4.4.5.4	'dateTimeAt' (data field)	transaction date and time	data provision format in accordance with Specification RFC 3339 [11]	
1.4.5	'device' (data subblock)	parameters of the device used to access		

		the automated system and software for the purpose of money transfer without the customer's consent		
1.4.5.1	'ip' (data field)	network address of a computer and/or a communication device (router) (IP)	The IPv4 network address shall comply with Specification RFC 791 [12]	
1.4.5.2	'imsi' (data field)	International Mobile Subscriber Identity (IMSI) means the international identifier of a mobile subscriber (individual number of a subscriber (an individual customer) with which the system recognises a mobile communication user using GSM and UMTS standards	number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**	
1.4.5.3	'imei' (data field)	International Mobile Equipment Identity (IMEI) - international identifier of mobile equipment (mobile device of an individual customer)	number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**	

		-		
1.4.5.4	‘aiic’ (data field)	identifier of the participant who is an acquiring bank when transferring funds using payment cards	identifier of the participant who is an acquiring bank in the course of money transfer transactions using payment cards (Acquiring institution identification code) - field ‘F032’ of ISO 8583 [7], [8], [9]	
1.4.5.5	‘cati’ (data field)	identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn	identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn (Card acceptor terminal identification) - field ‘F041’* of the ISO 8583 Financial Messaging Standard [7], [8], [9] * The terminal identifier value shall be aligned to the left and supplemented with spaces on the right with up to 8 characters	
1.4.5.6	‘caic’ (data field)	identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn by its geographical location	identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) field ‘F042’* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The service point identifier value shall be aligned to the left and supplemented with spaces on the right with up to 15 characters	
1.5	‘payee’ (data block)	information identifying the payee		

		-	
1.5.1	'bik' (data field)	BIC of the money transfer operator serving the payee	in the **AAAAAAAAA** format
1.5.2	'inn' (data field)	TIN of the payee that is a legal entity, and (or) an individual entrepreneur, and (or) a person engaged in private business	in the **XXXXXXXXX** format - for legal entities, in **XXXXXXXXX** or **XXXXXXXXX** formats - for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation
1.5.3	'payeeName' (data field)	the name of the organisation that is the payee	textarea (text field)
1.5.4	'payeeTransferId' (data subblock)	identification data depending on the money transfer method	
1.5.4.1	'transferType' (data field)	type of a money transfer method	One code should be selected from the limited set of possible values: • **[paymentCard]** – when transferring funds using payment cards; • **[settlement]** – when transferring funds in bank accounts; • **[phoneNumber]** – when transferring funds by a subscriber's telephone number; • **[idNumber]** – if the balance of electronic funds changes

1.5.4.2	'paymentCard' (data subblock)	when transferring funds using payment cards		
1.5.4.2.1	'number' (data field)	number of the payment card of the payee issued to him/her and (or) the person authorised by the payee, by the money transfer operator – the issuer	in the **XXXXXXXXXXXXXXXXXX** format payment card number shall be provided without spaces (_) and separation marks (-).	
1.5.4.2.2	'sum' (data field)	amount of the money transfer transaction using payment cards	transaction amount - field 'F004' of ISO 8583 Financial Messages Standard [7], [8], [9]	
1.5.4.2.3	'currency' (data field)	currency of the money transfer transaction	transaction currency – field 'F049' of ISO 8583 Financial Messages Standard [7], [8], [9]	
1.5.4.2.4	'status1' (data subblock)	transaction suspension status		
1.5.4.2.4.1	'enrollment' (data field)	transaction suspension identifier	One code should be selected from the limited set of possible values: • **[successful]** – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • **[unsuccessful]** – it is impossible to suspend funds crediting to the payee's bank account or to suspend	

			increasing the balance of the payee's electronic funds	
1.5.4.2.4.2	'dateTimeAt' (data field)	date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) an increase in the balance of the payee's electronic funds	data provision format in accordance with Specification RFC 3339[11]	
1.5.4.3	'settlement' (data subblock)	when transferring funds in bank accounts by debiting them from payers' bank accounts		
1.5.4.3.1	'number' (data field)	the settlement account number of the payee opened with the money transfer operator serving the payee	In the **XXXXXXXXXXXXXXXXXXXX** format bank account number shall be provided without spaces (_) and separation marks (-).	
1.5.4.3.2	'sum' (data field)	money transfer amount	textarea (text field)	

1.5.4.3.3	'currency' (data field)	money transfer currency	textarea (text field)	
1.5.4.3.4	‘status1’ (data subblock)	transaction suspension status		
1.5.4.3.4.1	‘enrollment’ (data field)	transaction suspension identifier	One code should be selected from the limited set of possible values: • **[successful]** – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • **[unsuccessful]** – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee’s electronic funds	
1.5.4.3.4.2	'dateTimeAt' (data field)	date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) an increase in the balance of the payee’s electronic funds	data provision format in accordance with Specification RFC 3339[11]	
1.5.4.4	'phoneNumber' (data subblock)	when ransferring funds by a		

		subscriber's telephone number		
1.5.4.4.1	'number' (data field)	payee's phone number	in the **KKKXXXNNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-).	
1.5.4.4.2	'sum' (data field)	'sum' (data field)	transaction amount	
1.5.4.4.3	'currency' (data field)	'currency' (data field)	transaction currency	
1.5.4.4.4	'status1' (data subblock)	transaction suspension status		
1.5.4.4.4.1	'enrollment' (data field)	transaction suspension identifier	One code should be selected from the limited set of possible values: • **[successful]** – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • **[unsuccessful]** – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee's electronic funds	
1.5.4.4.4.2	'dateTimeAt' (data field)	date and time of suspending (failure to suspend) funds crediting to the payee's	data provision format in accordance with Specification RFC 3339 [11]	

		bank account or suspending (failure to suspend) increasing in the balance of the payee's electronic funds		
1.5.4.5	'idNumber' (data subblock)	if the balance of electronic funds changes		
1.5.4.5.1	'number' (data field)	identification number of the payee, in particular, the number of the electronic wallet of the payee used by him/her on the basis of a bank account agreement and (or) an agreement on the use of electronic payment instruments concluded with the money transfer operator	textarea (text field)	
1.5.4.5.2	'sum' (data field)	transaction amount	textarea (text field)	
1.5.4.5.3	'currency' (data field)	transaction currency	textarea (text field)	
1.5.4.5.4	'status1' (data subblock)	transaction suspension status		

1.5.4.5.4.1	'enrollment' (data field)	transaction suspension identifier	One code should be selected from the limited set of possible values: • **[successful]** – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • **[unsuccessful]** – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee's electronic funds	
1.5.4.5.4.2	'dateTimeAt' (data field)	date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) an increase in the balance of the payee's electronic funds	data provision format in accordance with Specification RFC 3339[11]	

10. The form for submitting a request to the Bank of Russia from information request participants who are not structural units of the Bank of Russia using the speedy and non-speedy money transfer services, about imposing (or lifting) restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban to debit funds upon detecting incidents related to violations of data protection requirements during money transfers at the information infrastructure facilities of information exchange participants

Mandatory information provision conditions:

[O] – data block (field) information shall be provided as required;

[N] – data block (field) information shall be provided if it is technically feasible.

Time-response characteristics of information provision:

Information on imposing restrictions on bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to a violation of information protection requirements during money transfers at information infrastructure facilities of information exchange participants shall be sent immediately upon detection of the relevant incident.

The data submission form used by information exchange participants for sending a request to the Bank of Russia to impose restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds in the event of detection of incidents related to a violation of data protection requirements shall be applied as follows:

when the Bank of Russia is informed by information exchange participants who are not Bank of Russia structural units using the express money transfer service and the non-rapid money transfer service about imposing restrictions on their banks (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to violations of data protection requirements during money transfers at the information infrastructure facilities of information exchange participants [21];

when the Bank of Russia is informed by information exchange participants who are not Bank of Russia structural units using the speedy money transfer service and the non-speedy money transfer service about lifting restrictions in the form of a ban on debiting funds on their banks (correspondent) accounts (sub-accounts) upon detecting incidents related to violations of information protection requirements during money transfers at the information infrastructure facilities of information exchange participants [21].

10.1. Identification data of a request of information exchange participants to the Bank of Russia to impose (or lift) the restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to a violation of data protection requirements. Data block **[HEADER]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format	Obligation of informing
1.1	'schemaType' (data field)	type of electronic message	Specify the value of **[lockRequest]** – a request of information exchange participants to impose or lift the restriction on debiting funds on their bank (correspondent) accounts (sub-accounts)	{ 'header': { 'schemaType': 'lockRequest', 'schemaVersion': '1', 'version': '1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z' },	[O]
1.2	'schemaVersion' (data field)	electronic message type scheme	textarea (text field)		[O]
1.3	'version' (data field)	electronic message version number during information exchange	numeric value (int)		[O]
1.4	'memberId' (data field)	identifier of an information exchange participant assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] and assigned by the Bank of Russia		[O]
1.5	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant		[N]
1.6	'publishedAt' (data field)	date and time when the request was submitted to the Bank of Russia	data presentation format in accordance with Specification RFC 3339 [11]		[O]

10.2. Description of a request of information exchange participants to the Bank of Russia to impose (or lift) the restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to a violation of data protection requirements. Data block **[lockRequest]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format	Obligation of informing
2.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	'lockRequest': [{ 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'orgBik': '123456789', 'regNumber': '123456789', 'uniqIdentifier': '1234567891', 'actionStatus': 'status of restriction on funds debiting', 'dateAt': '20180101', 'text': 'additional description','persons': { 'lastName': 'last name', 'firstName': 'name', 'middleName': 'middle name', 'landlineNumber': '1212312345678', 'mobileNumber': '1212312345678', 'email': 'qwerty1@example.ru', 'position': 'position' }, 'attachment': { 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'comment': 'description of the attachment', 'dateTimeAt': '2018-03-22T08:14:38Z', 'file': { 'name': 'file name', 'size': 'file size in bytes', 'base64': 'attachment in base64 format' } } }] }	[O]
2.2	'orgBik' (data field)	BIC of an information exchange participant	In the **AAAAAAAAA** format		[O]
2.3	'regNumber' (data field)	registration number from the register of state registration of credit institutions	textarea (text field)		[O]
2.4.	'uniqIdentifier' (data field)	unique identifier of the originator of an electronic message (UIS) [22]	In the **XXXXXXXXXX** format		[O]
2.5	'actionStatus' (data field)	status of restriction on funds debiting	One code shall be selected from the limited set of possible values: • **[on]** – a request for the restriction in the form of a ban on debiting funds from bank (correspondent) accounts (sub-accounts); • **[off]** – a request to lift the restriction in the form of a ban on debiting funds from bank (correspondent) accounts (sub-accounts)		[O]
2.6	'dateAt'	a calendar date from	data submission format		[O]

	(data field)	which it is necessary to suspend the exchange of electronic messages when funds are transferred within the Bank of Russia payment system due to the identification of problems in providing information protection and making (suspicion about making) unauthorised money transfers	in accordance with ISO 8601:2004 [23]		
2.7	'text' (data field)	additional description	textarea (text field)		[N]
2.8	‘person’ (data block)	identifiers of the point of contact who sent a request to impose or lift the restriction in the form of a ban on debiting funds to bank (correspondent) accounts (sub-accounts)			[O]
2.8.1	‘lastName’ (data field)	surname	textarea (text field)		[O]
2.8.2	‘firstName’ (data field)	name	textarea (text field)		[O]
2.8.3	‘middleName’ (data field)	middle name	textarea (text field)		[O]
2.8.4	‘landlineNumber’ (data field)	stationary phone	textarea (text field)		[O]
2.8.5	‘mobileNumber’ (data field)	mobile phone	textarea (text field)		[O]
2.8.6	‘email’ (data field)	e-mail address	textarea (text field)		[O]
2.8.7	‘position’ (data field)	position	textarea (text field)		[O]
2.9	'attachment' (data block)	additional data to confirm the imposition or lift of the restriction in the form of a			[O]

		ban on debiting funds			
2.9.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant		[O]
2.9.2	‘comment’ (data field)	attachment description	textarea (text field)		[O]
2.9.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[O]
2.9.4	'file' (data block)	data file	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding		[O]

11. The form of an information message of the Bank of Russia on imposing (or lifting) the restriction on bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds

The form of an information message of the Bank of Russia on imposing (or lifting) the restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban to debit funds shall be used as follows:

when sending a notification to an information exchange participant in the event of achieving a positive result of integrity control and acceptance of requests to impose or lift the restriction in the form of a ban to debit funds [21];

when sending a notification to an information exchange participant in the event of achievement of a negative result of integrity control and non-acceptance of requests to impose or lift the restriction in the form of a ban on funds debiting [21].

11.1. Identification data of an information message of the Bank of Russia on imposing (or lifting) the restriction on bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds. Data block **[HEADER]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format
1.1	'schemaType' (data field)	type of electronic message	Specify the value of **[lockResponse]** – an information message of the Bank of Russia on imposing (or lifting) the restriction on bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds	{ 'header': { 'schemaType': 'lockResponse', 'schemaVersion': '1', 'version': '1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z' },
1.2	'schemaVersion' (data field)	electronic message type scheme version	textarea (text field)	
1.3	'version' (data field)	electronic message version number during information exchange	numeric value (int)	
1.4	'memberId' (data field)	identifier of an information exchange participant assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by the Bank of Russia	

1.5	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant	
1.6	‘publishedAt’ (data field)	date and time of providing information to information exchange participant	data submission format in accordance with Specification RFC 3339 [11].	

11.2. Description of the form of an information message of the Bank of Russia on imposing or lifting the restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban to debit funds. Data block **[lockResponse]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format
2.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	‘lockResponse’: [{ ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘orgBik’: ‘123456789’, ‘regNumber’: ‘123456789’, ‘uniqIdentifier’: ‘1234567891’, ‘actionStatus’: ‘status of restriction on debiting funds’, ‘coordinationStatus’: ‘the status of integrity control of a request to impose or lift the restriction in the form of a ban on debiting funds ‘dateAt’: ‘20180101’, ‘text’: ‘additional description’,’attachment’: { ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘comment’: ‘attachment description’, ‘dateTimeAt’: ‘2018-03-22T08:14:38Z’, ‘file’: { ‘name’: 'file name', ‘size’: ‘file size in bytes’, ‘base64’: 'attachment in base64 format' } } }]
2.2	‘orgBik’ (data field)	BIC of an information exchange participant	in the **AAAAAAAAA** format	
2.3	‘regNumber’ (data field)	registration number from the register of state registration of credit institutions	textarea (text field)	
2.4	‘uniqIdentifier’ (data field)	unique identifier of the originator of an electronic message (UIS) [22]	In the **XXXXXXXXXX** format	
2.5	‘actionStatus’ (data field)	status of restriction on funds debiting	One code is selected from the limited set of possible values: • **[on]** – a request for the restriction in the form of a ban on debiting funds from bank (correspondent) accounts (sub-accounts);	

			• **[off]** – a request to lift the restriction in the form of a ban on debiting funds from bank (correspondent) accounts (sub-accounts) -	}
2.6	'coordination Status' (data field)	the status of integrity control of a request to impose (or lift) the restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds	One code is selected from the limited set of possible values: • **[accepted]** – a positive result of integrity control and acceptance of the request for imposing (or lifting) the restriction in the form of a ban on debiting funds; • **[rejected]** – a negative result of integrity control and non-acceptance of the request to impose (or lift) the restriction in the form of a ban on debiting funds	
2.7	'dateAt' (поле данных)	calendar date from which it is necessary to cancel the suspension of the exchange of electronic messages when funds are transferred within the Bank of Russia payment system due to the identification of problems in providing information protection and making (suspicion about making) unauthorised money transfers	data submission format in accordance with ISO 8601:2004 [23]	
2.8	'text' (data field)	additional description	textarea (text field)	
2.9	'attachment'	additional data		

	(data block)	containing information on transactions in bank (correspondent) accounts (sub-accounts) of an information exchange participant		
2.9.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant	
2.9.2	'comment' (data field)	attachment description	textarea (text field)	
2.9.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339[11]	
2.9.4	'file' (data block)	data file	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding	

12. The form of distribution by the Bank of Russia among information exchange participants of data on the detected incidents associated with violations of data protection requirements

12.1. Information bulletin identification data. Data block **[HEADER]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format
1.1	'schemaType' (data field)	type of electronic message	Specify **[REACTION]** value – Bank of Russia Information Bulletin	{ 'header': { 'schemaType': 'reaction', 'schemaVersion': '1', 'version': '1', 'publishedAt': '2002-10-02T15:00:00.05Z' },
1.2	'schemaVersion' (data field)	electronic message type scheme version	textarea (text field)	
1.3	'version' (data field)	electronic message version number during exchange participant	numeric value (int)	
1.4	'publishedAt' (data field)	date and time of information provision	data submission format in accordance with Specification RFC 3339 [11]	

12.2. Description of the form of the information bulletin. Data block **[REACTION]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format
1.1	'fixationAt' (data field)	date and time of the incident with an information exchange participant	data provision format in accordance with Specification RFC 3339[11]	'reaction': { 'fixationAt': '2002-10-02T15:00:00.05Z', 'rootCause': 'key causes of the incident', 'vectorCode': 'computer attack vector identifier', 'serviceType': [{ 'type': 'type of attacked object', 'name': 'name of software/hardware', 'version': 'version of software/hardware',
1.2	'rootCause' (data field)	key causes of the incident	textarea (text field)	
1.3	'vectorCode' (data field)	computer attack vector identifier	One code is selected from the limited set of possible values: vector **[INT]** – aimed at	- -

			the infrastructure of an information exchange participant;
			• vector **[EXT]** – aimed at an information exchange participant's customer;
				'description': 'additional description of the type of object under attack'
				}],
				'typeOfAttack': 'computer attack type code',
				;antifraudDistribution': [{
				'device': {
				'ip': '127.0.0.1',
				'imsi': 'international mobile subscriber identifier (individual subscriber number)',
				'imei': 'international mobile equipment identifier',
				'aiic': 'acquiring institution identification code (32 field ISO 8583)',
				'cati': 'card acceptor terminal identification (41 field ISO 8583)',
				'caic': 'card acceptor identification code (42 field ISO 8583)'
				},
				'payee': {
				'bik': '123456789',
				'hash': 'P79969612A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA44 11',
				'hashSnils': 'B49087832A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA44 44',
				'inn': '123456789000',
				'transferId': {
				'paymentCard': {
				'number': '123412341234123412'
				},
				'settlement': {
				'number': '12345123451234512345'
				},
				'phoneNumber': {
				'number': '1212312345678'
				},
				'idNumber': {
				'number':

1.4	'serviceType'(data block)	identifier of an information infrastructure object	If it is necessary to specify several data field values (type, name, version, description), specify one or several objects in the data block 'serviceType"	
1.4.1	'type' (data field)	type of the object under attack	One code should be selected from the limited set of possible values: 1) system levels: • **[hw]** – hardware, • **[net]** – network equipment, • **[net _ s]** – network applications and services, • **[hw _ s]** – server components of virtualisation, software infrastructure services, • **[os]** – operating systems, database management systems, application servers; 2) the level of the AS and applications used to provide services within the framework of business or technological processes of an information exchange participant: • **[rbs]** – remote banking system, • **[front-office]** – payment card transaction processing system, • **[web]** – information resources of the Internet, • **[abs]** – automated banking system, • **[back-office]** – a system of	

			post-transaction servicing of transactions carried out using payment cards;
			• **[participant _ w]** – automated systems used by employees of an information exchange participant
			
