Anti-Fraud 2.0: New Measures to Combat Cyber Fraud

FAO executives and employees of telecommunications operators, credit institutions, representatives of the business community, and persons wishing to protect themselves against fraudsters

---

Pepeliaev Group advises that the second package of measures aimed at combating cyber fraud has been adopted.

Federal Law No. 210-FZ[1] dated 26 June 2026, commonly referred to as the "second package of anti-cyber fraud measures" (the "Law"), has been adopted. We previously prepared a detailed overview[2] of the initial draft of the legislation during the public consultation stage. However, the text underwent substantial changes during the legislative process, and we therefore present an updated overview of the new provisions.

The new measures are planned to strengthen protection for individuals against cyber fraud. At the same time, they will impose significant financial costs on business. The principal burden will fall on telecommunications operators and the banking sector, while companies operating in other industries (including e-commerce and web hosting) will also incur additional costs.

The key changes include: an obligation for banks and telecommunications operators to reimburse stolen funds; the establishment of an IMEI database, which will be drawn up by telecommunications operators and public authorities; stricter regulation of virtual private branch exchanges (PBXs); an obligation for aggregators to interact with the 'Anti-Fraud' State Information System (SIS); the expansion of the list of lawful mass calls; and the introduction of security certificates issued by the National Certification Authority.

A separate set of amendments concerns the national payment system: the regulation has been strengthened of transfers made without the customer's voluntary consent, while new obligations have been introduced for money transfer operators, a unified payment card register has been established, and certain powers of the Bank of Russia have been expanded.

---

[1] Federal Law No. 210-FZ dated 26 June 2026 On Amending the Federal Law "On Communications" and Certain Legislative Instruments of the Russian Federation.

[2] https://www.pgplaw.ru/analytics-and-brochures/alerts/vtoroy-paket-mer-protivodeystviya-kibermoshennichestvu/

The Law will take effect on the date when it is officially published, but a number of its provisions will be introduced gradually between 1 September 2026 and 1 January 2028.

Below are the principal features of the amendments.

Anti-fraud measures relating to telecommunications operators

Entry into force is planned for 1 March 2027.

1. Telecommunications operators reimbursing funds stolen from individuals

The Law introduces an entirely new mechanism for protecting victims of cyber fraud. A telecommunications operator will be required to reimburse to an individual funds debited without the person's consent or with consent given under the influence of deception or an abuse of trust.

Liability arises where there is a causal link between the telecommunications operator failing to act and the theft. Examples are where the operator has not submitted information about a fraudulent telephone number to the 'Anti-Fraud' SIS, has not suspended telecommunications services in relation to that number, or has not blocked the call when it was detected.

If a telecommunications operator refuses to reimburse the individual, that individual will be entitled to go to court to demand reimbursement.

The Law contains numerous conditions for reimbursement to be possible. More details

A telecommunications operator will be obliged to reimburse stolen funds if all of the following conditions are met:

1) the subscriber number from which the fraudulent call and/or message originated is specified in the agreement with the payment service provider as a means of communication;

2) there is a causal link, namely the transfer to the fraudsters resulted from a call or SMS received from a number displaying signs of fraudulent activity;

3) the telecommunications operator is at fault because the transfer became possible as a result of the telecommunications operator breaching one or more of its duties as follows:

    a) it has not submitted information concerning the victim's subscriber number to the 'Anti-Fraud' SIS;

    b) it has not suspended telecommunications services or the transmission of traffic relating to the fraudulent number after receiving information from the 'Anti-Fraud' SIS;

c) it has not suspended incoming traffic to its network at the time a call from a fraudulent number was established where that number met criteria to be determined subsequently by the Russian Government;

d) it has not suspended telecommunications services relating to the fraudulent number at the time of an on-net call to the victim where that number meets criteria to be determined subsequently by the Russian Government;

4) the payment service provider has duly performed all actions required under parts 3^{1}–3^{5} and 3^{8}–3^{11} of article 8 of the Law on the National Payment System[3] in terms of having verified that the transfer was made voluntarily;

5) at the time of the transfer, the Bank of Russia's database of actual and attempted transfers made without the customer's voluntary consent (article 27(5) of the Law on the National Payment System) contained no information regarding actual or attempted transfers involving the individual concerned;

6) communication was timely – the victim contacted the payment operator no later than ten working days after the transfer was made or after receiving notification of the transfer from the bank;

7) there is a resolution to initiate criminal proceedings – by the time of the reimbursement, the victim holds a resolution to initiate criminal proceedings in relation to the theft.