			3) the level of the AC and applications of the information exchange participant's customer:
			• **[cfs]** – file server,
			• **[crbs]** – remote banking system,
			• **[ecs]** – e-mail server;
			• **[client_ w]** – automated systems used by employees of an information exchange participant's client;
			
			4) other system:
			• **[oth]** – other system
				'1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT'
				}
				}
				},
				'additionalStatus': {
				'crossBorder': 'cross-border identifier'
				-
				'additionalTransactionApprove': ['additional transaction
				confirmation identifier'
				]
				}
				}],

1.4.2	'name' (data field)	name of software/hardware	textarea (text field)	
1.4.3	'version' (data field)	version of software-/hardware information	textarea (text field)	
1.4.4	'description' (data field)	additional description of the type of the object under attack	textarea (text field)	
1.5	'typeOfAttack' (data field)	computer attack type identifier	One code is selected from a limited set of possible values: • **[trafficHijackAttacks]** – computer attacks related to changes in route and address information; • **[malware]** – computer attacks related to the use of	

			malicious software in relation to information infrastructure objects of information exchange participants and their customers; • **[socialEngineering]** – computer attacks resulting from inducing customers to carry out money transfer transactions through deceit or abuse of trust; • **[ddosAttacks]** – 'denial-of-service' type computer attacks (DDoS attacks) in relation to the information infrastructure of information exchange participants; • **[atmAttacks]** – computer attacks related to unauthorised access to ATMs and payment terminals of information exchange participants; • **[vulnerabilities]** – computer attacks associated with information infrastructure vulnerabilities of information exchange participants and their clients; • **[bruteForces]** – computer attacks related to searching (hacking) and compromising authentication data (login) data; • **[spams]** – computer attacks related to spam mailouts to information exchange participants and their customers; • **[controlCenters]** – computer attacks related to detecting the interaction of information infrastructure objects of information exchange participants with Botnet command centres;	

			• **[sim]** – computer attacks associated with the change (substitution) of the mobile subscriber identifier (IMSI) of the SIM card number, as well as with the replacement of the mobile equipment identifier (IMEI); • **[phishingAttacks]** – computer attacks related to information that misleads information exchange participants and their clients, as well as other persons interacting with them, about the ownership of the information disseminated via the Internet due to the similarity of domain names, design or content. • **[prohibitedContents]** – computer attacks related to the distribution of information related to the offer and/or provision of financial services in the Russian Federation by persons not authorised to do so in accordance with the legislation of the Russian Federation. Posting prohibited content on the Internet; • [**[maliciousResources]** – computer attacks related to the placement on the Internet of information enabling illegal access to information systems of information exchange participants and their customers used when providing (buying) financial services, including through illegal access to confidential customer information.	

			Placing a malicious resource on the Internet; • **[changeContent]** – computer attacks related to changes in content; • **[scanPorts]** – computer attacks related to scanning software ports of information infrastructure objects of information exchange participants by persons who do not have the relevant authority; • **[other]** – other computer attacks against information infrastructure objects of information exchange participants and their clients	
	'antifraudDistribution' (data block)		If it is necessary to specify several data field values (device, payee, additionalStatus), specify one or several objects in the data block 'antifraudDistribution'	
1.6	'device' (data subblock)	identifiers of the device used for conducting an unauthorised transaction -		
1.6.1	'ip' (data field)	network address of a computer and/or a communication device (router) (IP)	Logical IPv4 address shall comply with Specification RFC 791 [12]	
1.6.2	'imsi' (data field)	International Mobile Subscriber Identity (IMSI) means the international identifier of a mobile subscriber (individual number of a subscriber (individual customer) by which the system recognises a mobile communication user applying GSM and UMTS standards	number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**	

1.6.3	'imei' (data field)	International Mobile Equipment Identity (IMEI) – the international identifier of mobile equipment (mobile device of an individual customer)	number (15-bit in decimal) **AA-BBBBBB-CCCCCC-EE**	
1.6.4	‘aiic’ (data field)	identifier of the participant who is an acquiring bank when it transfers funds using payment cards	identifier of the participant who is an acquiring bank in the course of money transfer operations using payment cards (Acquiring institution identification code) - field ‘F032’ of ISO 8583 Financial Messaging Standard [7], [8], [9]	
1.6.5	‘cati’ (data field)	identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn	identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn (Card acceptor identification code), – field ‘F041’* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The terminal identifier value should be aligned to the left and supplemented with spaces on the right with up to 8 characters	
1.6.6	‘caic’ (data field)	identifier of the ATM and/or electronic terminal where funds are transferred and/or withdrawn by its geographical location	identifier of the ATM and/or electronic terminal where funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) – field ‘F042’* of ISO 8583 Financial Messaging Standard [7], [8], [9]	

			* The value of the service point identifier shall be aligned to the left and supplemented with spaces on the right with up to 15 characters	
1.7	‘payee’ (data block)	information determining the payee when funds are transferred without the customer's consent (hereinafter, information on the payee)		
1.7.1	'bik' (data field)	BIC of the money transfer operator serving the payee	in the **AAAAAAAAA** format	
1.7.2	‘hash’ (data field)	sequence of symbols obtained as a result of calculating the SHA-256 hash function from the identification document series and number	The sequence of symbols obtained as a result of the calculation of the SHA-256 hash function from the identification document series and number. The series and number of the identification document are provided for calculating a hash function: without spaces (_), the number sign (N), letters (if any) in upper register (ABC). For the Russian passport this is **XXXXYYYYYY**, where: **XXXX** is four-digit passport series; **YYYYYY** is a six-digit passport number. Source text encoding (before hash) - Windows-1251; Hash text encoding – Windows-1251.	

1.7.3	'hashSnils' (data field)	SNILS number as the SHA-256 hash function	The sequence of symbols obtained as a result of calculating the SHA-256 hash function from the payer SNILS. SNILS is provided for calculating a hash function: without spaces (_) and separation marks (-). SNILS type: **XXXXXXXXXXX** Source text encoding (before hash) - Windows-1251; Hash text encoding – Windows-1251.	
1.7.4	'inn' (data field)	TIN of the payee - a legal entity	In the **XXXXXXXXXX** format – for legal entities, in **XXXXXXXXXX** or **XXXXXXXXX** formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation	
1.7.5	'transferId' (data subblock)	identification data depending on the money transfer method		
1.7.5.1	'paymentCard' (data subblock)	when transferring funds using payment cards	If it is necessary to specify several values of data blocks (number), specify one or several objects in the data block 'paymentCard'	
1.7.5.1.1	'number' (data field)	number of the payment card of the payee issued to him/her and (or) the person authorised by the payee, by the money transfer operator – the issuer	in the **XXXXXXXXXXXXXXXXXX** format payment card number shall be provided without spaces (_) and separation marks (-).	
1.7.5.2	'settlement'	when making money	If it is necessary to specify	

	(data sub-block)	transfers in bank accounts by debiting funds from payers' bank accounts	several values of the data field (number), specify one or several objects in the 'settlement' data sub-block	
1.7.5.2.1	'number' (data field)	the settlement account number of the payee opened with the money transfer operator serving the payee	in the **XXXXXXXXXXXXXXXXXXXX** format bank account number shall be provided without spaces (_) and separation marks (-).	
1.7.5.3	'phoneNumber' (data subblock)	when making money transfers by telephone number	If it is necessary to specify an additional value of the data field (number), specify one or more objects in the data sub-block 'phoneNumber"	
1.7.5.3.1	'number' (data field)	telephone number of the payee	In the **KKKXXXNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number shall be provided without a plus sign (+), spaces (_) and separation signs (-).	
1.7.5.4	'idNumber' (data subblock)	if the balance of electronic funds changes	If it is necessary to specify an additional value of the data field (number), specify one or more objects in the data sub-block 'idNumber'	
1.7.5.4.1	'number' (data field)	identification number of the payee, in particular, the number of the electronic wallet of the payee used by him on the basis of a bank account	textarea (text field)	

		agreement and (or) an agreement on the use of the electronic means of payment concluded with the money transfer operator		
1.8	'crossBorder' (data field)	cross-border banking identifier	One code is selected from the limited set of possible values: • **[CRB]** – cross-border transfer; • **[DOM]** – domestic transfer	
1.9	'additionalTransactionApprove' (data field)	identifier of additional transaction confirmation	One or more codes shall be selected from the limited set of possible values: • **[3DS]** – an operation was confirmed using 3D Secure; • **[DCS]** – implementation of technological measures to use separate technologies [3]; • **[NAA]** – an operation without confirmation; • **[SMS]** – an operation was confirmed using short text messages (SMS); • **[LTR]** – an operation was performed in accordance with the list of trusted payees; • **[TEL]** – an operation was confirmed by telephone; • **[OAA]** – other confirmation method -	

12.3. Information on technical data describing computer attacks against information infrastructure facilities of information exchange participants and their customers, as well as on relevant forms of electronic messages. Data Block **[IMPACTS]**

12.3.1. Computer attacks related to changes in route and address information **[trafficHijackAttacks]** (for [INT], [EXT] vector)

Data block (field) No.	Data block (field) identifier	Data block (field) content	Data field format	E-mail format
1.1	'legalAsPath' (data field)	Legal AS-Path	textarea (text field)	'impacts': { 'trafficHijackAttacks': [{ 'legalAsPath': 'Legal As-Path', 'wrongAsPath': 'wrongAsPath': 'lookingGlass': 'Reference to the Looking Glass used to verify AS-Path', 'legalPrefix': 'Legal prefix', 'wrongPrefix': 'wrongPrefix' }],
1.2	'wrongAsPath' (data field)	Wrong AS-Path	textarea (text field)	
1.3	'lookingGlass' (data field)	Reference to the Looking Glass used to verify AS-Path	textarea (text field)	
1.4	'legalPrefix' (data field)	Legal prefix	textarea (text field)	
1.5	'wrongPrefix' (data field)	Wrong prefix	textarea (text field)	

12.3.2. Computer attacks related to the use of malicious software at information infrastructure facilities of information exchange participants and their clients **[malware]** (for [INT], [EXT] vector)

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format
2.2	'sources' (data block)	identifiers of sources of malicious resources on the Internet with which the attacked object interacts	If it is necessary to specify several data field values (ip, domain, url), specify one or several objects in the data block 'sources'.	'malware': [{ 'sources': [{ 'ip': '127.0.0.1', 'domain': 'example.com', 'url': 'http://example.com' }], 'classifications': [{ 'vendorName': 'the name of the MCSE tool used by the information exchange participant', 'vendorVerdict': 'MC class in accordance with the MCSE tool used by the information exchange participant'
2.2.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	
2.2.2	'domain' (data field)	domain name	Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13]	

				}],
				'malwareSamples': [{
				'hash': {
				'md5': '4BA5139A444538479D9D750E2E2779BF',
				'sha1': ' D2B063763378A8CB38B192B2F71E78BC13783EFE ',
				'sha256': ' E25059612A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A9AE48FA4444'
				},
				'attachment': {
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'comment': 'comment to the attachment',
				'dateTimeAt': '2018-03-22T08:14:38Z',
				'file': {
				'name': 'file name',
				'size': 'file size in bytes',
				'base64': 'attachment in base64 format'
				},
				'fileLink': 'http://domain.com/archive.rar'
				}
				}],
				'malwareMessageSenders': [{
				'email': 'qwerty@example.ru',
				'server': '127.0.0.1'
				}],
				'malwareMessageAttachment': {
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'comment': 'comment to attachment', 'dateTimeAt': '2018-03-22T08:14:38Z',
				'file': {
				'name': 'file name',
				'size': 'file size in

2.2.3	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	
2.3	'classifications' (data block)	classification of malicious code	If it is necessary to specify several data field values (vendorName, vendorVerdict), specify one or several objects in the data block 'classifications'	
2.3.1	'vendorName' (data field)	name of the MCSE tool used by an information exchange participant	textarea (text field)	
2.3.2	'vendorVerdict' (data field)	MC class in accordance with the MCSE tool used by an information exchange participant	textarea (text field)	
2.4	'malwareSamples' (data block)	specify MC samples that may be characterised as a hash function or an attachment	If it is necessary to specify several values of data sub-blocks (hash, attachment), specify one or several objects in the data block 'malwareSamples'	
2.4.1	'hash' (data subblock)	MC sample as hash functions (hash functions MD5, SHA-1, SHA-256 are calculated for each MC sample)		
2.4.1.1	'md5' (data field)	MC sample as the MD5 hash function	The sequence of symbols obtained as a result of calculating the MD5 hash function	
2.4.1.2	'sha1' (data field)	MC sample as the SHA-1 hash function	The sequence of symbols obtained as a result of calculating the SHA-1 hash function	
2.4.1.3	'sha256' (data field)	MC sample as the SHA-256 hash function	The sequence of symbols obtained as a result of calculating the SHA-256 hash function	
2.4.2	'attachment' (data sub-block)	MC sample as a file		
2.4.2.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16]	

			assigned by the information exchange participant	bytes',
				'base64': 'attachment in base64 format'
				},
				'fileLink': 'http://domain.com/archive.rar'
				},
				'harmfulResourceAddress': [{ 'ip': '127.0.0.1',
				'domain': 'example.com',
				'url': 'http://example.com'
				}],
				'iocs': [{
				'net': [{
				'impact': 'type of detected compromising identifier',
				'comment': 'additional description'
				}],
				'fil': [{
				'impact': 'type of detected compromising identifier',
				'comment': 'additional description'
				}],
				'reg': [{
				'impact': 'type of detected compromising identifier',
				'comment': 'additional description'
				}],
				'prc': [{
				'impact': 'type of detected compromising identifier',
				'comment': 'additional description'
				}],
				'oth': [{
				'impact': 'type of detected compromising identifier',
				'comment': 'additional

2.4.2.2	'comment' (data field)	attachment description	textarea (text field)	
2.4.2.3	'dateTimeAt' (data field)	date and time when the file was added	data submission format in accordance with Specification RFC 3339 [11]	
2.4.2.4.1	'file' (data subblock)	additional materials containing MC samples	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding	
2.4.2.5	'fileLink' (data field)	additional materials containing MC samples	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]	
2.5	'malwareMessage Senders' (data block)	identifiers of electronic mailboxes from which a letter with the attached MC was received	If it is necessary to specify several data field values (email, server), specify one or several objects in the data block 'malwareMessage'	
2.5.1	'email' (data field)	sender's e-mail address	The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18]	
2.5.2	'server' (data field)	IP address of the last mail server	Logical IPv4 address shall comply with Specification RFC 791 [12]	
2.6	malwareMessage-Attachment (data sub-block)	source code file of an e-mail (if an MC was sent to an e-mail box)		
2.6.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant	
2.6.2	'comment' (data field)	attachment description	textarea (text field)	
2.6.3	'dateTimeAt' (data field)	date and time when the file was added	data submission format in accordance with Specification RFC 3339 [11]	

2.6.4.1	'file' (data block)	data file containing sn MC sample	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding	description' }] }], 'infectionMethod': [{ 'type': 'type of probable infection method', 'comment': 'comment to the selected type' }] }],
2.6.4.2	'fileLink' (data field)	link for obtaining (downloading) a data file containing MC samples	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]	
2.7	'harmfulResource- Address' (data block)	identifiers of a malicious resource from which the MC was downloaded	If it is necessary to specify several data field values (ip, domain, url), specify one or several objects in the data block 'sources.' 'harmfulResourceAddress'	
2.7.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	
2.7.2	'domain' (data field)	domain name	Domain name according to RFC 1034 specification [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13]	
2.7.3	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	
2.8	'iocs' (data block)	identified compromise indicators	If it is necessary to specify several values of data fields (net, fil, reg, prc, oth), specify one or several objects in the 'iocs' data block	
2.8.1	'net' (data subblock)	network indicators	If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the 'net' data block	
2.8.1.1	'impact' (data field)	type of compromising identifier detected	One code is selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion	

			-
2.8.1.2	‘comment’ (data field)	additional description	textarea (text field)
2.8.2	‘fil’ (data sub-block)	file indicators	If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the ‘fil’ data sub-block
2.8.2.1	'impact' (data field)	type of compromising identifier detected	One code is selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion
2.8.2.2	‘comment’ (data field)	additional description	textarea (text field)
2.8.3	‘reg’ (data sub-block)	OS register indicators	If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the ‘reg’ data block
2.8.3.1	'impact' (data field)	type of compromising identifier detected	One code is selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion
2.8.3.2	'comment' (data field)	additional description	textarea (text field)
2.8.4	‘prc’ (data sub-block)	indicators of OS processes	If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the ‘prc’ data sub-block

2.8.4.1	'impact' (data field)	type of compromising identifier detected	One code is selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion	
2.8.4.2	'comment' (data field)	additional description	textarea (text field)	
2.8.5	'oth' (data sub-block)	indicators not included in (2.8.1 - 2.8.4.2.)	If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the 'oth' data sub-block	
2.8.5.1	'impact' (data field)	type of compromising identifier detected	One code is selected from the limited set of possible values: • **[CRT]** – creation of technical data; • **[UPD]** – change in technical data; • **[DLT]** – technical data deletion	
2.8.5.2	'comment' (data field)	additional description	textarea (text field)	
2.9	'infectionMethod' (data block)	identifier of the assumed method of 'infection'	If it is necessary to specify several values of data fields (type, comment), specify one or several objects in the data block 'infectionMethod'	
2.9.1	'type' (data field)	type of probable infection method	One code is selected from the limited set of possible values: • **[EML]** – via e-mail channels; • **[DSD]** – from a storage medium; • **[LCL]** – distributed via a	

			local network; • **[OTH]** – other method	
2.9.2	‘comment’ (data field)	comment to the selected type	textarea (text field)	

12.3.3. Computer attacks that have been launched as a result of inducing clients to conduct money transfer transactions through deception or abuse of trust **[socialEngineering]** (for [EXT] vector)

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format

3.1	'soiTypes' (data field)	social engineering method identifiers	One or more codes shall be selected from the limited set of possible values:
			• **[MOB]** – a call from a mobile telephone number;
			• **[TPH]** – a call from a telephone number starting with 8-800;
			• **[SMS]** – an SMS message;
			• **[SNW]** – social engineering using social networks;
			• **[MSG]** – social engineering using instant messaging tools;
			• **[OTH]** – another way to implement social engineering methods
				‘socialEngineering’: {
				‘soiTypes’: [‘identifiers of social engineering methods']
				‘soiSenders’: [{
				‘phoneNumber’: ‘1212312345678’,
				‘email’: ‘qwerty@yandex.ru’,
				‘server’: ‘127.0.0.1’
				}],
				‘messageAttachment’: {
				‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
				‘comment’: ‘attachment description’, ‘datetimeAt’: ‘2018-03-22T08:14:38Z’,
				‘file’: {
				‘name’: 'file name',
				‘size’: 'file size in bytes',
				‘base64’: ‘attachment in base64 format’
				},
				‘fileLink’: ‘http://domain.com/archive.rar’
				},
				‘description’: 'additional description'
				},

3.2	'soiSenders' (data block)	social engineering implementation identifiers	If it is necessary to specify several data field values (phoneNumber, email, server), specify one or several objects in the data block ‘soiSenders’	
3.2.1	'phoneNumber' (data field)	telephone number	in the **KKKXXXNNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. A telephone number shall be provided without	

			a plus sign (+), spaces (_) and separation signs (-).	
3.2.2	'email' (data field)	e-mail address	The sender's e-mail address shall be provided in the format in accordance with RFC 5322 specification [18]	
3.2.3	'server' (data field)	IP address of the last mail server	Logical IPv4 address shall comply with RFC 791 specification [12]	
3.3	'message Attach-ment' (data block)	data files describing the social engineering method		
3.3.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with RFC 4122 specification [16] assigned by the information exchange participant	
3.3.2	'comment' (data field)	attachment description	textarea (text field)	
3.3.3	'dateTimeAt' (data field)	date and time when the file was added	data presentation format in accordance with RFC 3339 specification [11]	
3.3.4.1	'file' (data subblock)	data files describing the social engineering method	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding	
3.3.5	'fileLink' (data field)	data files describing the social engineering method	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with RFC 3986 specification [15]	
3.4	'description' (data field)	additional description	textarea (text field)	

12.3.4. Denial of service computer attacks (DDoS attacks) in relation to the information infrastructure of information exchange participants **[ddosAttacks]** (for [INT] vector)

Data block (field) number	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format

4.2	'attackType' (data block)	attack type		'ddosAttacks': [{
				'attackType': {
				'type': 'type of attack (by OSI levels)',
				'comment': 'additional description'

4.2.1	'type' (data field)	attack type (by OSI levels)	One code shall be selected from the limited set of possible values:	

			[1]– ‘L2/3: ICMP-flood’,
			[2]– ‘L2/3: NTP-amplification’,
			[3]– ‘L2/3: TFTP-amplification’,
			[4]– ‘L2/3: SENTINEL-amplification’,
			[5]– ‘L2/3: DNS-amplification’,
			[6]– ‘L2/3: SNMP-amplification’,
			[7]– ‘L2/3: SSDP-amplification’,
			[8]– ‘L2/3: CHARGEN-amplification’,
			[9]– ‘L2/3: RIPv1-amplification’,
			[10]– ‘L2/3: BitTorrent-amplification’,
			[11]– ‘L2/3: QTPD-amplification’,
			[12]– ‘L2/3: Quake-amplification’,
			[13]– ‘L2/3: LDAP-amplification’,
			[14]– ‘L2/3: 49ad34-amplification’,
			[15]– ‘L2/3: Portmap-amplification’,
			[16]– ‘L2/3: Kad-amplification’,
			[17]– ‘L2/3: NetBIOS-amplification’,
			[18]– ‘L2/3: Steam-amplification’,
			[19]– ‘L3: DPI-attack’,
			[20]– ‘L4: LAND-attack’,
			[21]– ‘L4: TCP-SYN-attack’,
			[22]– ‘L4: TCP-ACK-attack’,
			[23]– ‘L4: Smurf-attack’,
			[24]– ‘L4: ICMP/UDP-frag’,
			[25]– ‘L4: TCP-frag’,
			[26]– ‘L6: SSL-attack’,
			[27]– ‘L7: DNS Water Torture Attack’,
			[28]– ‘L7: Wordpress Pingback DDoS’,
				description' ‘sources’: [{
				‘ip’: ‘127.0.0.1’
				}],
				‘power’: {
				‘pps’: ‘number of packets per second’,
				‘mps’: ‘number of megabits per second’, ‘rps’: ‘number of requests per second’
				},
				‘startTimeAt’: ‘2018-03-22T08:14:38Z ‘, ‘endTimeAt’: ‘2018-03-22T08:14:38Z’,
				‘negativeImpact’: {
				‘type’: ‘type of negative impact’,
				‘comment’: 'additional
				}
				}],

			[29]– 'L7: DNS-flood', **[30]**– 'L7: HTTP/S-flood', **[31]**– 'L7: FTP-flood', **[32]**– 'L7: SMTP-flood', **[33]**– 'L7: VoIP/SIP-attack', **[34]**– 'L7: POP3-flood', **[35]**– 'L7: SlowRate-attack,' **[36]**– 'other'	
4.2.2	'comment' (data field)	additional description	textarea (text field)	
4.3	'sources' (data block)	identifiers of attack sources	If it is necessary to specify several values of the data field (ip), specify one or several objects in the data block 'sources'	
4.3.1	'ip' (data field)	IP address of an attack source (in case of a large number of computer attack sources in the block 'sources', the top 100 IP addresses of the attackers are specified, with the complete list attached in a text file)	Logical IPv4 address shall comply with Specification RFC 791 [12]	
4.4	'power' (data block)	attack power		
4.4.1	'pps' (data field)	number of packets per second	Packets per second	
4.4.2	'mps' (data field)	number of megabits per second	Megabit per second	
4.4.3	'rps' (data field)	number of requests per second	Request per second	
4.5	'startTimeAt' (data field)	attack start time	data provision format in accordance with Specification RFC 3339 [11].	
4.6	'endTimeAt' (data field)	attack end time	data presentation format in accordance with Specification RFC	

			3339 [11]	
4.7	‘negativeImpact’ (data block)	negative effect from an attack		
4.7.1	‘type’ (data field)	type of negative impact	One code should be selected from the limited set of possible values: • **[NAW]** – service availability interruption; • **[OTH]** – service degradation; • **[NCQ]** – service was not adversely affected	
4.7.2	‘comment’ (data field)	additional description	textarea (text field)	

12.3.5. Computer attacks related to unauthorised access to ATMs and payment terminals of information exchange participants **[atmAttacks]** (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format

5.1	‘target’ (data block)	identifier of object to be attacked object		‘atmAttacks’: {
				‘target’: {
				‘type’: ‘type of attack’, ‘description’: 'additional description’,
				},
				‘attackType’: [{
				‘type’: ‘type of attack depending on object under attack’,
				’description’’: 'additional description’
				}],
				‘attackImages’: {
				‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
				‘comment’: 'description of attachment', 'dateTimeAt': ‘2018-03-22T08:14:38Z’,
				‘file’: {
				‘name’: 'file name',
				‘size’: ‘file size in bytes’,

5.1.1	‘type’ (data field)	attacked object type	One code is selected from the limited set of possible values: • **[ATM]** is an ATM; • **[CIN]** is an ATM capable to accept cash; • **[REC]** is an ATM with a recycling function; • **[POS]** is a POS-terminal; • **[SST]** is a payment terminal; • **[OTH]** is other facility	
5.1.2	‘description’ (data field)	additional description	textarea (text field)	
5.2	'attackType' (data block)	attack type	If it is necessary to specify several values of data fields (type, description), specify one or several objects in the data block ‘sources’	

			-	'base64': 'attachment in base64 format' }, 'fileLink': 'http://domain.com/archive.rar' } },
5.2.1	'type' (data field)	type of attack depending on the target	One code is selected from the limited set of possible values: • **[BBX]** – blackbox attacks; • **[DSP]** – 'direct dispense' attacks and their variations; • **[SKM]** – skimming; • **[OTH]** – other method	
5.2.2	'description' (data field)	additional description	textarea (text field)	
5.3	attackImage (data block)	additional materials of attack launch		
5.3.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant	
5.3.2	'comment' (data field)	attachment description	textarea (text field)	
5.3.3	'dateTimeAt' (data field)	date and time when the file was added	data submission format in accordance with Specification RFC 3339 [11]	
5.3.4.1	'file' (data subblock)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding	
5.3.5	'fileLink' (data field)	link for obtaining (downloading) a data file containing additional materials	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]	

12.3.6. Computer attacks related to information infrastructure vulnerabilities of information exchange participants and their clients **[vulnerabilities]** (for vector [INT], [EXT])

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format

6.2	'sources' (data block)	identifiers of sources exploiting vulnerability	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block 'sources'	'vulnerabilities': [{
				'sources': [{
				'ip': '127.0.0.1',

				'url': 'http://example.com' }], 'identifier': 'vulnerability identifier', 'CVSS': 'CVSS metrics' }],
6.2.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	
6.2.2	'url' (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	
6.3	'identifier' (data field)	vulnerability identifier	If a vulnerability is detected, its type shall be specified in accordance with the classification of the FSTEC of Russia, CVE: • FSTEC of Russia - https://bdu.fstec.ru/vul; • Common Vulnerabilities and Exposures (CVE) – https://cve.mitre.org/data/downloads/all items.html	
6.4	'CVSS' (data field)	CVSS metrics	Specify the CVSS v 3.0 (The Common Vulnerability Scoring System (CVSS) if < * > is defined. Specify the maximum possible number of metrics listed as follows: basic metrics, temporary metrics, context metrics, and environment metrics. If no metrics are specified, use the FSTEC of Russia calculator – https://bdu.fstec.ru/cvss3	

12.3.7. Computer attacks related to searching (hacking) and compromising authentication data (login) data

[bruteForces] (for [INT] vector)

Data block (field) No.	Data block (field) identifier	Data block (field) content	Data field format	E-mail format

7.2	'sources'
	(data block)
		identification of attack sources	If it is necessary to specify several values of the data field (ip), specify one or several objects in the data block 'sources'	'bruteForces': [{
				'sources': [{
				'ip': '127.0.0.1 '
				}]
				}],

7.2.1	'ip'	IP address of the attack source	Logical IPv4 address shall	

	(data field)	(in the case of a large number of computer attack sources, the data block 'sources' shall contain the top 100 IP addresses of the attackers, with the complete list attached in a text file)	comply with Specification RFC 791 [12]	

12.3.8. Computer attacks related to spam mailings to information exchange participants and their clients **[spams]** (for [INT], [EXT] vector)

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format

8.1	'receivedAt' (data field)	date and time when a spam message was received	data submission format in accordance with Specification RFC 3339 [11]	'spams': [{
				'receivedAt': '2018-03-22T08:14:38Z',
				'sources': [{
				'ip': '127.0.0.1',
				'domain': 'example.com', 'email': 'qwerty@example.ru'
				}],
				'spamImages': {
				'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
				'comment': 'comment to attachment', 'dateTimeAt': '2018-03-22T08:14:38Z',
				'file': {
				'name': 'file name',
				'size': 'file size in bytes',
				'base64': 'attachment in base64 format'
				},
				'fileLink': 'http://domain.com/archive.rar'
				}
				}],

8.2	'sources' (data block)	attack source identifiers (spam senders)	If it is necessary to specify several data field values (ip, domain, email), specify one or several objects in the data block 'sources'	
8.2.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	
8.2.2.	'domain' (data field)	domain name	Domain name according to RFC 1034 specification [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13]	
8.2.3	'email' (data field)	email address of a spam message sender	The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18]	
8.3	'spamImage' (data block)	sample spam message		
8.3.1	'sourceId' (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with	

			Specification RFC 4122 [16] assigned by the Bank of Russia participant	
8.3.2	‘comment’ (data field)	attachment description	textarea (text field)	
8.3.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]	
8.3.4	'file' (data block)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding	
8.3.5	'fileLink' (data field)	link for obtaining (downloading) a data file containing additional materials	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]	

12.3.9. Computer attacks related to detecting the interaction of information infrastructure facilities of information exchange participants with Botnet command centres **[controlCenters]** (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format

9.2	'hostUrl' (data field)	URL hosting the Botnet Command Centre	URL in accordance with Specification RFC 3986 [15]	‘controlCenters’: [{
				‘hostUrl’:
				‘http://example.com ‘,
				‘intruderIp’: ‘1.1.1.1’,
				‘intruderActions’: ‘what preceded the incident’,
				‘description’: ‘additional description of the Botnet command centre’,
				‘nodes’: [{
				‘ip’: ‘127.0.0.1’,
				‘lastRequestRateTime’: ‘2018-03-22T08:14:38Z ‘
				}]
				}],

9.3	'intruderIp' (data field)	IP address of the attacker who hosted the Botnet Command Centre	Logical IPv4 address shall comply with Specification RFC 791 [12]	
9.4	'intruderActions' (data field)	description of unauthorised activity in the information infrastructure of an information exchange participant	textarea (text field)	
9.5	‘description’ (data field)	additional description Botnet command centre	textarea (text field)	
9.6	'nodes' (data block)	identifiers of the access to the Botnet command centre	If it is necessary to specify several data field values (ip, lastRequestRateTimeAt), specify one or several objects in the data block	
9.6.1	‘ip’	external IP address	Logical IPv4 address shall comply with	

	(data field)	(of an information exchange participant)	Specification RFC 791 [12]	
9.6.2	'lastRequest RatetimeAt' (data field)	date and time of the last interaction with the Botnet command centre	data submission format in accordance with Specification RFC 3339 [11]	

12.3.10. Computer attacks related to a change (substitution) of the mobile subscriber identifier (IMSI) of the SIM card number, as well as the replacement of the mobile equipment identifier (IMEI) **[sim]** (for [EXT] vector)

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format
9.1	'mobileOperator' (data field)	mobile telecom operator name	textarea (text field)	'sim': { 'mobileOperator': 'name of mobile telecom operator', 'phoneNumber': '1212312345678', 'imsi': 'unique sim card number', 'imsiChangedAt': '2018-03-22T08:08:49Z ' },
9.2	'phoneNumber' (data field)	mobile telephone number	In the **KKKXXXNNNNNNNN** format, where: **KKK** – a country code of one to three characters; **XXX** – operator's code; **NNNNNNN** - seven characters of the number. The telephone number shall be provided without a plus sign (+), spaces (_) and separation signs (-).	
9.3	'imsi' (data field)	unique SIM card number (imsi number)	**XXXXXXXXXXXXXX**	
9.4	'imsiChangedAt' (data field)	date and time when the IMSI change was recorded	data submission format in accordance with Specification RFC 3339 [11]	

12.3.11. Computer attacks related to the dissemination of information related to offers and/or provision of financial services in the Russian Federation by persons not entitled to provide them in accordance with the legislation of the Russian Federation. Posting prohibited content on the Internet **[prohibitedContents]**(for [EXT], [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format

12.1	‘sources’ (data block)	identifiers of prohibited content sources	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block ‘target’	‘prohibitedContents’: [{
				‘sources’: [{
				‘ip’: ‘127.0.0.1’,
				‘url’: ‘http://example.com ‘
				}],
				‘type’: 'type of content'
				}],

12.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	
12.1.2	‘url’ (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	
12.2	‘type’ (data field)	prohibited content type	textarea (text field)	

12.3.12. Computer attacks related to information that misleads information exchange participants and their clients, as well as other persons interacting with them, about the ownership of the information disseminated via the Internet due to the similarity of domain names, design or content. Phishing **[phishingAttacks]** (for [EXT], [INT] vector)

Data block (field) No.	Data block (field) identifier	Content of data block (field)	Data field format	E-mail format

11.2	‘harmful’ (data block)	phishing resource source identifiers	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block ‘harmful’	‘phishingAttacks’: [{
				‘harmful’: [{
				‘ip’: ‘127.0.0.1’,
				‘url’: ‘http://example.com’
				}],
				‘fixationAt’: ‘2018-03-22T08:14:38Z’,
				‘messageAttachment’: {
				‘sourceId’: ‘f34030ef-358a-445c-8567-
				25985ce6d91c’,
				‘comment’: ‘attachment description’,

11.2.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	
11.2.2	‘url’ (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	

11.3	‘fixationAt’ (data field)	date and time of phishing message recording	data submission format in accordance with Specification RFC 3339 [11]	‘dateTimeAt’: ‘2018-03-22T08:14:38Z‘,
				‘file’: {
				‘name’: 'file name',
				‘size’: 'file size in bytes',
				‘base64’: 'attachment in base64 format'
				},
				‘fileLink’: ‘http://domain.com/archive.rar’
				}
				}],

11.4	‘message Attachment’ (data block)	phishing message sample		
11.4.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant	
11.4.2	‘comment’ (data field)	attachment description	textarea (text field)	
11.4.3	'dateTimeAt' (data field)	date and time when the file was added	data submission format in accordance with Specification RFC 3339 [11]	
11.4.4.1	'file' (data block)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding	
11.4.5	'fileLink' (data field)	link for obtaining (downloading) a data file containing additional materials	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]	

12.3.13. Computer attacks related to the placement on the Internet of information enabling illegal access to information systems of information exchange participants and their customers used in the provision (receipt) of financial services, including through illegal access to confidential customer information. Posting a malicious resource on the Internet **[prohibitedContents]** (for [EXT], [INT] vector)

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format

13.1	‘sources’ (data block)	malicious resource source identifiers	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block ‘target’	‘maliciousResources’: [{
				‘sources’: [{
				‘ip’: ‘127.0.0.1’,
				‘url’: ‘http://example.com’
				}],
				‘activityType’: ‘type of malicious activity’
				}],

13.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	

13.1.2	‘url’ (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	
13.3	‘activityType’ (data field)	type of malicious activity	textarea (text field)	

12.3.14. Computer attacks related to a change in the content [changeContent] (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format

14.1	‘targets’ (data block)	identifiers of attacked objects which content was changed	If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block ‘target’	‘changeContent’: [{
				‘targets’: [{
				‘ip’: ‘127.0.0.1’,
				‘url’: ‘http://example.com’
				}],
				‘type’: ‘type of changed content’
				}],

14.1.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	
14.1.2	‘url’ (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	
14.2	‘type’ (data field)	type of changed content	textarea (text field)	

12.3.15. Computer attacks related to the scanning of software ports of information infrastructure facilities of information exchange participants by persons not authorised to do so **[scanPorts]** (for [INT] vector)

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format

15	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant	‘scanPorts’: [{
				‘sources’: [{
				‘ip’: ‘127.0.0.1’
				}],
				‘ports’: [‘23’],
				‘method’: ‘information on scanning methods or software used for this purpose’,
				‘startTimeAt’: ‘2018-03-22T08:14:38Z’, ‘endTimeAt’: ‘2018-03-22T08:14:38Z’
				}],

15.2	‘sources’ (data block)	malicious activity source identifiers	If it is necessary to specify several values of the data field (ip), specify one or several objects in the data block ‘sources’	
15.2.1	‘ip’ (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791	

			[12]	
15.3	‘ports’ (data field)	port numbers that have been scanned	textarea (text field)	
15.4	'method' (data field)	information on scanning methods or software used for this purpose	textarea (text field)	
15.5	'startTimeAt' (data field)	scan start time	data provision format in accordance with Specification RFC 3339 [11]	
15.6	'end time' (data field)	scan end time	data provision format in accordance with Specification RFC 3339 [11]	

12.3.16. Other computer attacks against information infrastructure facilities of information exchange participants and their clients **[other]** (for [INT], [EXT] vector)

16.1	‘description’ (data field)	description of a computer attacked object	textarea	‘other’: { ‘description’: ‘computer attack description’, ‘target’: { ‘ip’: ‘127.0.0.1’, ‘url’: ‘http://example.com ‘ }, ‘type’: ‘type of content’, ‘attachment’: { ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’, ‘comment’: ‘comment to attachment’, ‘dateTimeAt’: ‘2018-03-22T08:14:38Z’, ‘file’: { ‘name’: 'file name', ‘size’: 'file size in bytes', ‘base64’: 'attachment in base64 format' }, ‘fileLink’: ‘http://domain.com/archive.rar’ } }
16.2	‘source’ (data block)	identifiers of another source of malicious, prohibited content /resource		
16.2.1	'ip' (data field)	IP address	Logical IPv4 address shall comply with Specification RFC 791 [12]	
16.2.2	‘url’ (data field)	URL-address	URL in accordance with Specification RFC 3986 [15]	
16.2.3	‘type’ (data field)	other type of prohibited, malicious, modified content	textarea (text field)	
16.3	'attachment' (data block)	additional data to identify a computer attack		
16.3.1	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant	
16.3.2	‘comment’	attachment description	textarea (text field)	

	(data field)			},
16.3.3	'dateTimeAt' (data field)	date and time when the file was added	data submission format in accordance with Specification RFC 3339 [11]	
16.3.4	'file' (data block)	data file containing additional materials	Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding	
16.3.5	'fileLink' (data field)	link for obtaining (downloading) a data file containing additional materials	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]	

12.4. Technical recommendations of the information bulletin **[signatures]**

Data block (field) No.	Identifier of data block (field)	Data block (field) content	Data field format	E-mail format

2.1	'mainActions' (data field)	recommended measures to counter computer attack	textarea (text field)	'mainActions': 'recommended measures to counter computer attack',
				'signatures': [{
				'identifier': 'signature identifier', 'yara': 'yara-rule',
				'snort': ['rule1','rule2']
				}]
				}

2.2	'signatures' (data block)	signature	If it is necessary to specify several data field values (identifier, yara, snort), specify one or several objects in the data block 'source'	
2.3	'identifier' (data field)	unique signature identifier	sequence of symbols obtained as a result of calculating the MD5 hash function	
2.4	'yara' (data field)	YARA-rule	textarea (text field)	
2.5	'snort' (data field)	Snort-rules	submission format in the form of: <Action > <Protocol> <IP addresses of senders> <Senders' ports> <Destination operator> <IP addresses of recepients> <Recipient ports> (key_1: value_1; key_2: value_2;.. key_n: value_n;)	

13. The form of data submission used by information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violations of data protection requirements and timeframes for their submission to the Bank of Russia

13.1. Mandatory conditions and time characteristics of information provision

Mandatory information conditions:

[O] – data block (field) information shall be provided as required;

[N] – data block (field) information shall be provided if it is technically feasible. Time characteristics of information provision (stages of information provision):

[1] – data block (field) information shall be provided by an information exchange participant as part of the initial notification no later than one business day before the incident disclosure event;

[2] – data block (field) information shall be provided by an information exchange participant as part of the subsequent notification if information on possible incident disclosure is changed.