Pepeliaev Group's Comment

The proposed reimbursement mechanism contains several provisions that may significantly limit its practical application. First, it remains unclear how an individual would be able to prove compliance with all statutory conditions if a telecommunications operator refuses reimbursement. Most of the relevant information (for example, whether information was submitted to the 'Anti-Fraud' SIS or whether a call was blocked in time) is controlled by the operator and stored within its internal systems. Secondly, the condition that criminal proceedings must have been initiated obliges victims to apply to law enforcement authorities, as otherwise they would be unable to bring a court claim.

It should also be noted that a substantial proportion of fraudulent communications are made through messaging applications. However, the obligation to reimburse stolen funds does not extend to providers of messaging services, which creates unequal regulatory conditions compared with telecommunications operators.

[3] Federal Law No. 161-FZ dated 27 June 2011 On the National Payment System.

2. New obligations relating to interaction with the 'Anti-Fraud' SIS

The Law introduces a new requirement for all users of the 'Anti-Fraud' SIS (including telecommunications operators, credit institutions and others): they must not only interact with the system but also detect indicators of unlawful activity and transmit such information to it. The list of these measures will be determined by the Russian Government, in agreement with the Federal Security Service (known in Russian by the acronym FSB).

In terms of complying with this requirement, the Law has established the following obligations for telecommunications operators:

- to identify "fraudulent" numbers – an operator must independently monitor subscriber numbers displaying indicators of fraudulent activity and send information about them to the 'Anti-Fraud' SIS;
- to identify victims' numbers – a similar obligation with respect to numbers receiving calls or messages displaying indicators of fraud;
- to suspend the provision of telecommunications services to subscribers using a "fraudulent" number; and
- to transmit information to the 'Anti-Fraud' SIS.

The Russian Government will establish a list of criteria for identifying "fraudulent" numbers and victims' numbers and a list of the information to be submitted to the 'Anti-Fraud' SIS, as well as specifying the period during which telecommunications services will be suspended for subscribers with "fraudulent" numbers. For international calls there will be labelling and the right to opt out.

In relation to the growing number of fraudulent schemes involving foreign telephone numbers, the Law establishes special rules for incoming international calls[4]:

- telecommunications operators will be required to label international calls. The rules for labelling will be established by the Russian Government;
- the Law grants individuals the right to set a self-imposed ban on incoming calls using foreign numbering resources or coming from the network of a foreign telecommunications operator. The procedure for setting and removing such a restriction will mirror the procedure applicable to self-imposed restrictions on entering into telecommunications service agreements.

3. SIM cards for children

The Law gives individuals the right to notify their telecommunications operator when a subscriber number has been provided to family members under the age of 18 and to specify that person's age. The specific aspects of how such services are provided will be determined by the Russian Government.

---

[4] For the purposes of the Law, an international call means a call made using foreign numbering resources and originating from the network of a foreign telecommunications operator.

Pepeliaev Group's Comment

The need for specific legislative regulation of telecommunications services for minors has been discussed for many years. Most telecommunications operators already offer tariff plans designed to protect children against fraud, spam and inappropriate content, although these services have until now been voluntary and subject to additional payment. The amendments that have been adopted establish a legal basis for uniform standards for such protection to be introduced through secondary legislation and for the protection to be free of charge.

4. Prohibition on terminating telecommunications service agreements during the first 90 days

The amendments introduce a new restriction applicable to individual subscribers: they may not terminate a telecommunications service agreement during the first 90 days after a subscriber number is allocated to them.

Where a subscriber nevertheless submits a termination request before the 90-day period expires, the telecommunications operator must suspend providing telecommunications services without charging any fees.

5. New requirements for virtual private branch exchanges (PBXs)

The Law introduces the following requirements concerning the use of virtual PBXs:

- an obligation for telecommunications operators to submit information on subscriber numbers and virtual PBX network addresses to the State Information System for Countering Computer Attacks[5];
- a prohibition on providing telecommunications services using virtual PBXs. This requirement is particularly relevant in light of the draft order that the Ministry of Digital Development recently published requiring lawful interception systems to be installed when virtual PBXs are used[6].

6. Expansion of the list of lawful mass calls that may be made without subscriber consent

The current version of article 44.1-1 of the Law on Communications[7] recognises only one category of lawful mass calls that may be made without the subscriber's consent: calls initiated by public authorities, organisations subordinate to them, local authorities, their subordinate organisations, and other authorities or organisations designated by the Russian Government.

---

[5] The State Information System for Monitoring Compliance by Telecommunications Operators with Their Obligations in Providing Communications Services.

[6] The Draft Order of the Russian Ministry of Digital Development of Russia On Approving the Requirements for Using Switching Equipment when Operating Virtual Telephone Exchanges… (Draft ID: 168689).

[7] Federal Law No. 126-FZ dated 7 July 2003 On Communications.

It is planned to add the following grounds to this list:

- calls made for the purpose of providing information where such notification is required by Russian legislation. The organisation initiating the mass calls must inform recipients that the calls are legitimate under the law;
- calls initiated by credit institutions for customer notification purposes pursuant to an agreement with the customer, where such notification is provided for by Russian legislation. The organisation initiating the mass calls must inform recipients that the calls are legitimate by virtue of the relevant contract.

Pepeliaev Group's Comment

The existing regulatory framework created significant practical difficulties for organisations for which telephone communication with customers forms an integral part of their activities, including research organisations, credit institutions, utility companies and others. Expanding the list of permitted cases is planned to remove these obstacles. Importantly, the new grounds are strictly linked to there being either statutory notification requirements or a contractual relationship, and they are accompanied by an obligation to inform subscribers of the legitimate basis for the call. In doing so, the legislature is seeking to maintain a balance between the interests of business and protecting the public against unwanted calls.

7. Creation of an IMEI database

The Law provides that a database will be established of International Mobile Equipment Identity (IMEI) numbers containing information on devices that are either prohibited or permitted for use within Russia.

Information about IMEI will be entered into the database by telecommunications operators and also by public authorities on a list that the Russian Government will approve.

The Russian Government will establish the rules for how the IMEI database will function and will approve its operator. The Ministry of Digital Development will establish the procedure governing how telecommunications operators will interact with the database operator.

Pepeliaev Group's Comment

The Law establishes only the general concept of the IMEI database, leaving the key operational issues to be addressed through secondary legislation. However, it is precisely these rules that will determine how important practical matters are resolved, including the treatment of duplicated, cloned and invalid IMEI numbers, the handling of eSIMs, IoT/M2M devices, modems and POS terminals, the procedure for processing information when devices are repaired or a motherboard is replaced, and the rules for foreign subscribers using roaming services. Until the relevant rules have been approved, telecommunications operators and participants in the secondary device market will lack legal certainty regarding their obligations.

8. Am obligation for telecommunications operators to terminate agreements with foreign subscribers where verification procedures have not been completed

Between 8 August 2024 and 1 July 2025, telecommunications operators were required to verify foreign nationals and stateless persons for compliance with the requirements for which articles 44 and 45.1 of the Law on Communications provide (for example, regarding the quantity of subscriber numbers and the inclusion of IMEI information in agreements with operators)[8]. Where such verification was not completed, an operator was obliged to cease providing telecommunications services. The Law, in turn, introduces an obligation to terminate such agreements rather than to cease providing services.

This amendment will enter into force from the time when the Law is officially published.

9. A telecommunications operator not meeting its obligations as a ground for terminating the provision of telecommunications services

The amendments change the grounds for the provision of telecommunications services to be terminated at the request of operational investigative authorities or pursuant to an order issued by the telecommunications regulator Roskomnadzor. Instead of the previous ground, stipulated by article 46(1)(9) of the Law on Communications and linked to the liquidation of a subscriber that was a legal entity or individual entrepreneur, a broader ground is being introduced: the failure by a telecommunications operator to comply with its statutory obligations and the rules for the provision of telecommunications services. In such cases, the telecommunications operator must terminate the provision of telecommunications services on the day after the relevant request or order is received.