13.2. Identification data on planned measures to disclose information about incidents. Data block **[HEADER]**

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision
1.1	'schemaType' (data field)	type of electronic message	Specify the value of [PUB] – publication	{ 'header': { 'schemaType': 'pub', 'schemaVersion': '1', 'version': '1', 'memberId':'9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId':'f34030ef-358a-445c-8567-25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z',	[O]	[1], [2]
1.2	'schemaVersion' (data field)	electronic message type scheme version	textarea (text field)		[O]	[1], [2]
1.3	'version'	version number of an electronic	numeric value (int)		[O]	[1], [2]

	(data field)	message during information exchange		‘modifiedAt’: ‘2002-10-02T15:00:00.05Z’ },		
1.4	‘memberId’ (data field)	information exchange participant identifier assigned by the Bank of Russia	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia		[O]	[1], [2]
1.5	‘sourceId’ (data field)	identifier assigned by an information exchange participant	128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant -		[O]	[1], [2]
1.6	‘publishedAt’ (data field)	date and time of initial provision of information	data provision format in accordance with Specification RFC 3339 [11]		[O]	[1], [2]
1.7	‘modifiedAt’ (data field)	date and time of providing interim information	data provision format in accordance with Specification RFC 3339 [11]		[O]	[2]

13.3. Description of planned measures to disclose information about incidents. Data block **[PUB]**

Data block (field) No.	Identifier of data block (field)	Content of data block (field)	Data field format	E-mail format	Obligation of informing	Stages of information provision

2.1	‘orgName’ (data field)	name of the organisation that is an information exchange participant	textarea (text field)	‘pub’: {
				‘orgFullName’: ‘full name of an information exchange participant’,
				‘persons’: [{
				‘lastName’: ‘last name’,
				‘middleName’: ‘patronymic name’,
					[O]	[1], [2]

2.2	‘persons’	contact data	If it is necessary to		[O]	[1], [2]

	(data block)	of the responsible person	indicate several values of data fields (lastName, middleName, firstName, landlineNumber, mobileNumber, email, position, eventScheduledAt) specifies one or several objects in the block of data 'persons'	'firstName': 'name', 'landlineNumber': 'stationary phone', 'mobileNumber': 'mobile phone', 'e-mail': 'e-mail address', 'position': 'position' }], 'eventScheduledAt': '2002-10-02T15:00:00.05Z', 'location': { 'subjectOfFederation': '00', 'locality': 'residential area name' }, 'description': 'additional data on the event', - 'typeOfActivity': ['type of planned event'], 'nameOfActivity': name of the planned event or resource where information is to be disclosed', 'text': 'text for the planned event', 'messageAttachment': { 'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c', 'comment': 'description of attachment', 'dateTimeAt': '2018-03-22T08:14:38Z ', 'file': { 'name': 'file name', 'size': 'file size in bytes', 'base64': 'attachment in Base64 formate' }, 'fileLink': ' http://domain.com/archive.rar ' } } }		
2.2.1	'lastName' (data field)	surname	textarea (text field)		[O]	[1], [2]
2.2.2	'middleName' (data field)	middle name	textarea (text field)		[O]	[1], [2]
2.2.3	'firstName' (data field)	name	textarea (text field)		[O]	[1], [2]
2.2.4	'landlineNumber' (data field)	stationary telephone	textarea (text field)		[O]	[1], [2]
2.2.5	'mobileNumber' (data field)	mobile telephone	textarea (text field)		[O]	[1], [2]
2.2.6	'email' (data field)	e-mail address	The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18]		[O]	[1], [2]
2.2.7	'position' (data field)	position	textarea (text field)		[O]	[1], [2]
2.3	'eventScheduledAt (data field)	date and time of the planned event (speech) or publication of information on incidents	data provision format in accordance with Specification RFC 3339 [11]		[O]	[1], [2]
2.4	'location' (data block)	event (speech) location			[O]	[1], [2]

2.4.1	‘subjectOfFedera- (data field)	upper-level OKTMO code	textarea (text field)		[O]	[1], [2]
2.4.2	'locality' (data field)	name of a residential area	textarea (text field)		[O]	[1], [2]
2.5	‘description’ (data field)	additional data on the event	textarea (text field)		[O]	[1], [2]
2.6	‘typeofActivity’ (data field)	type of the planned event	One or more codes should to be selected from the limited set of possible values: • **[CNF]** – conference; • **[PBE]** – publication using an external resource (including printed publications); • **[PBI]** – publication on the information exchange participant's own resource (including printed publications)		[O]	[1], [2]
2.7	‘nameofActivity’ (data field)	name of the planned event or resource where information is to be disclosed	textarea (text field)		[O]	[1], [2]
2.8	'text' (data field)	text to the planned event	textarea (text field)		[O]	[1], [2]
2.9	‘messageAttachm e nt’ (data block)	description of the information being disclosed			[N]	[1], [2]
2.9.1	‘sourceId’ (data field)	identifier assigned by an information exchanged participant	128-bit identifier (GUID) generated in accordance with		[N]	[1], [2]

			Specification RFC 4122 [16] assigned by an information exchange participant			
2.9.2	‘comment’ (data field)	attachment description	textarea (text field)		[N]	[1], [2]
2.9.3	'dateTimeAt' (data field)	date and time when the file was added	data provision format in accordance with Specification RFC 3339 [11]		[N]	[1], [2]
2.9.4	'file' (data block)	data file	Specify the name and size of the file (no more than 5 MB) and perform encoding in Base64 formate		[N]	[1], [2]
2.9.5	'fileLink' (data field)	reference link for obtaining (downloading) a data file containing additional materials	Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15]		[N]	[1], [2]

14. Conditions for information exchange participants to submit to the Bank of Russia data on detected incidents related to violation of data protection requirements

14.1. Informing the Bank of Russia about revealed events of the type:

[MTR_WC] means the receipt by the money transfer operator serving the payer, including the electronic money operator, of notifications in the form stipulated by the agreement from customers which include individuals, legal entities, individual entrepreneurs or individuals engaged in private businesses about cases and (or) attempts to transfer funds without the customer's consent, including about the use of electronic payment instruments;

[A_SC] means the receipt by the payment system settlement centre notifications from payment system participants about debiting funds from their correspondent accounts without their consent and/or using distorted information contained in the instructions of payment clearing centres or payment system participants;

[UO_WC] means the identification by the money transfer operator serving the payer, including the electronic money operator, of transactions with signs of a money transfer without the customer's consent as established by the Bank of Russia and posted on the Bank of Russia website;

[FMA_WC] means the receipt of notifications from customers which include individuals, and (or) individual entrepreneurs, and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation, and (or) legal entities about an illegal financial transaction;

[MTR_UA] means the identification by the money transfer operator serving the payer, including the electronic money operator, of money transfer operations and cash receipts as a result of unauthorised access to the information infrastructure of the money transfer operator, including when the balance of electronic funds is reduced, except for virtual payment cards;

[FMS_UA] means the identification of illegal financial transactions conducted as a result of unauthorised access to information infrastructure facilities of a non-bank financial institution;

[**UPT_PSP]** means an unauthorised withdrawal of funds of the money transfer operator at ATMs;

[DT_ALL] means a failure to provide services by the money transfer operator for more than two hours in total for all constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) remote banking systems (funds);

[DT_SEL] means a failure to provide services by the money transfer operator for more than two hours in total for individual constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) remote banking system (s);

[UPT_EMP] means an unauthorised withdrawal of funds of the electronic money operator at ATMs;

[DT_SC] means that a settlement centre has failed to provide settlement services for more than one operational day;

[DTPT_SC] means a failure by a settlement centre to make payments during an operational day against orders of a payment clearing centre or payment system participants accepted for execution;

[DT_CC] means the termination by a clearing centre in providing payment clearing services for a period of more than one operational day;

[DTPT_CC] means a clearing centre's failure to clear a payment subject to the accepted orders of payment system participants during one operational day;

[DT_OC] means the suspension by an operational centre of the provision of operational services for a period of more than two hours;

[DT_FS_ALL] means a financial institution's failure to provide services for more than two hours in total for all constituent territories of the Russian Federation where the financial institution provides financial services;

[DT_FS_ALL] means a financial institution's failure to provide services for more than two hours in total for individual constituent territories of the Russian Federation where the financial institution provides financial services;

shall be carried out for each event separately.

14.2. Identification by an information exchange participant of computer attacks which may lead to the events specified in Clause 14.1:

[PSP_CMTR] means the detection by the money transfer operator, including the electronic money operator, and/or the payment infrastructure service provider of attacks the consequences of which may lead to events and attempts of making money transfers without their customer's consent;

[CO_CFS] means the detection by a credit institution of computer attacks, the consequences of which may lead to events and attempts to carry out a financial (banking) transaction without its customer's consent;

[NCFI_CFS] means the detection by a non-bank financial institution of computer attacks, the consequences of which may lead to events and attempts to carry out a financial (banking) transaction in the financial market without its customer's consent;

To be done according to the following criteria (V is the information provision criterion):

Objects of computer attacks	Types of computer attacks															
	detection of a computer attack on the external perimeter of the information infrastructure	detection of a computer attack on the internal or external perimeter of the information infrastructure							detection of a computer attack on the internal perimeter of the information infrastructure		detection of a computer attack against customers or employees of an information exchange participant		detection of a computer attack against payment infrastructure elements	other types of attacks		
System levels	[ddos Attacks]	[traffic Hijack Attacks]	[vulner abili-ties]	[spams]	[phishing Attacks]	[mali-cious Resources]	[mal-ware]	[control Centers]	[brute Forces]	[scan-Ports]	[socialEn-gineering]	[sim]	[atm Attacks]	[prohibited Content]	[change Content]	[other]
[hw] – hardware	V		V				V		V	V		V	V			V
[net] - network equipment	V	V	V			V	V	V	V	V						V
[net_s] – network applications and services	V		V				V									V
[hw_s] – virtualisation server components, software infrastructure	V	V	V				V	V								V
[os] – operating systems, database management systems, application servers	V		V				V	V								V
The level of AS and applications operated for the provision of	[ddos Attacks]	[traffic Hijack At-	[vulner abili-	[spams]	[phishing Attacks]	[malicious Re-	[mal-ware]	[control Centers]	[brute Forces]	[scan Ports]	[social Enginee r-	[sim]	[atm Attacks]	[prohi-bited	[change Content]	[other]

services within business or technological processes of an information exchange participant		**tacks]**	**ties]**			**sources]**				**ing]**			**Content s]**		
[rbs] – a remote banking system	V		V				V		V	V					V
[front-office] – a payment card transaction processing system	V		V				V		V	V			V		V
[web] – Internet information resources	V						V		V	V					V
[abs] – an automated banking system	V		V				V		V	V					V
[back-office] – a system for post-transaction servicing of payment card transactions	V		V				V		V	V					V
[int-services] – internal information infrastructure for supporting the business processes of an information exchange participant (mail servers, file servers)			V		V	V	V	V	V	V					V

[participant_w] means terminal equipment (automated workstation) used by employees of an information exchange participant			V	V							V	V		V	V	V
The level of AS and applications operated by an information exchange participant's client	**[ddos Attacks]**	**[traffic Hijack At-tacks]**	**[vulne - rabili-ties]**	**[spams]**	**[phish-ing Attacks]**	**[mali-cious Resour ces]**	**[mal-ware]**	**[control Centers]**	**[brute Forces]**	**[scan Ports]**	**[social Enginee ring]**	**[sim]**	**[atm Attacks]**	**[prohi-bited Content s]**	**[change Content**	**[other]**
[cfs] – a file server		V	V				V									V
[crbs] – a remote banking system	V	V	V				V									V
[ecs] – an e-mail account					V	V	V									V
[client_w] – an automated systems used by employees of an information exchange participant's client			V								V	V		V	V	V
Other system	**[ddos Attacks]**	**[traffi c Hijac k At-tacks]**	**[vulne r-abili-ties]**	**[spam s]**	**[phishi ng Attack s]**	**[mali-ciousR e-source s]**	**[mal-ware]**	**[contro Centers**	**[brute Forces**	**[scan Ports]**	**[social Engine ering]**	**[sim]**	**[atm Attacks]**	**[prohib ited Conten ts]**	**[chang Conten**	**[other]**
[oth] – other system	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V

14.3. Assessment of the severity of consequences of an incident. When informing the Bank of Russia about identified incidents related to a violation of information protection requirements by an information exchange participant, it is necessary to make a relative (qualitative) assessment of the scale (severity of consequences) of the occurrence of data protection events in accordance with the following criteria:

№	Code and type of the event	Characteristics of the scale of consequences of the occurrence of the event as a whole	Threshold values		
			Moderate **[MOD]**	Essential **[ESS]**	Critical **[CRIT]**
1	**[UPT_PSP]** – unauthorised withdrawal of funds of the money transfer operator at ATMs	The amount of debited (withdrawn) funds, rubles	1,400,000	5,000,000	15,000,000
		The number of unauthorised access events, units	100	500	1,000
		The amount of operational expenses of the money transfer operator as a result of debits (withdrawals) of funds, rubles	2,000,000	10,000,000	25,000,000
2	**[DT_ALL]** – a failure by the money transfer operator to provide services for a period of more than two hours in total to individual constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) a remote banking system (s); **[DT_SEL]** – a failure by the money transfer operator to provide services for a period of more than two hours in total to individual constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) a remote banking system (s);	The number of events related to non-provision of money transfer services, unit	-	-	1
		A region of non-provision of money transfer services, constituent territories of the Russian Federation -	2	5	10
3	**[UPT_EMP]** – unauthorised withdrawal of funds of the e-money operator at ATMs	The amount of a decrease in the electronic money balance, rubles	100,000	500,000	1,000,000
		The number of unauthorised access events, units	100	500	1,000
		The amount of operating expenses of the electronic money operator as a result of the decrease in the electronic money balance, rubles	500,000	1,500,000	5,000,000

4	**[DT_SC]** means that a settlement centre has failed to provide settlement services for more than one operational day; **[DTPT _ SC]** means a settlement centre's failure to conduct payment transactions during an operational day as per accepted orders of a payment clearing centre or payment system participants	The number of events related to the non-provision of settlement services, units	3	5	10
5	**[DT_CC]** means the termination by a clearing centre in providing payment clearing services for a period of more than one operational day; **[DTPT_CC]** means a settlement centre's failure to clear payments during an operational day according to accepted orders of payment system participants	The number of events related to non-provision of payment clearing services, units	3	5	10
6	**[DT_OC]** means the suspension by an operational centre of the provision of operational services for a period of more than two hours	The number of events related to non-provision of operational Services, units	3	5	10
7	**[DT_FS_ALL]** means a non-bank financial institution's failure to provide services for more than two hours in total to all constituent territories of the Russian Federation where this non-bank financial institution provides financial services; **[DT_FS_ALL]** means a non-bank financial institution's failure to provide services for more than two hours in total to individual constituent territories of the Russian Federation where this non-bank financial institution provides financial services	The number of events related to non-provision or untimely provision of financial services, units A region of non-provision of money transfer services, units	3	5	10

15. Description of the technology for preparing and sending electronic messages during information exchange with the Bank of Russia

15.1. Electronic message preparation technology[1]

15.1.1. An electronic message shall be prepared using:

- personal account of the participant (https://lk.fincert.cbr.ru);
- a specialised application installed by an information exchange participant (hereinafter, the desktop application);[2]

15.1.2. The personal account of an information exchange participant makes it possible to generate an electronic message by filling in the on-line form for sending data in accordance with the provisions of this standard.

15.1.3. The desktop application makes it possible to generate an electronic message by filling in the application form for sending data to the FINCERT ASIP (Automated System of Incident Processing)

15.2. Electronic messaging technology[3]

Information is transmitted via the Bank of Russia's information resources on the Internet by providing information exchange participants with access to their personal accounts (https://lk.fincert.cbr.ru).

Backup methods of information transmission to the Bank of Russia are used by an information exchange participant only in cases when the personal account of the information exchange participant does not have telecommunication accessibility and (or) it is not technically feasible to transmit information.

Backup methods of information transmission include:

- use of e-mail (fincert@cbr.ru);
- telephone calls to the Bank of Russia (+ 7 (495) 772 70 90).[4]

---

[1] The protection of the transmitted information is implemented using the certified CIPF established in accordance with document BCMD.42 5790.520.I3.2 'Participant's Manual for Working with FinCERT ASIP' (using the certified CIPF 'Continent-TLS'), The participant who sends information to FinCERT shall be identified and authenticated on the basis of information transmitted to FinCERT (information about the participant).