[8] This obligation was introduced by article 5(7) of Federal Law No. 303-FZ dated 8 August 2024 On Amending the Federal Law "On Communications" and Certain Legislative Instruments of the Russian Federation.

Measures to Combat Fraud Relating to the Activities of Credit Institutions

1. New Sources of Information for Verifying Transactions

When checking for indications that a transfer of funds has been carried out without the client's voluntary consent, money transfer operators will use information from the 'Anti-Fraud' SIS.

Money transfer operators will also submit to the 'Anti-Fraud' SIS information about the subscriber numbers used when servicing a client, and to the Bank of Russia information about clients and/or their electronic means of payment for the purpose of creating a database of cases and attempted transfers of funds without the client's voluntary consent (the "Database").

The Bank of Russia will transfer information from the Database to the 'Anti-Fraud' SIS. Information in the Database will be retained for one year when it is first included and for three years following any subsequent inclusion. For mobile telephone subscriber numbers, a period of 180 days has been set. If criminal proceedings are discontinued, information relating to the client and/or the client's electronic means of payment will be removed ahead of schedule.

The amendments are planned to enter into force on 1 March 2027.

2. Information Security Tools and the Rejection of a Transaction

Money transfer operators will be obliged to use information security tools designed to protect against malicious software in relation to the software they provide for use by individual clients when making transfers, including mobile applications and official websites.

Such security tools must undergo a conformity assessment in accordance with the requirements of Russian legislation in the field of information security and must detect the impact of malicious software before the client's funds are debited.

Individual clients must be given the opportunity to use such security tools on their devices, subject to their consent. By 1 September 2027, money transfer operators must incorporate the relevant provisions into agreements with individual clients and obtain from them either consent to having such security tools installs or a refusal of such consent.

Information concerning the impact of malicious software, together with information received from the 'Anti-Fraud' SIS, will be included in the list of information used to identify transactions that correspond to the characteristics of transfers made without the client's voluntary consent.

Where information indicating the impact of malicious software is available, the money transfer operator must refuse to accept the client's payment instruction for execution or refuse to carry out a transaction using payment cards, electronic money transfers or transfers made via the Bank of Russia's Faster Payments System, where the transaction is initiated using the relevant user device. The client is informed of the reasons for the refusal and of the

opportunity to make the transfer using another device or by attending the money transfer operator in person.

The amendments are planned to enter into force on 1 March 2027.

3. A Six-Hour Cooling-Off Period and Reimbursing the Client

Where a client confirms an electronic payment instruction or attempts to repeat a transaction, the money transfer operator is entitled, for a period of six hours, to refrain from executing the payment instruction, refuse to carry out the repeated transaction, or decline to process any subsequent repeated transactions.

After the six-hour period expires, the money transfer operator must execute the payment instruction or carry out the subsequent repeated transaction if there are no other statutory grounds for refusal. We stress that this rule applies unless article 8(3.10) of the Law on the National Payment System provides otherwise.

A money transfer operator servicing a payer will be obliged to reimburse an individual client for the amount of a transfer or transaction carried out without the client's voluntary consent where, after receiving information from the 'Anti-Fraud' SIS, the money transfer operator executes the payment instruction or carries out the transaction in breach of the applicable requirements. A separate ground for reimbursement is where the money transfer operator does not perform the obligation to refuse the transaction when there is information about the impact of malicious software.

Reimbursement must be made no later than 30 days after the client submits a claim, provided that a resolution has been issued instituting criminal proceedings in connection with the theft of funds.

The amendments are planned to enter into force on 1 March 2027.

4. Transactions Involving Telephone Calls and Short Text Messages

A special claims procedure is being introduced for transfers and other payment transactions carried out without the voluntary consent of an individual client as a result of telephone calls and/or short text messages.

The client is entitled to submit a claim for reimbursement no later than 10 working days after the date of the transaction or after receiving notification of the transaction from the money transfer operator. Where the money transfer operator has duly complied with the established requirements and the 'Anti-Fraud' SIS does not contain the information prescribed by law, the claim must be submitted to the telecommunications operator.

In other cases, the money transfer operator must deal with the client's claim in accordance with the reimbursement procedure and may not refuse reimbursement solely because the 10-day deadline has been missed.

The amendments are planned to enter into force on 1 March 2027.

5. Transactions Involving Digital Roubles

The operator of the digital rouble platform will receive a right to refuse to execute a transaction involving digital roubles where the Database contains relevant information.

At the same time, the regulation of transactions with digital roubles will no longer be linked to indicators of transfers being made without the client's voluntary consent established by the Bank of Russia.

The amendments are planned to enter into force on 1 March 2027.

6. Payment Cards, the Unified Payment Card Register and Banking Confidentiality

From 1 March 2027, the regulation of electronic means of payment will be clarified. The types of electronic means of payment, the conditions governing their issuance and distribution, the procedures for carrying out transactions, transaction documentation and the requirements applicable to internal banking rules will all be established by a regulatory instrument of the Bank of Russia.

From 1 September 2027, an individual client may have no more than twenty payment cards issued in total, which may be used to carry out transfers of funds. The Board of Directors of the Bank of Russia will be able to establish a higher limit on the number of cards. Before issuing a payment card, the money transfer operator must obtain information from the Unified Payment Card Register. Where the applicable limit has already been exceeded, the operator must refuse to issue the payment card.

From 1 September 2026, a Unified Payment Card Register will be established. The operator of the Register will be the operator of the National Payment Card System, while its users will be the Bank of Russia and money transfer operators. The Register will contain information on payment card numbers and types, the taxpayer identification numbers (TINs) of individual clients, and the total number of payment cards issued to each client. From the same date, money transfer operators, including credit institutions and branches of foreign banks acting as money transfer operators, must submit information to the Register concerning payment cards that have been issued and terminated, the types of such cards, and the TINs obtained from clients.

The Bank of Russia will be entitled to obtain information from the Register. The operator of the Register has no right to disclose to third parties information constituting a banking secret and will be liable for any such disclosure, including to compensate any damage.

7. Supervisory Powers of the Bank of Russia

The Bank of Russia will be able to obtain from credit institutions information and documents relating to measures implemented to prevent transfers of funds from being carried out without the client's consent or with consent obtained through deception or an abuse of trust.

Such information and documents will be added to the list of information that the Bank of Russia is entitled to request in exercising its supervisory powers over credit institutions.

The amendments are planned to enter into force on 1 March 2027.

Other Anti-Fraud Measures

1. Obligation for Online Platform Operators to Connect to the 'Anti-Fraud' SIS

The Law obliges operators of intermediary online platforms to interact with the 'Anti-Fraud' SIS. The procedure and conditions for such interaction will be established by the Russian Government.

The amendments are planned to enter into force on 1 March 2027.

2. Right to Report Fraud via the SIS

An individual against whom unlawful acts have been committed will be entitled to submit information about this directly to the 'Anti-Fraud' SIS through the Gosuslugi government services portal. The procedure governing the use of such information will be established by the Russian Government in coordination with the Federal Security Service (known in Russian by the acronym FSB).

The amendments are planned to enter into force on 1 March 2027.

3. Restrictions on the Circulation of Radio-Electronic Equipment Using Foreign Satellite Communication Systems

Currently, article 71(3) of the Law on Communications prohibits the import into the Russian Federation of radio-electronic equipment intended for transmitting and/or receiving radio signals from foreign space communication facilities (communication satellites, including dual-use satellites) where no decision has been issued by the State Commission for Radio Frequencies allocating the relevant radio frequency bands. In pursuance of this restriction, the Law introduces a ban on the sale of such equipment and on the dissemination of information offering such equipment for sale. This applies, in particular, to Starlink satellite terminals and other similar devices. Any such offers that appear will be included in the register of prohibited information for which article 15.1 of the Law on Information provides.

The amendments are planned to enter into force on 1 March 2027.