[2] It is transferred to FinCERT as part of the participant's package when the exchange participant is connected to the ASIP (when updating the application, its versions are posted on the FinCERT specialised ASIP portal – https://portal.fincert. Cbr.ru in the section 'FinCERT ASIP (Participant Documentation and Software)'). Access to the FinCERT ASIP specialised portal without the installation of a certified CIPF is not provided.

[3] The protection of the transmitted information is implemented using the certified CIPF established in accordance with document BCMD.42 5790.520.I3.2 'Participant's Manual for Working with FinCERT ASIP' (using the certified CIPF 'Continent-TLS'), The participant who sends information to FinCERT shall be identified and authenticated on the basis of information transmitted to FinCERT (information about the participant).

[4] Voice data are not protected. The caller is identified by interviewing him/her regarding the name of his/her organisation, full name, position and contact telephone number, which are compared with the participant's card.

15.2.1. When transmitting information via e-mail, it is necessary to indicate the subject matter of the message and the accompanying text with attaching the following files:

- the electronic message generated in accordance with Section 15.1 hereof;
- other files, the maximum size of which should not exceed 25 MB (if the specified size is exceeded, it is allowed to send files in several parts with archiving them in several emails).

15.2.2. When transmitting information using the personal account of an information exchange participant, fields marked 'required to be filled' with the possibility of adding attachments of up to 2 GB shall be filled in;

15.2.3. If samples of malicious software (viruses) are sent to the Bank of Russia for investigation, they shall be transmitted to the archive (rar or zip) with one of the following passwords: 'virus' or 'infected'. If the password is not set in the transferred archive, it is deleted automatically.

Annex 1. Schemes of interaction between an information exchange participant and the Bank of Russia

Data submission form used by information exchange participants for registration with the Bank of Russia	Form of data submission used by information exchange participants to inform the Bank of Russia about incidents related to violation of data protection requirements and deadlines for their submission to the Bank of Russia	Form of data submission used by information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violation of data protection requirements and timeframes for their submission to the Bank of Russia	Data submission form used by information exchange participants to provide a response to the Bank of Russia's request to the information exchange participant serving the payee and the timeframes for their submission to the Bank of Russia	Data submission form used by information exchange participants to submit a request to the Bank of Russia on the establishment of a restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on the debiting of funds in case of revealed incidents related to violation of data protection requirements
{ 'header': { 'schemaType': 'participant', 'schemaVersion': '1', 'version': '1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567- 25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z', 'modifiedAt': '2002-10-	{ 'header': { 'schemaType': 'incident', 'schemaVersion': '1', 'version':'1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef- 358a-445c-8567-25985ce6d91c', 'publishedAt': '2002- 10-02T15:00:00.05Z', 'modifiedAt': '2002-10-02T15:00:00.05Z' }, 'incident': { 'fincertId': '20180324215113',	{ 'header': { 'schemaType': 'pub', 'schemaVersion': '1', 'version':'1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567- 25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z', 'modifiedAt': '2002-10-02T15:00:00.05Z' }, 'pub': {	{ 'header': { 'schemaType': 'sche-maType': 'anifraudResponse', 'schemaVersion': '1', 'version':'1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567- 25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z' }, 'anifraudResponse': [{ 'sourceId': 'f34030ef-358a-445c-8567-	{ 'header': { 'schemaType': 'lockRequest', 'schemaVersion': '1', 'version':'1', 'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'sourceId': 'f34030ef-358a-445c-8567- 25985ce6d91c', 'publishedAt': '2002-10-02T15:00:00.05Z' }, 'lockRequest': [{ 'sourceId': 'f34030ef-358a-445c-8567- 25985ce6d91c', 'orgBik': '123456789',

```
02T15:00:00.05Z’
        },
        ‘participant’: {
            ‘orgId’: 'identifier of the type of the information exchange participant',
            ‘orgBrand’: 'brand name of the information exchange participant',

            ‘orgShortName’: 'short name of the information exchange participant',

            ‘orgFullName’: 'full name of the information exchange participant',
            ‘orgE-mails’: [‘qwerty1@example.ru’,
                ‘qwer- ty2@example.ru’],
            ‘orgIncomingEmail’: ‘requestsFromfincert@example.ru’,
            ‘orgBik’: ‘123456789’,
            ‘orgLegalEntityForm’: ‘12345’,
            ‘orgBin’: [‘123456’, ‘123456’],
            ‘orgInn’: ‘1234567890’,
```

```
            ‘fixationAt’: ‘2002-10-02T15:00:00.05Z’,
            ‘description’: 'incident description',
            ‘lawEnforcementRequest’: {
                ‘addressed’: 'a subject who has applied to law enforcement agencies',
                ‘request’: 'information on the fact of an information exchange participant's appeal to the police',
                ‘number’: 'application number from the register of crime reports',
                ‘numberTicket’: 'the ticket number for accepting and registering the application',
                ‘dateTimeAt’: 'date and time of the application acceptance'
            },
            ‘assistance’: 'identifier of the need to support the information exchange participant by the Bank of Russia',
            ‘vectorCode’: 'computer attack vector identifier',
            ‘serviceType’: [{
                ‘sourceId’: ‘f34030ef-358a-445c-8567-25985av6d91c’,
                ‘type’: 'type of the object under attack'
```

```
            ‘orgFullName’: 'full name of the information exchange participant',
            ‘persons’: [{
                ‘lastName’: ‘last name’,
                ‘middleName’: ‘patronymic name’,
                ‘firstName’: ‘name’,
                ‘landlineNumber’: 'stationary telephone',
                ‘mobileNumber’: 'mobile telephone,'
                ‘email’: 'e-mail address',

                ‘position’: 'position'
            }],
            ‘eventScheduledAt’: ‘2002-10- 02T15:00:00.05Z’,
            ‘location’: {
                ‘subjectOfFederation’: ‘00’,

                ‘locality’: 'residential area name'
            },
            ‘description’: 'additional data on the event',
```

```
25985ce6d91c’,
            ‘victim’: 'information on the legal status of the payer',
            ‘recipient’: 'information on the legal status of the recepient of funds',
            ‘payeeIdentifier’: {

                ‘hash’: ‘P79969612A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA441E11’,

                ‘hashSnils’: ‘B49087832A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA441E44’
            },
            ‘payer’: {
                ‘bik’: ‘123456789’,

                ‘inn’: ‘123456789000’,

                ‘payerName’: 'organisation name that is the payer',

                ‘payerTransferId’: {

                ‘transferType’: 'money transfer method type',
```

```
                ‘regNumber’: ‘123456789’,
                ‘uniqIdentifier’: ‘1234567891’,
                ‘actionStatus’: 'status of the restriction on funds debiting',

            ‘dateTimeAt’: ‘2018-03- 22T08:14:38Z’,
                ‘text’: 'additional description',
                ‘persons’: {
                    ‘lastName’: ‘last name’,
                    ‘firstName’: ‘name’,
                    ‘middleName’: ‘patronymic name’,
                    ‘landlineNumber’: ‘1212312345678’,
                    ‘mobileNumber’: ‘1212312345678’,
                    ‘email’: ‘qwerty1@example.ru’,
                    ‘position’: 'position'
                },
                ‘attachment’: {
                    ‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
                    ‘comment’: ‘attachment description’,

            ‘dateTimeAt’: ‘2018-03- 22T08:14:38Z’,
                    ‘file’: {
```

```
'orgKpp': '123456789',
'orgOgrn': '1234567890000',
'isp': [{
'name': 'telecom operator name',
'ipAddress': ['192.168.1.0', '192.168.2.0']
}],
'software': [{
'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
'type': 'type of software/hardware of the information exchange participant',
-
'name': 'name of software/ hardware',
'version': 'software hardware version',
-
'name': 'name of software/hardware',
'version': 'software/hardware version',
'description': 'additional description of the type of the attacked object'
}],
'registration': {
'department': 'the structural (organisational) unit of an information exchange participant where the incident was registered (detected)',
'technicalDevice': 'incident registration technical device'
},
'typeOfAttack': 'computer attack type code',
'measuresAndRecomendations': [{
'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
'dateTimeAt': '2018-03-22T08:14:38Z ',
'action': 'actions taken to eliminate the incident'
'text': 'text of measures or recommendations'
'attachment': {
'typeOfActivity': ['type of the planned activity'],
'nameOfActivity': 'name of the planned activity or resource where information is to be disclosed',
'text': 'text to the planned activity',
'messageAttachment': {
'sourceId': 'f34030ef - 358a-445c-8567-25985ce6d91c',
'com - ment': 'attachment description',
'dateTimeAt': '2018-03-22T08:14:38Z ',
'file': { 'name': 'file name',
'size': 'file size in bytes',
'base64': 'attachment in base64 format'
},
'fileLink': 'http://domain.com/archive.rar'
}
'paymentCard': {
'number': '12341234123412',
'sum': 'amount of the money transfer transaction using payment cards',
'currency': 'currency of the money transfer transaction',
'dateTimeAt': '2018-01-13T09:14:38Z',
'rrn': 'the number generated for a money transfer transaction during its authorisation'
},
'settlement': {
'number': '12345123451234512345',
'sum': 'amount of the money transfer transaction',
'currency': 'name': 'file name',
'size': 'file size in bytes',
'base64': 'attachment in base64 format'
}
}]
}
```

‘description’: addition
al description of
software/hardware',
}],
‘persons’:
[{
‘memberId’:
‘9527dd0c-0765-4f1c-
8f5f- 70a02cf4046c’,
‘sourceId’:
‘f34030ef-358a-445c-
8567- 25985ce6d91c’,
‘lastName’: 'last
name',
‘middleName
’: ‘patronymic name’,
‘firstName’:
'name',
'landlineNumber':
'stationary telephone',
‘mobileNumber’: '
mobile telephone',
‘email’: 'e-
mail address',
‘position’:
'positio
n',
-
	{
	‘sourceId’: ‘f34030ef-
	358a- 445c-8567-25985ce6d91c’,
	‘comment’:
	‘attachm
	ent description’,
	‘dateTimeAt’: ‘2018-
	03- 22T08:14:38Z’,
	‘file’:
	{
	‘name’: 'file name',
	‘size’: 'file size in
	bytes',
	‘base64’: 'attachment in
	base64 format'
	},
	‘fileLink’:
	‘http://domain.com/archive.rar
	‘
	}
	}],
	‘location’: {
	‘subjec-
	tOfFederation’: ‘00’,
	‘locality’:
	'residential area name'
	},
	‘classification’: {
	‘typeOfInci-
		}
		}
			'currency of money transfer
			transaction',
			‘dateTimeAt
			’: ‘2018-01-13T09:14:38Z’
			},
			‘phoneNumber’: {
			‘number’:
			‘1212312345678’,
			‘sum’:
			'amount
			of the transaction',
			‘currency’
			: ‘transaction
			currency’,
			‘dateTimeAt
			’: ‘2018-01-13T09:14:38Z’
			},
			‘idNumber’: {
			‘number’:
			‘1KoX6AA5VTdbBTkw27YEqK
			FaTtEQq97AAT’,
			‘sum’:
			'amount
			of the transaction',
			‘currency’
			: ‘transaction
			currency’,	

‘active’: ‘exitence of access to the personal account of an information exchange participant',
 	
‘category’: 'category of structural unitn of the responsible person of an information exchange participant'
}],
‘id_cii’: 'identifier of the CII object',
‘orgType’: 'type of an information exchange participant',
‘legalAddress’: {
 	
‘oktmo’: ‘12345678’,
 	
‘postalCode’: 'postal code',
 	
‘country’: 'three-letter country code',
 	
‘federalDistrict’: 'federal district code',
 	
‘subjectOfFederation’: ‘00’,
	dent’: 'incident type',
	‘ext’: [{
	
	‘events’: 'data protection events',
	
	‘method’: 'the method of preparing and transferring transaction instructions which make it possible to conduct a financial operation'
	}],
	‘int’: [{
	
	‘events’: 'data protection events',
	
	‘typeOfIntruder’: 'violator type'
	}],
	‘damage’: {
	‘operating’: 'assessment of operational expenses of an information exchange participant at the moment of providing data on the occurrence of an incident (INT vector)',
	‘relative’: 'relative (qualitative) assessment of the scale (severity of consequences) of the incident implementation (INT vector)'
	},
	‘schemaConclusion’: 'description of the money withdrawal scheme',
			‘dateTimeAt’: ‘2018-01-13T09:14:38Z’
			
			}
			},
			‘device’: {
			
			‘ip’: 'network address of the device',
			
			‘imsi’: 'international mobile subscriber identifier (individual subscriber number)',
			
			‘imei’: 'international mobile equipment identifier',
			
			‘aiic’: ‘Acquiring institution identification code (32 поле ISO 8583)’,
			
			‘cati’: ‘Card acceptor terminal identification (41 field ISO 8583)’,
			
			‘caic’: ‘Card acceptor identification code (42 поле ISO 8583)’
			}
			},
			‘payee’: {
			‘bik’: ‘123456789’,	

‘fiasId’: ‘e6668cfd-ae08- 4b02-a385-88179dfb1097’,
‘district’: ‘district’,
‘city’: 'city',
'cityDistrict': 'inner city district',
‘locality’: 'residential area,'
‘street’: ‘street’,
‘house’: 'house number',
‘building’: 'block/building',
‘room’: 'room/ office',
‘additionalInformati on’: 'additional information'
},
‘postAddress’:
{ ‘oktmo’: ‘12345678’,
‘postalCode’: ‘postal
	‘attachments’: [{
	‘sourceId’: ‘f34030ef-358a- 445c-8567-25985ce6d91c’,
	‘comment’: ‘attachment description’,
	‘dateTimeAt’: ‘2018-03- 22T08:14:38Z’,
	‘file’: {
	‘name’: 'file name',
	‘size’: 'file size in bytes',
	‘base64’: 'attachment in base64 format'
	},
	‘fileLink’: ‘http://domain.com/archive.rar’
	}]
	},
	‘antifraud’: [{
	‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
	‘victim’: ‘information on the legal status of the payer’,
	‘payerIdenti-
			‘inn’: ‘123456789000’,
			‘payeeName’: 'the name of the organisation that is the payee',
			‘payeeTransferId’: {
			‘transferType’: 'money transfer method type',
			‘paymentCard’: {
			‘number’: ‘123412341234123412’,
			‘sum’: 'amount of the money transfer transaction using payment cards',
			‘currency’: 'currency of the money transfer transaction using payment cards',
			‘status1’: {
			‘enrollment’: 'transaction suspension identifier',	

code',
 	
'country': 'three-letter country code',
 	
'federalDistrict': 'federal district code',
 	
'subjectOfFedera- tion': '00',
'fiasId': '8abe47a7-24dd- 4951-ae16-f2781eba9d93',
 	
'district': 'district',
 	
'city': 'city',
 	
'cityDistrict': 'inner city district',
 	
'locality': 'residential area,'
 	
'street': 'street',
 	
'house': 'house number'
 	
'building': 'block/building',
 	
'room': 'room/ office',
	fier': {
	
	'hash': 'E25059612A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA441E44',
	
	'hashSnils': 'C49337884A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A9AE48FA441E44'
	},
	'payer': {
	'bik': '123456789',
	'inn': '123456789000',
	'payerName': 'name of the organisation that is the payer',
	'payerTransferId': {
	
	'transferType': 'money transfer method type',
	
	'paymentCard': {
	
	'number': '123412341234123412',
	
	'sum': 'amount of the money transfer transaction using payment cards',
			'dateTimeAt': '2002-10-02T15:00:00.05Z'
			
			}
			
			},
			
			'settlement': {
			
			'number': '12345123451234512345',
			
			'sum': 'amount of the money transfer transaction',
			
			'currency': 'currency of the money transfer transaction',
			
			'status1': {
			
			'enrollment': 'transaction suspension identifier',
			
			'dateTimeAt': '2002-10-02T15:00:00.05Z'
			
			}
			
			},	

‘additionalInformati on’: 'additional information'
},
‘physicalAddress’: [{
‘oktmo’: ‘12345678’,
‘postalCode’: 'postal code',
‘country’: 'three-letter country code',
‘federalDistrict’: 'federal district code',
‘subjectOfFedera- tion’: ‘00’,
‘fiasId’: ‘8661e93f-6c6a- 4b19-b485-14e27e564169’,
‘district’: ‘district’,
‘city’: 'city',
'cityDistrict': 'inner city district',
‘locality’: 'residential area,'
	‘currency’: 'currency of the money transfer transaction',
	‘dateTimeAt’: ‘2018-01-13T09:14:38Z’,
	‘rrn’: 'the number generated for a money transfer transaction during its authorisation'
	},
	‘settlement’: {
	‘number’: ‘12345123451234512345’,
	‘sum’: 'amount of the money transfer transaction',
	‘currency’: 'currency of money transfers',
	‘dateTimeAt’: ‘2018-01-13T09:14:38Z’
	},
	‘phoneNumber’: {
			‘phoneNumber’: {
			‘number’: ‘1212312345678’,
			‘sum’: 'amount of the transaction',
			‘currency’: ‘transaction currency’,
			‘status1’: {
			‘en-rollment’: 'transaction suspension identifier',
			‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’
			}
			},
			‘idNumber’: {
			‘number’: ‘1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT’,
			‘sum’: 'amount of the transaction for changing the balance of funds',
			‘currency’:	

‘street’: 'street',
 	
‘house’: 'house number',
 	
‘building’: 'block/building',
 	
‘room’: 'room/office',
 	
‘additionalInformation’: 'additional information'
}]
}
}
	‘number’: ‘1212312345678’,
	
	‘sum’: 'amount of the transaction',
	
	‘currency’: 'currency of the transaction',
	
	‘dateTimeAt’: ‘2018-01-13T09:14:38Z’
	
	},
	
	‘idNumber’: {
	
	‘number’: ‘1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT’,
	
	‘sum’: 'transaction amount',
	-
	
	‘currency’: 'currency of the transaction',
	
	‘dateTimeAt’: ‘2018-01-13T09:14:38Z’
	
	}
	},
	‘device’: {
	
	‘ip’: 'network address of the device',
	-
			'amount of the transaction for changing the balance of funds',
			
			‘status1’: {
			
			‘enrollment’: 'transaction suspension identifier',
			
			‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’
			
			}
			
			}
			}
			}
			}]
			}	

	‘imsi’: 'international mobile subscriber identifier (individual subscriber number)',
	
	‘imei’: 'international mobile equipment identifier',
	
	‘aiic’: ‘Acquiring institution identification code (32 field ISO 8583)’,
	
	‘cati’: ‘Card acceptor terminal identification (41 field ISO 8583)',
	
	‘caic’: ‘Card acceptor identification code (42 поле ISO 8583)’
	}
	},
	‘payee’: {
	‘bik’: ‘123456789’,
	‘inn’: ‘123456789000’,
	‘payeeName’: 'name of the organisation that is the payee',			

	‘payeeTransferId’: { ‘transferType’: 'type of of the method of transferring funds',			