4. Prohibition on Hosting Services for Owners of Blocked Resources

The Law prohibits hosting providers from supplying services to the owners of websites, information systems and software that provide access to resources blocked within Russian Federation.

This amendment enters into force on the date when the Law is officially published.

5. Restriction of Access to Information Facilitating the Distribution of Malicious Software

The Law expands the list of information that is subject to access restrictions so it includes information enabling software to be identified that is designed for unauthorised access to information, and for the destruction, modification, blocking, copying, disclosure or dissemination of such information, as well as offers to acquire such software.

This amendment enters into force on the date when the Law is officially published.

6. Identification of the Users of Messenger Services by Subscriber Number

Operators of multifunctional messaging services will be entitled to identify users by means of their subscriber numbers using the State Information System for Monitoring Compliance by Telecommunications Operators with Their Obligations in Providing Communications Services. The identification procedure will be established by the Russian Government.

The amendments are planned to enter into force on 1 March 2027.

7. Security Certificates Issued by the National Certification Authority (NCA)

The Law introduces a new category of certificates, namely NCA security certificates. These will be used:

- to ensure that interaction with information systems and websites is secure and reliable, as well as to authenticate such systems and sites;
- to confirm the integrity and Russian origin of software included in the national software register;
- to authenticate and protect those involved in electronic interaction within corporate information systems.

Several categories of certificates are established depending on the purpose they are used for. Security certificates will be distinguished depending on whether the information they contain concerns:

- an information system or website;
- the ownership of an information system or website;
- a developer of software from the national software register;
- those involved in electronic interaction within a corporate information system;

as well as a security certificate that is designed for creating all the other certificates.

The use of security certificates will be mandatory for: the holders of licences relating to encryption (cryptographic) tools used to access information on websites; developers of Russian software from the list approved by the Russian

Government; and organisations and public authorities engaged in interacting electronically with individuals and legal entities in accordance with article 13(2(3)) of the Law on Information. The Russian Government is entitled to establish additional cases where the use of such certificates will be mandatory.

The Law also introduces two new concepts, an identification key and an authentication key, which are intended for a security certificate to be obtained. The NCA must refuse to issue a certificate where the applicant has not confirmed possession of an identification key or where the authentication key is not unique.

The amendments are planned to enter into force on 1 March 2027.

What to Think About, What to Do

Organisations should identify which of the new requirements introduced by the Law affect their activities, and should assess the scope of the changes that will be required.

Telecommunications operators and credit institutions should pay particular attention to the Law, as it places the greatest compliance burden on them, namely: the creation of the IMEI database; integration with the 'Anti-Fraud' SIS; new procedures for verifying payment transactions; limits for payment cards; and the protection of applications against malicious software.

The owners of aggregator services need in advance to work through how to connect to the 'Anti-Fraud' SIS. Developers of software included in the list approved by the Russian Government and holders of licences relating to encryption (cryptographic) tools should also clarify beforehand the procedural requirements for obtaining NCA security certificates.

Given that the amendments will enter into force in stages, organisations are advised to begin preparing now by doing the following: introducing or updating internal compliance procedures; appointing responsible personnel; and allocating a sufficient budget for the necessary upgrading of IT infrastructure.

We recommend closely monitoring the law-making activities of the Russian Government and the relevant regulatory authorities and, where possible, participating in consultation exercises regarding draft regulations, as subordinate legislation will determine the detail of how the new obligations will be implemented in practical terms.

Help from Your Adviser

Pepeliaev Group's specialists have extensive experience of advising telecommunications operators, credit institutions and other organisations on legal matters.

We are ready to provide comprehensive legal support to companies in:

- determining what risks there are in view of the Law being adopted;
- preparing legal positions on contentious issues arising from the Law being adopted;

- developing internal regulations and procedures necessary to ensure compliance with the Law's provisions;
- representing clients in their interactions with public authorities.

Contact details

Natalia Kovalenko
Partner

T: +7 (495) 767 00 07
n.kovalenko@pgplaw.ru

Lidia Gorshkova
Partner

T: +7 (495) 767 00 07
l.gorshkova@pgplaw.ru