	‘paymentCard’: {
	‘number’
	:
	‘123412341234123412’
	},
	‘settlement’: {
	‘number’:
	‘12345123451234512345’
	},
	‘phoneNumber’: {
	‘number’:
	‘1212312345678’
	},
	‘idNumber’: {
	‘number’:
	‘1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT’
	}
	}
	},
	‘additional-Status’: {
	‘crossBorder’: 'identifier of			

	cross-border banking',
	'ad-ditionalTransactionApprove': [
	'identifier of the additional approval of the transaction'
	]
	}
	}],
	'impacts': {
	'trafficHi-jackAttacks': [{
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'le-galAsPath': 'legal AS-Path',
	'wrongAsPath': 'wrong AS-Path',
	'lookingGlass': 'link to to the Looking Glass used to verify AS-Path',
	'le-galPrefix': 'legal prefix',
	'wrongPrefix': 'wrong prefix'
	}],
	'malware': [{
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'tar-			

	get': {
	
	'ip': '127.0.0.1'
	},
	
	'sources': [{ 'ip':
	
	'127.0.0.1',
	
	'domain': 'example.com',
	
	'url': 'http://example.com'
	}],
	
	'classifications': [{
	
	'vendorName': 'name of the MCSE tool,
	
	'vendorVerdict': 'MC classification'
	}],
	
	'malwareSamples':
	
	[{ 'hash': {
	
	'md5': '4BA5139A444538479D9D750E2E2779BF',
	
	'sha1': 'D2B063763378A8CB38B192B2F71E78BC13783EFE',			

	'sha256': 'E25059612A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A9AE48FA441E44'
	
	},
	
	'attachment': {
	
	'sourceId': 'f34030ef- 358a-445c-8567-25985ce6d91c',
	
	'comment': 'attachment description',
	
	'dateTimeAt': '2018-03-22T08:14:38Z ',
	
	'file': {
	
	'name': 'file name',
	
	'size': 'file size in bytes',
	
	'base64': 'attachment in base64 format'
	
	},
	
	'fileLink': 'http://domain.com/archive.rar'
	
	}
	}],			

	‘malwareMessageSenders’: [{
	‘email’: ‘qwerty@example.ru’,
	‘server’: ‘127.0.0.1’
	}],
	‘malwareMessageAttach-ment’: {
	‘sourceId’: ‘f34030ef-358a- 445c-8567-25985ce6d91c’,
	‘comment’: 'comment to the attachment',
	‘dateTimeAt’: ‘2018-03- 22T08:14:38Z’,
	‘file’: {
	‘name’: 'file name',
	'size': 'file size in bytes',
	Base64 formate'
	'attachment in base64 format'
	},
	‘fileLink’: ‘http://domain.com/archive.rar‘
	},			

	‘harmfulResourceAddress’:
	[{ ‘ip’: ‘127.0.0.1’,
	‘domain’: ‘example.com’,
	‘url’: ‘http://example.com’
	}],
	‘iocs’: [{
	‘net’: [{
	‘impact’: 'type of the detected compromising identifier',
	‘comment’: 'additional description',
	}],
	‘fil’: [{
	‘impact’: 'type of the detected compromising identifier',
	‘comment’: 'additional description',
	}],
	‘reg’: [{			

	‘impact’: 'type of the detected compromising identifier',
	
	‘comment’: 'additional description',
	
	}],
	
	‘prc’: [{
	
	‘impact’: 'type of the detected compromising identifier',
	
	‘comment’: 'additional description',
	
	}],
	
	‘oth’: [{
	
	‘impact’: 'type of the detected compromising identifier',
	
	‘comment’: 'additional description',
	
	}]
	}],
	‘in-fectionMethods’: [{
	
	‘type’: 'type of the suggested			

	infection method',
	
	‘comment’: 'additional description'
	}]
	}],
	‘socialEngi-neering’: {
	
	‘sourceId’: ‘f34030ef-358a- 445c-8567-25985ce6d91c’,
	
	‘soiTypes’: ['identifier of the social engineering method'],
	
	‘soiSenders’: [{
	
	‘phoneNumber’: ‘1212312345678’,
	
	‘email’: ‘qwerty@example.ru’,
	
	‘server’: ‘127.0.0.1’
	}],
	
	‘messageAttachment’: {
	
	‘sourceId’: ‘f34030ef-
	
	358a-445c-8567-25985ce6d91c’,
	
	‘comment’: 'comment to the attachment',
	
	‘dateTimeAt’: ‘2018-03-			

	22T08:14:38Z ‘,
	‘file’: {
	‘name’: 'file name',
	'size': 'file size in bytes',
	‘base64’: 'attachment in base64 format'
	},
	‘fileLink’: ‘http://domain.com/archive.rar ‘
	},
	‘description’: 'additional description'
	},
	‘ddosAttacks’: [{
	‘sourceId’: ‘f34030ef-358a- 445c-8567-25985ce6d91c’,
	‘target’: {
	‘ip’: ‘127.0.0.1’,
	‘domain’: ‘example.com’,
	‘url’: ‘http://example.com’,			

	‘assignment’: 'purpose of the attacked object',
	
	‘serviceType’: 'type of the information service',
	
	‘network’: 'network address'
	},
	‘attackType’: {
	
	‘type’: 'attack type (by OSI levels)',
	
	‘comment’: 'additional description'
	},
	
	‘sources’: [{ ‘ip’:
	
	‘127.0.0.1’
	}],
	
	‘power’: {
	
	‘pps’: 'number of packets per second',
	
	‘mps’: 'number of megabits per second',
	
	‘rps’: 'number of requests per second',
	},			

	"startTimeAt": "2018-03- 22T08:14:38Z ",
	
	"endTimeAt": "2018-03- 22T09:15:44Z ",
	"negativeImpact": {
	
	"type": 'negative impact type',
	
	"comment": 'comment to the selected type'
	}
	}],
	"atmAttacks": {
	
	"sourceId": "f34030ef-358a- 445c-8567-25985ce6d91c",
	"target": {
	
	"type": 'attacked object
	
	type','description':
	
	'additional description'
	},
	'attackType": [{
	
	"type": 'attack type depending on the attached target',			

	'additional description'
	}],
	'attackImage': {
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'comment': 'comment to the attachment',
	'dateTimeAt': '2018-03- 22T08:14:38Z ',
	'file': {
	'name': 'file name',
	'size': 'file size in bytes',
	'base64': 'attachment in base64 format'
	},
	'fileLink': 'http://domain.com/archive.rar '
	}
	},
	'vulnerabilities': [{
	'sourceId': 'f34030ef-			

	'additional description'
	}],
	'attackImage': {
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'comment': 'comment to the attachment',
	'dateTimeAt': '2018-03- 22T08:14:38Z ',
	'file': {
	'name': 'file name',
	'size': 'file size in bytes',
	'base64': 'attachment in base64 format'
	},
	'fileLink': 'http://domain.com/archive.rar '
	}
	},
	'vulnerabilities': [{
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',			

	‘target’: {
	‘ip’: ‘127.0.0.1’,
	‘domain’: ‘example.com’, ‘url’
	‘http://example.com’,
	‘serviceType’: 'information service type'
	},
	‘sources’: [{ ‘ip’:
	‘127.0.0.1’,
	‘url’: ‘http://example.com’
	}],
	‘identifier’: 'vulnerability identifier',
	‘cvss’: 'CVSS metrics',
	'idCustom': {
	‘description’: 'vulnerability description'
	‘swName’: 'software name',
	‘swVer’: 'software version',			

	‘cweType’: 'CWE error type', - ‘class’: 'vulnerability class', 'osName': 'operating system that controls software with detected vulnerability', ‘detectedAt’: 'date and time when vulnerability is detected', ‘baseCVSS’: 'baseline vector of vulnerability', ‘danger’: 'hazard level of the detected vulnerability', ‘measures’: 'possible measures to eliminate vulnerability', ‘status’: 'vulnerability status', 'exploit': 'existence of exploit', - ‘recommendation’: 'information on vulnerability elimination', ‘link’: 'links to sources of information on the elimination of vulnerability',			

	‘manufacturer’: 'a company (organisation) that manufactures (develops) software in which a vulnerability has been detected'
	}
	}],
	‘bruteForces’: [{
	‘sourceId’: ‘f34030ef-358a- 445c-8567-25985ce6d91c’,
	‘target’: {
	‘ip’: ‘127.0.0.1’,
	‘url’: ‘http://example.com’,
	‘serviceType’: 'service type'
	},
	‘sources’: [{
	‘ip’: ‘127.0.0.1’
	}],
	‘accountOs’: {
	‘name’: 'account name',
	-
	‘privileges’: 'level of (privilege) of account name'
	}			

	}],
	'spams': [{
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	're - ceivedAt': '2018-03-22T08:14:38Z',
	'tar-gets': [{
	'email': 'qwerty@example.ru'
	}],
	'sources': [{
	'ip':
	'127.0.0.1',
	'domain': 'example.com',
	'email': 'qwerty@example.ru'
	}],
	'spamImages': {
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'comment': 'attachment description',
	'dateTimeAt': '2018-03- 22T08:14:38Z',
	'file': {			

	‘name’: 'file name',
	
	‘size’: 'file size in bytes',
	
	‘base64’: 'attachment in base64 format'
	
	},
	
	‘fileLink’: ‘http://domain.com/archive.rar‘
	}
	}],
	‘con-trolCenters’: [{
	
	‘sourceId’: ‘f34030ef-358a- 445c-8567-25985ce6d91c’,
	‘tar-get’: {
	
	‘ip’: ‘127.0.0.1’,
	
	‘url’: ‘http://example.com’
	},
	
	‘hostUrl’: ‘http://example.com’,
	‘in-truderIp’: ‘1.1.1.1’,
	‘in-truderActions’: 'what preceded the incident',
	‘de-			

	scription': 'known information about the Botnet Command Centre',
	
	'nodes': [{
	
	'ip': '127.0.0.1',
	
	'lastRequestRateTimeAt': '2018-03-22T08:08:49Z'
	}]
	}],
	'sim': {
	
	'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
	'mobileOperator': 'mobile phone operator name',
	
	'phoneNumber': '1212312345678',
	
	'imsi': 'unique SIM card number',
	'imsiChangedAt': 'date when the IMSI change was recorded'
	},
	'phishingAttacks': [{
	
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'target': {			

	'ip': '127.0.0.1',
	'domain': 'example.com'
	},
	'harmful': [{ 'ip':
	'127.0.0.1',
	'url': 'http://example.com'
	}],
	'fixa- tionAt': '2018-03-22T08:08:49Z ',
	'messageAttachment': {
	'sourceId': 'f34030ef-
	358a-445c-8567-25985ce6d91c',
	'comment': 'attachment description',
	'dateTimeAt': '2018-03- 22T08:08:49Z ',
	'file': {
	'name': 'file name',
	'size': 'file size in bytes',
	'base64': 'attachment in base64 format'			

	}, 'fileLink': 'http://domain.com/archive.rar' } }], 'prohibit-edContents': [{ 'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c', 'sources': [{ 'ip': '127.0.0.1', 'url': 'http://example.com' }], 'type': 'prohibited content type' }], 'mali-ciousResources': [{ 'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c', 'sources': [{ 'ip': '127.0.0.1', 'url': 'http://example.com'			

	}],
	'activityType': 'description of malicious activity'
	}],
	'changeContent': [{
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'targets': [{
	'ip': '127.0.0.1',
	'url': 'http://example.com'
	}],
	'type': 'type of content'
	}],
	'scanPorts': [{
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'sources': [{
	'ip': 'IP address'
	}],
	'ports': ['21'],
	'method': 'information on scanning methods			

	or software used for this purpose'
	
	'startTimeAt': '2018-03- 22T08:08:49Z',
	
	'endTimeAt': '2018-03- 22T08:09:49Z'
	}],
	'other': {
	
	'sourceId': 'f34030ef-358a- 445c-8567-25985ce6d91c',
	'description': 'computer attack description',
	
	'source': {
	
	'ip': '127.0.0.1',
	
	'url': 'http://example.com'
	},
	
	'type': 'other type of prohibited, malicious, altered content',
	'attachment': {
	
	'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
	
	'comment': 'attachment description',			

	‘dateTimeAt’: ‘2018-03- 22T08:08:49Z’,
	‘file’: {
	‘name’: 'file name',
	'size': 'file size in bytes',
	‘base64’: 'attachment in base64 format'
	},
	‘fileLink’: ‘http://domain.com/archive.rar’
	}
	}
	},
	‘finalReport’: {
	‘closeDateAt’: 'date and time of incident closure'
	‘recovery’: 'incident recovery identifier',
	‘description’: ‘additional description if recovery is impossible’,
	‘rootCause’: 'key causes of the incident',
	‘mainActions’:			

	'actions taken to prevent future incidents',
	‘signatures’: [{
	‘identifier’: 'signature identifier',
	‘name’: 'detection tool',
	‘source’: 'signature source',
	‘eventsAmount’: 'number of signature activations'
	}],
	‘snort’: [‘rule1’, ‘rule2’],
	‘attachment’: {
	‘sourceId’: ‘f34030ef-358a- 445c-8567-25985ce6d91c’,
	‘comment’: ‘attachment description’,
	‘dateTimeAt’: ‘2018-03- 22T08:14:38Z’,
	‘file’: {
	‘name’: 'file name',			

	'size': 'file size in bytes', 'base64': 'attachment in base64 format' }, 'fileLink': 'http://domain.com/archive.rar' } } } }			

Annex 2. Schemes of interaction between the Bank of Russia and an information exchange participant

The form of distribution by the Bank of Russia among information exchange participants of data on the detected incidents associated with violations of data protection requirements	The form of a Bank of Russia request to an information exchange participant servicing the payee	The form of a Bank of Russia information message to an information exchange participant servicing the payer	The form of a Bank of Russia information message on imposing (or lifting) a restriction on bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds

{
'header': {
'schemaType': 'reaction',
'schemaVersion': '1',
'version': '1',
'publishedAt': '2002-10- 02T15:00:00.05Z'
},
'reaction': {
'fixationAt': '2002-10- 02T15:00:00.05Z',
'rootCause': 'key causes of the incident',
	{
	'header': {
	'schemaType': 'anti-fraudRequest',
	'schemaVersion': '1',
	'version': '1',
	'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c',
	'publishedAt': '2002- 10-02T15:00:00.05Z'
	},
		{
		'header': {
		'schemaType': 'antifraudReturn',
		'schemaVersion': '1',
		'version': '1',
		'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c',
		'publishedAt': '2002-10-02T15:00:00.05Z'
			{
			'header': {
			'schemaType': 'lockRe-sponse',
			'schemaVersion': '1',
			'version': '1',
			'memberId': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c',
			'sourceId': 'f34030ef - 358a-445c-8567-25985ce6d91c',
			'publishedAt': '2002-10-02T15:00:00.05Z'

<table>
<tr>
<td>'vectorCode': 'computer attack vector identifier',
'serviceType': [{
'type': type of the attacked object',
'name': 'software/hardware name',
'version': 'software/hardware version',
'description': 'additional description of the type of the attacked object'
}],
'typeOfAttack': 'computer attack type code',
'antifraudDestributed': [{
'device': {
'ip': '127.0.0.1',
'imsi': 'international mobile subscriber identifier (individual subscriber number)',
'imei': 'international mobile equipment identifier',
'aiic': 'acquiring institution identification code (32 поле ISO 8583)',
'cati': 'card acceptor terminal identification (41 поле ISO 8583)',
'caic': 'card acceptor identification code (42 поле ISO 8583)'
},
'payee': {
'bik': '123456789',
'hash': 'P79969612A71BAB224C7CB534FD7A0D3C1C78AD40(
64C48F12A9AE48FA441E11',
'hashSnils': 'B49087832A71BAB224C7CB534FD7A0D3C1C78AD40(
64C48F12A9AE48FA441E44',
'inn': '123456789000',</td>
<td>'antifraudRequest': [{
'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
'victim': 'information on the legal status of the payer',
'payer': {
'bik': '123456789',
'inn': '123456789000',
'namePayer': 'organisation name that is the payer',
'payerTransferId': {
'transferType': type of money transfer method ',
'paymentCard': {
'number': '123412341234123412',
'sum': 'amount of the money transfer transactions using payment cards',
'currency': 'currency of a money transfer transaction',
'dateTimeAt': '2018-01-13T09:14:38Z',
'rrn': 'the number generated</td>
<td>},
'anifraudReturn': [{
'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
'victim': 'information on the legal status of the payer'
'recipient': 'information on the legal status of the payee',
'payer': {
'bik': '123456789',
'inn': '123456789000',
'payerName': 'name of the organisation that is the payer',
'payerTransferId': {
'transferType': 'type of money transfer method',
'paymentCard': {
'number': '123412341234123412',
'sum': the amount a money transfer transaction using payment cards',
'currency': 'currency of money transfer transaction',</td>
<td>},
'lockResponse': [{
'sourceId': 'f34030ef - 358a-445c-8567-25985ce6d91c',
'orgBik': '123456789',
'regNumber': '123456789',
'uniqIdentifier': '1234567891',
'actionStatus': 'status of the restriction on funds debiting',
'coordinationStatus': 'status of integrity control of the request to impose or lift the restriction in the form of a ban on debiting funds',
'dateTimeAt': '2018-03-22T08:14:38Z',
'text': 'additional description'
'attachment': {
'sourceId' : 'f34030ef-358a-445c-8567-25985ce6d91c',
'comment': 'attachment description',
'dateTimeAt ': '2018-03-22T08:14:38Z',
'file': {
'name': 'file name',
'size': 'file size in bytes',
'base64': 'attachment in Base64 format'
}
}</td>
</tr>
</table>

‘transferId’: { ‘payment-Card’: { ‘num-ber’: ‘123412341234123412’ }, ‘settlement’: { ‘num-ber’: ‘12345123451234512345’ }, ‘pho-neNumber’: { ‘num-ber’: ‘1212312345678’ }, ‘idNumber’: { ‘num - ber’: ‘1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT’ } } }, ‘additionalStatus’: { ‘crossBorder’ : 'cross-border banking identifier', ‘additionalTransac-tionApprove’: ['additional transaction approval identifier'] } }], ‘impacts’: { ‘trafficHijackAttacks’: [{ ‘legalAsPath’: 'legal AS-Path', ‘wrongAsPath’: ‘wrongAsPath’: ‘lookingGlass’: ‘Reference link to Looking Glass used to verify	for a money transfer transaction during its authorisation' }, ‘set-tlement’: { ‘number’: ‘12345123451234512345’, ‘sum’: 'amount of the money transfer transaction', ‘currency’: 'currency of the money transfer transaction', ‘dateTimeAt’: ‘2018-01- 13T09:14:38Z’ }, ‘phoneNumber’: { ‘number’: ‘1212312345678’, ‘sum’: ‘transaction amount’, ‘currency’: 'currency of transaction - ‘dateTimeAt’: ‘2018-01- 13T09:14:38Z’ }, ‘id-Number’: { ‘number’: ‘1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT’,	‘dateTimeAt’: ‘2018-01-13T09:14:38Z’, ‘rrn’: 'the number generated for a money transfer transaction during its authorisation' }, ‘settlement’: { ‘number’: ‘12345123451234512345’, ‘sum’: 'amount of the money transfer transaction', ‘currency’: 'currency of the money transfer transaction', ‘dateTimeAt’: ‘2018-01-13T09:14:38Z’ }, ‘phoneNumber’: { ‘number’: ‘1212312345678’, ‘sum’: 'transaction amount', - ‘currency’: 'transaction currency’,	}] }

AS-Path',
'legalPrefix': 'legal prefix',
'wrongPrefix': 'wrongPrefix'
}],
'malware': [{
'sources': [{
'ip': '127.0.0.1',
'domain': 'example.com',
'url': 'http://example.com'
}],
'classifications': [{
'vendorName': 'name of the MCSE tool used by the information exchange participant',
'vendorVerdict': 'MC class in accordance with the MCSE tool of the information exchange participant'
}],
'malwareSamples': [{
'hash': {
'md5': '4BA5139A444538479D9D750E2E2779BF',
'sha1': 'D2B063763378A8CB38B192B2F71E78BC13783EFE ',
'sha256': 'E25059612A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A9AE48FA441E44'
},
'attachment': {
'sourceId': 'f34030ef-358a-445c-8567- 25985ce6d91c',
	'sum': 'transaction amount',
	'currency': 'currency of transaction
	-
	'dateTimeAt': '2018-01- 13T09:14:38Z'
	}
	},
	'device': {
	'ip': 'network address of the device',
	'imsi': 'international mobile subscriber identifier (individual subscriber number)',
	'imei': 'international mobile equipment identifier',
	'aiic': 'Acquiring institution identification code (32 поле ISO 8583)',
	'cati': 'Card acceptor terminal identification (41 поле ISO 8583)',
	'caic': 'Card acceptor identification code (42 поле ISO 8583)'
	}
	},
	'payee': {
	'bik': '123456789',
	'inn': '123456789000',
		'dateTimeAt': '2018-01-13T09:14:38Z'
		},
		'idNumber': {
		'number': '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT',
		'sum': 'transaction amount',
		-
		'currency': 'transaction currency',
		-
		'dateTimeAt': '2018-01-13T09:14:38Z'
		}
		},
		'device': {
		'ip': 'network address of the device',
		'imsi': 'international mobile subscriber identifier (individual subscriber number)',
		'imei': 'international mobile equipment identifier',
		'aiic': 'Acquiring institu-	

'comment': 'comment to attachment',
 	
'dateTimeAt': '2018-03-22T08:14:38Z',
'file': {
 	
'name': 'file name',
 	
'size': 'file size in bytes', 'base64':
 	
'attachment in base64 format'
},
 	
'fileLink': 'http://domain.com/archive.rar'
}
}],
'malwareMessag-eSenders': [{
'email': 'qwer-ty@example.ru',
'server': '127.0.0.1'
}],
'malwareMes-sageAttachment': {
'sourceId' : 'f34030ef-358a-445c-8567-25985ce6d91c',
'comment': 'comment to the attachment',
'dateTimeAt': '2018-03-22T08:14:38Z',
'file': {
 	
'name': 'file name',
'size': 'file size in bytes',
 	
'base64': 'attachment in base64 format'
},
	'payeeName': 'the name of the organisation that is the payee',
	'payeeTrans-ferId': {
	
	'transferType': 'money transfer method type',
	
	'paymentCard':
	
	{ 'number': '123412341234123412'
	},
	'set-tlement': {
	
	'number': 'the number of a settlement account of the payee opened with the money transfer operator serving the payee',
	},
	
	'phoneNumber': {
	
	'number': '1212312345678'
	},
	'id-Number': {
	
	'number': '1KoX6AA5VTdbBTkw27YEqKFaTtEQc97AAT'
	}
	}
	}
	}]
		tion identification code (32 field ISO 8583)',
		
		'cati': 'Card acceptor terminal identification (41 field ISO 8583)',
		
		'caic': 'Card acceptor identification code (42 field ISO 8583)'
		}
		},
		'payee': {
		'bik': '123456789',
		'inn': '123456789000',
		'pay-eeName': 'the name of the organisation that is the payee',
		'payeeT-ransferId': {
		
		'transferType': 'type of money transfer method',
		
		'paymentCard':
		
		{ 'number': '123412341234123412',
		
		'sum': 'amount of the money transfer transaction using payment cards',
		
		'currency': ' currency of a money transfer transaction	

‘fileLink’: ‘http://domain.com/archive.rar’
},
‘harmfulResourceAddress’: [{
‘ip’: ‘127.0.0.1’,
‘domain’: ‘example.com’,
‘url’: ‘http://example.com’
}],
‘iocs’: [{
‘net’: [{
‘impact’: 'type of compromising identifier detected',
‘comment’: 'additional description'
}],
‘fil’: [{
‘impact’: 'type of compromising identifier detected',
‘comment’: 'additional description'
}],
‘reg’: [{
‘impact’: 'type of compromising identifier detected',
‘comment’: 'additional description'
}],
‘prc’: [{
‘impact’: 'type of compromising identifier detected',
	}	using payment cards'.
		‘status1’: {
		‘enrollment’: 'transaction suspension identifier',
		‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’
		}
		},
		‘settlement’:
		{ ‘number’: ‘12345123451234512345’,
		‘sum’: 'amount of the money transfer transaction',
		‘currency’: 'currency of the money transfer transaction',
		‘status1’: {
		‘enrollment’: 'transaction suspension identifier',
		‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’	

‘comment’: 'additional description'
}],
‘oth’: [{
‘impact’: 'type of compromising identifier detected',
‘comment’: 'additional description'
}]
}],
‘infectionMethod’: [{
‘type’: 'type of Possible infection method',
‘comment’: 'comment to the selected type'
}]
}],
‘socialEngineering’: {
‘soiTypes’: ['identifiers of social engineering methods']
‘soiSenders’: [{
‘phoneNumber’: ‘1212312345678’,
‘email’: ‘qwerty@yandex.ru’,
‘server’: ‘127.0.0.1’
}],
‘messageAttachment’: {
‘sourceId’: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
‘comment’: ‘attachment description’,
‘datetimeAt’: ‘2018-03-22T08:14:38Z’,
‘file’: {
‘name’: 'file name',
		}
		},
		‘phoneNumber’:
		{ ‘number’: ‘1212312345678’,
		‘sum’: 'transaction amount',
		-
		‘currency’: 'transaction currency',
		рации’,
		‘status1’: {
		‘enrollment’: 'transaction suspension identifier',
		‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’
		}
		},
		‘idNumber’: {
		‘number’: ‘1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT’,
		‘sum’: 'amount of the transaction for changing the balance of funds',
		‘currency’: 'currency of	

‘size’: ‘file size in bytes’,
‘base64’: 'attachment in base64 format'
},
‘fileLink’: ‘http://domain.com/archive.rar’
},
‘description’: 'additional description'
},
‘ddosAttacks’: [{
‘attackType’: {
‘type’: 'type of attack (by OSI levels)’,
‘comment’: 'additional description'
},
‘sources’: [{
‘ip’: ‘127.0.0.1’
}],
‘power’: {
‘pps’: 'number of packets per second',
‘mps’: 'number of megabits per second',
‘rps’: 'number of requests per second',
},
‘startTimeAt’: ‘2018-03-22T08:14:38Z’,
‘endTimeAt’: ‘2018-03-22T08:14:38Z’,
‘negativeImpact’: {
‘type’: 'type of negative impact',
‘comment’: 'additional description'
		the transaction for changing the balance of funds',
		‘status1’: {
		‘enrollment’: 'transaction suspension identifier',
		‘dateTimeAt’: ‘2002-10-02T15:00:00.05Z’
		}
		}
		}
		}
		}]	

}
}],
'atmAttacks': {
'target': {
'type': 'type of the object under attack',
'description': 'additional description'
},
'attackType': [{
'type': 'type of attack depending on the target',
'description': 'additional description'
}],
'attackImages': {
'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
'comment': 'attachment description',
'dateTimeAt': '2018-03-22T08:14:38Z',
'file': {
'name': 'file name',
'size': 'file size in bytes',
'base64': 'attachment in base64 format'
},
'fileLink': 'http://domain.com/archive.rar'
}
},
'vulnerabilities': [{
'sources': [{
'ip': '127.0.0.1',
'url':			

‘http://example.com’
}],
‘identifier’:
'vulnerability identifier',
‘CVSS’: ‘
CVSS metrics’
}],
‘bruteForces’: [{
‘sources’: [{
‘ip’: ‘127.0.0.1
‘
}]
}],
‘spams’: [{
‘receivedAt’: ‘2018-03-
22T08:14:38Z’,
‘sources’: [{
‘ip’:
‘127.0.0.1’,
‘domain’:
‘example.com’,
‘email’: ‘qwer-
ty@example.ru’
}],
‘spamImages’: {
‘sourceId’
: ‘f34030ef-358a-445c-8567-25985ce6d91c’,
‘comment’:
'comment to the attachment',
‘dateTimeAt’:
‘2018-03-22T08:14:38Z’,
‘file’: {
‘name’: 'file name',
‘size’:
‘file size in bytes’,
‘base64’: 'attachment in base64 format'
},			

‘fileLink’: ‘http://domain.com/archive.rar’
}
}],
‘controlCenters’: [{
‘hostUrl’: ‘http://example.com’,
‘intruderIp’: ‘1.1.1.1’,
‘intruderActions’: 'what preceded the incident',
‘description’: 'additional description of the Botnet command centre',
‘nodes’: [{
‘ip’: ‘127.0.0.1’,
‘lastReques-tRateTime’: ‘2018-03-22T08:14:38Z ‘
}]
}],
‘sim’: {
‘mobileOperato r’: 'name of a mobile telecom operator',
‘phoneNumber’: ‘1212312345678’,
‘imsi’: 'unique SIM card number',
‘imsiChangedAt’: ‘2018-03-22T08:08:49Z ‘
},
‘prohibitedContents’: [{
‘sources’: [{
‘ip’: ‘127.0.0.1’,
‘url’: ‘http://example.com’
}],
‘type’: 'type of content'
}],
‘phishingAttacks’: [{			

‘harmful’: [{
‘ip’: ‘127.0.0.1’,
‘url’: ‘http://example.com’
}],
‘fixationAt’: ‘2018-03-22T08:14:38Z’,
‘messageAttachment’: {
‘sourceId’ : ‘f34030ef-358a-445c-8567-25985ce6d91c’,
‘comment’: ‘attachment description’,
‘dateTimeAt’: ‘2018-03-22T08:14:38Z ‘,
‘file’: {
‘name’: 'file name',
‘size’: ‘file size in bytes’,
‘base64’: 'attachment in base64 format'
},
‘fileLink’: ‘http://domain.com/archive.rar’
}
}],
‘maliciousResources’: [{
‘sources’: [{
‘ip’: ‘127.0.0.1 ‘,
‘url’: ‘http://example.com’
}],
‘activityType’: 'type of malicious activity'
}],
‘changeContent’: [{			

'targets': [{
'ip': '127.0.0.1',
'url': 'http://example.com'
}],
'type': 'type of modified content'
}],
'scanPorts': [{
'sources': [{
'ip': '127.0.0.1'
}],
'ports': ['23'],
'method': 'information on scanning methods or software used for this purpose',
'startTimeAt': '2018-03-22T08:14:38Z',
'endTimeAt': '2018-03-22T08:14:38Z'
}],
'other': {
'description': 'description of a computer attack',
'target': {
'ip': '127.0.0.1',
'url': 'http://example.com'
},
'type': 'type of content', 'attachment': {
'sourceId': 'f34030ef-358a-445c-8567-25985ce6d91c',
'comment': 'comment to the attachment',
'dateTimeAt':			

‘2018-03-22T08:14:38Z’,
‘file’: {
‘name’: 'file name',
‘size’: ‘file size in bytes’,
‘base64’: 'attachment in base64 format'
},
‘fileLink’: ‘http://domain.com/archive.rar’
}
}
},
‘mainActions’: 'recommended actions to counter a computer attack',
‘signatures’: [{
‘identifier’: 'identifier of signature',
‘yara’: ‘yara-rule’,
‘snort’: [‘rule1’, ‘rule2’]
}]
}
}			

Annex 3. Diagrams of processes of interaction between an information exchange participant and the Bank of Russia

3.1. Sceme of registering an information exchange participant and changing its registration data

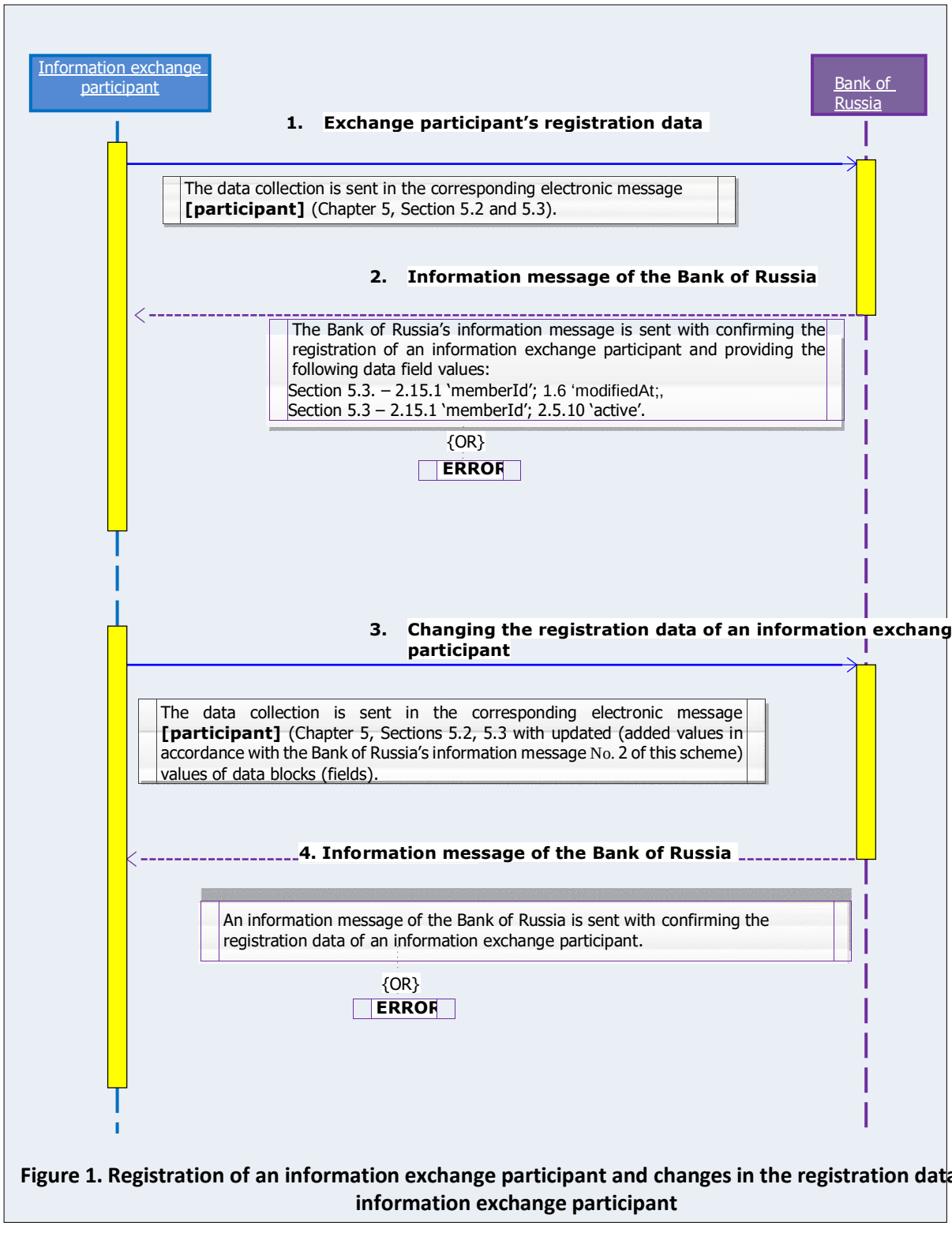

Figure 1. Registration of an information exchange participant and changes in the registration data of an information exchange participant

3.2 Scheme of informing the Bank of Russia by an information exchange participant about incidents related to violation of data protection requirements

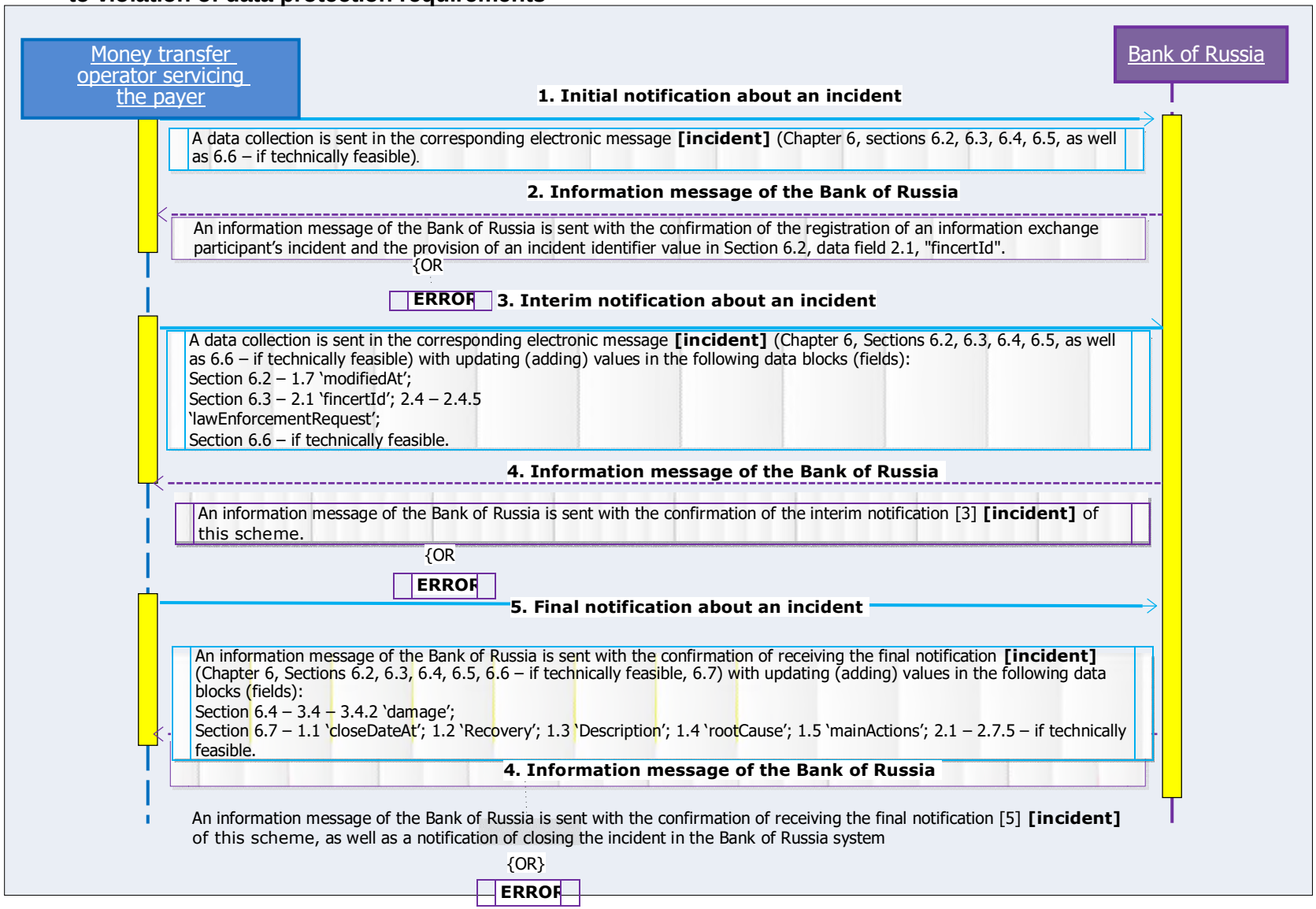

Figure 2. An information exchange participant informs the Bank of Russia about incidents related to violation of data protection requirements

3.3 Scheme of informing the Bank of Russia by an information exchange participant about all money transfers and (or) attempts to make them without the customer's consent, as well as notification by money transfer operators of suspending funds crediting to the payee's bank account or increasing the payee's electronic funds balance, or of the impossibility to suspend funds crediting to the payee's bank account or increase the payee's electronic funds balance

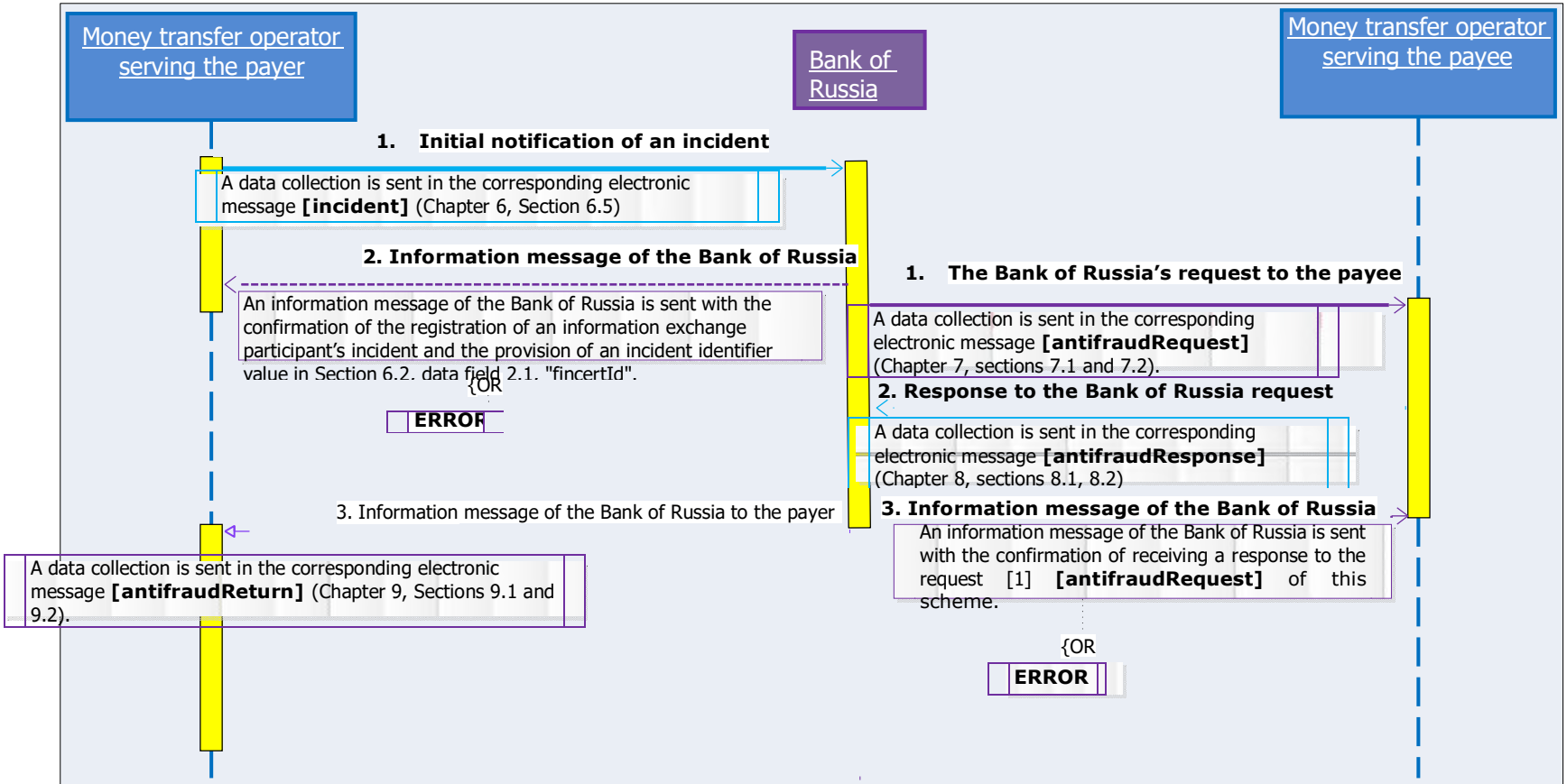

Figure 3. Informing the Bank of Russia by an information exchange participant about all money transfers and (or) attempts to make them without the customer's consent, as well as notification by money transfer operators of suspending funds crediting to the payee's bank account or increasing the payee's electronic funds balance, or of the impossibility to suspend funds crediting to the payee's bank account or increase the payee's electronic funds balance

3.4 Scheme of informing the Bank of Russia by information exchange participants other than the Bank of Russia structural units who uses express and non-rapid money money transfer services about imposing (or lifting) of the restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds in case of detection of incidents related to violation of the information protection requirements during money transfers at information infrastructure facilities of information exchange participants

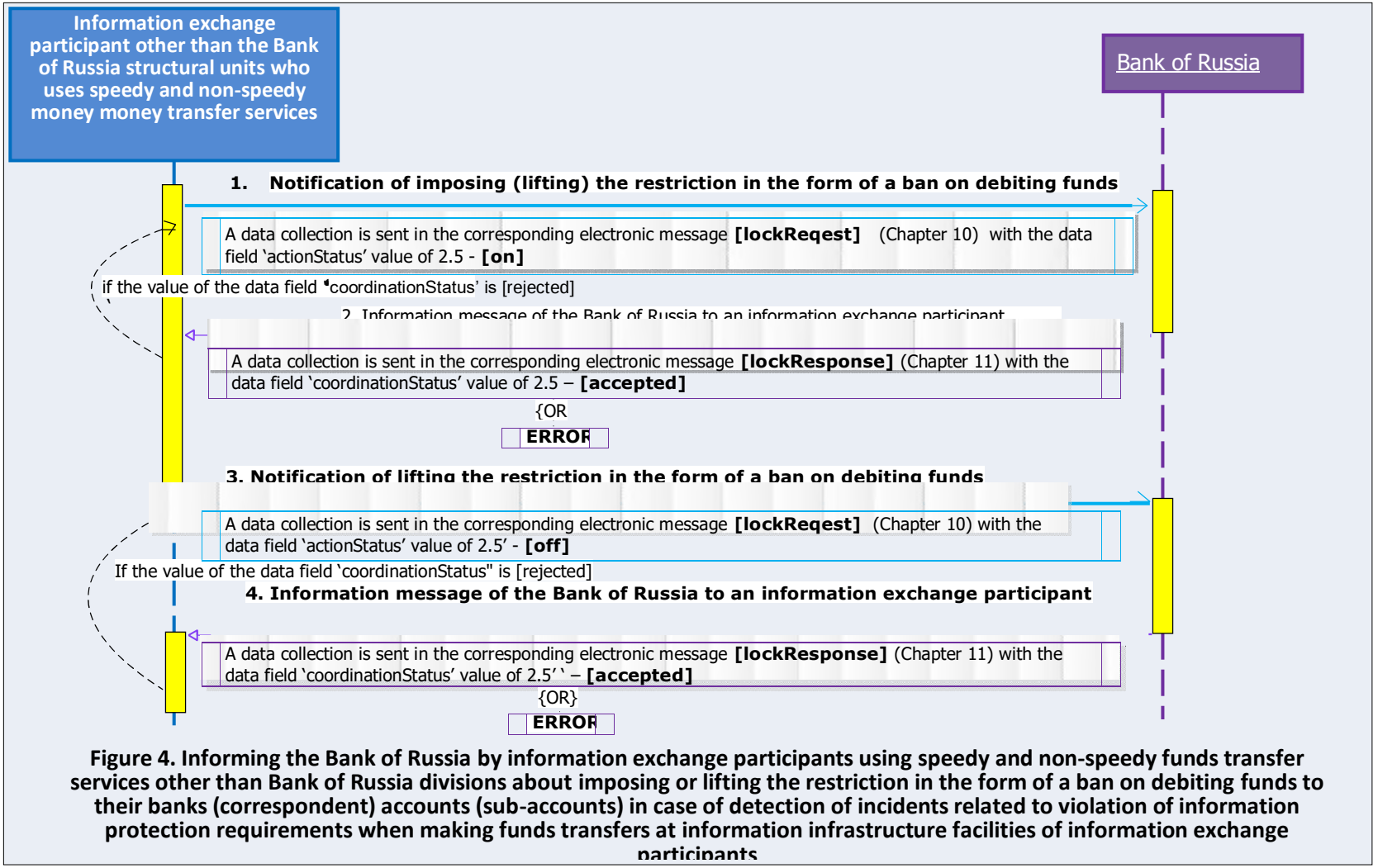

Figure 4. Informing the Bank of Russia by information exchange participants using speedy and non-speedy funds transfer services other than Bank of Russia divisions about imposing or lifting the restriction in the form of a ban on debiting funds to their banks (correspondent) accounts (sub-accounts) in case of detection of incidents related to violation of information protection requirements when making funds transfers at information infrastructure facilities of information exchange participants

3.5 Diagram of transmission by the Bank of Russia of information on detected incidents related to violation of data protection requirements to an information exchange participant

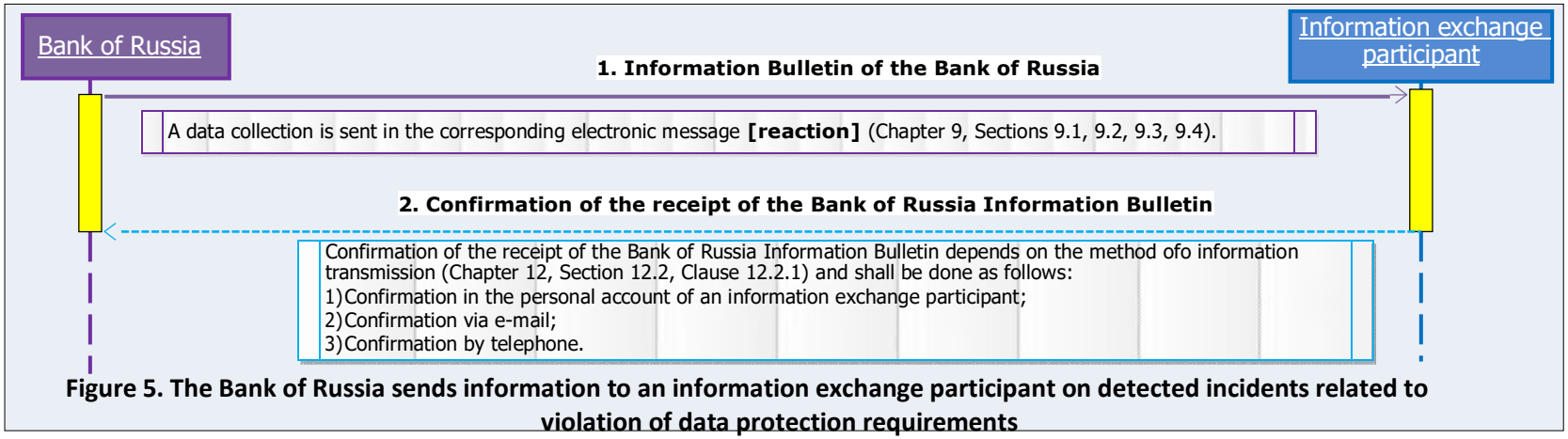

Figure 5. The Bank of Russia sends information to an information exchange participant on detected incidents related to violation of data protection requirements

3.6 Diagram of transmission by an information exchange participant to the Bank of Russia of information on planned measures to disclose information related to violations of data protection requirements

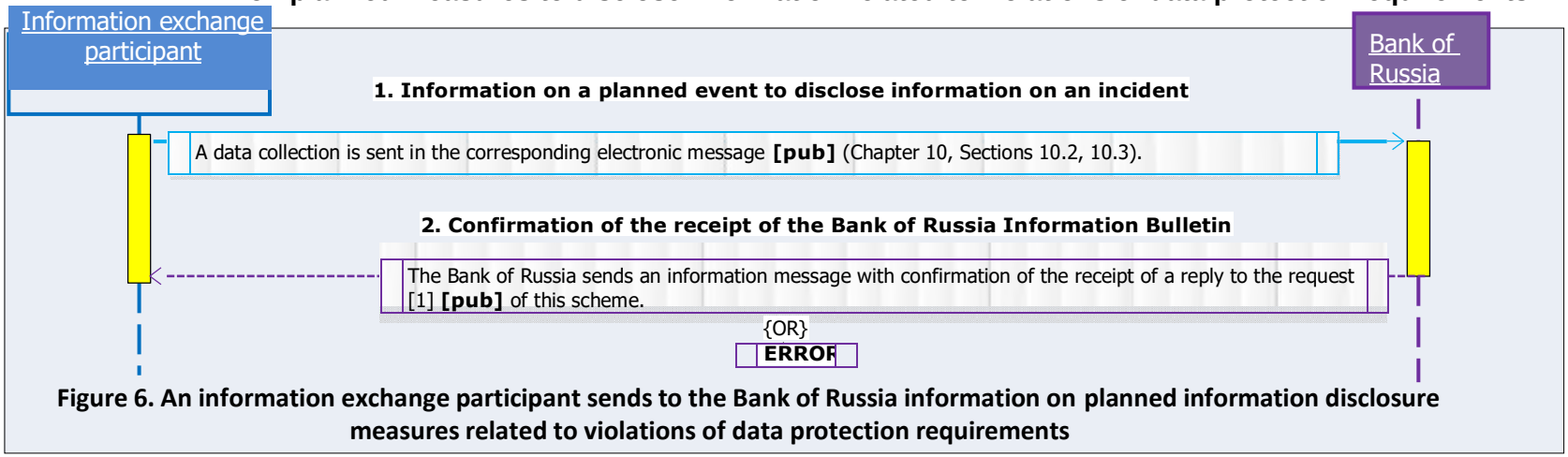

Figure 6. An information exchange participant sends to the Bank of Russia information on planned information disclosure measures related to violations of data protection requirements

3.7 Note:

ERROR - An information message of the Bank of Russia shall be sent as a result of the impossibility to accept the values of the data block (field) from an information exchange participant due to:
- absence of data block (field) value with status [0]; - non-conformance of data block (field) value presentation format; - other technical error.

Dotted lines in Figures 1, 2, 3, 4 show messages and components that are not part of this standard.

The lines are given to represent the interaction between the information exchange participant and the Bank of Russia.

Bibliography

1. Federal Law No. 86-FZ, dated 10 July 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)'.

2. Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System'.

3. Bank of Russia Regulation No. 382-P, dated 9 June 2012, 'On Requirements to Protect Information Related to Funds Transfers and on the Procedure for the Bank of Russia to Control the Compliance with Requirements to Protect Information Related to Funds Transfers'.

4. The Bank of Russia regulation establishing the forms and procedure for sending information by transfer operators, payment system operators, and payment infrastructure service providers to the Bank of Russia on all cases and attempts to make money transfers without the customer's consent and for receiving information from the Bank of Russia, contained in the database of cases and attempts to make money transfers without the customer's consent, and the procedure for taking measures by money transfer operators, payment system operators, and payment infrastructure service providers to counter money transfers without the customer's consent.

5. The Bank of Russia's regulation establishing mandatory requirements for credit institutions to ensure information protection during banking operations.

6. The Bank of Russia's regulation establishing mandatory requirements for non-bank financial institutions to ensure information protection in the course of financial market activities.

7. ISO 8583 – Financial transaction card originated messages – Interchange message specifications – Part 1: Messages, data elements and code values. URL: https://www.iso.org/obp/ui/#iso:std:iso:8583: – 1: ed-1: v1: en (reference date: 25 May 2018).

8. ISO 8583 – Financial transaction card originated messages – Interchange message specifications – Part 2: Application and registration procedures for Institution Identification Codes (IIC). URL: https:// www.iso.org/obp/ui/#iso:std:iso:8583: – 2: ed-1: v1: en (reference date: 24 March 2018).

9. ISO 8583 – Financial transaction card originated messages – Interchange message specifications – Part 3: Maintenance procedures for messages, data elements and code values. URL: https://www.iso.or g/obp/ui/#iso:std:iso:8583: – 3: ed-1: v1: en (reference date: 17 April 2018).

10. ISO 4217 – Codes for the representation of currencies and funds. URL: https://www.iso.org/obp /ui/#iso:std:iso:4217: ed-8: v1: en (reference date: 25 February 2018).

11. RFC3339–DateandTimeontheInternet:Timestamps.URL:https://www.rfc-editor.org/rfc/rfc3339. txt (reference date: 02 February 2018).

12. RFC 791 – Internet Protocol. URL: https://www.rfc-editor.org/rfc/rfc791.txt (reference date: 14 May 2018).

13. RFC 5890 – Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. URL: https://www.rfc-editor.org/rfc/rfc5890.txt (reference date: 08 February 2018).

14. RFC 1034 – Domain names – concepts and facilities. URL: https://www.rfc-editor.org/rfc/rfc1034. txt (reference date: 15 March 2018).

15. RFC 3986– Uniform Resource Identifier (URI): Generic Syntax. URL: https:// www.rfc-editor.org/rfc/rfc3986.txt (reference date: 07 March 2018).

16. RFC 4122 – A Universally Unique IDentifier (UUID) URN Namespace. URL: https:// www.rfc-editor.org/rfc/rfc4122.txt (reference date: 21 April 2018).
17. RFC 997 – Internet numbers. URL: https://www.rfc-editor.org/rfc/rfc997.txt (reference date: 23 January 2018).
18. RFC 5322 – Internet Message Format. URL: https://www.rfc-editor.org/rfc/rfc5322.txt (reference date: 24 January 2018).
19. National Standard of the Russian Federation GOST R ISO/IEC 15408-3-2013 'Information Technology. Security methods and tools. Criteria for assessing information technology security. Part 3. Security trust components'.
20. The Bank of Russia's regulation establishing the forms and procedure for money transfer operators to notify about the suspension of funds crediting to the payee's bank account or the increase in the payee's electronic funds balance, about the impossibility to suspend funds crediting to the payee's bank account or to suspend the increase in the payee's electronic funds balance.
21. The Bank of Russia's regulation establishing requirements for ensuring information protection in the Bank of Russia payment system.
22. Bank of Russia Regulation No. 595-P, dated 6 July 2017, 'On the Bank of Russia Payment System'.
23. ISO 8601:2004 – Data elements and interchange formats – Information interchange – Representation of dates and times. URL: https://www.iso.org/ru/standard/40 874.html (reference date: 29 June 2018).