The law on countering cyber fraud has come into effect

FAO heads and employees of telecom service providers, credit institutions and businesses using mass calling, and persons who want to protect themselves against scammers

---

Pepeliaev Group advises that, on 1 June 2025, the law on countering cyber fraud came into force (the "Law").[1] Telecom service providers and credit institutions are now obliged to comply with the newly introduced security measures. However, having been passed within tight deadlines, the Law contains conceptual drawbacks that may lead to adverse consequences for market participants.

It is stipulated that a state information system will be created to enable data to be exchanged in real time between government bodies, telecom service providers and banking institutions.

The Law introduces definitions for 'virtual telephone exchanges' (VTEs) and SIM boxes. It obliges the Russian federal government to regulate how communication services are provided using such equipment; imposes restrictions on mass calling; mandates call labelling; and introduces other security measures.

As for the financial sector, the Law obliges credit institutions to introduce restrictions on ATM cash withdrawals, to keep records of powers of attorney based on which cash is withdrawn, and introduces a definition of an 'authorised person for carrying out banking operations'.

The state information system

The Law provides for a state information system (SIS) to be created to counter offences using Internet technologies. The Russian Ministry of Digital Development, Communications and the Mass Media (the 'Digital Ministry') will operate the system.

The SIS will store data on individuals involved in unlawful activities and information relating to subscribers' numbers linked to attempted fraudulent actions.

---

[1] Federal Law No. 41- FZ "On establishing a state information system to counter offences committed using information and communication technologies and on amending certain items of legislation of the Russian Federation" dated 1 April 2025. Some provisions of the Law will come into force after 1 June 2025.

The Government will determine the exact list of information and how it will be accessed.

Telecom service operators, credit institutions, messaging services, hosting providers, owners of widely used social networks[2] and other persons will be required to submit data to the SIS.

In addition to storing data and exchanging it online, the SIS will promptly put a stop to offences and independently forward information to law enforcement bodies.

Access to the SIS will be granted to the General Prosecutor's Office, the Investigative Committee, the Bank of Russia, credit institutions and telecom service providers, as well as other competent government bodies and organisations, the list of which will be approved by the Government.

These provisions will come into effect on 1 March 2026.

Security measures connected with the activity of telecom service providers

The new developments relating to the activities of telecom service providers will come into effect on 1 September 2025.

Enshrining the definitions of 'virtual telephone exchanges' and SIM boxes in legislation

Telephone scammers exploit VTEs and SIM boxes to anonymise operations and bypass anti-fraud systems. The Concept of the system to counter illegal acts that are committed using information technologies[3] highlights that operations of VTEs must be regulated by law.

The Law enshrines the definitions of VTEs and SIM boxes ("subscriber traffic gateway terminals") and introduces an obligation of the Government to regulate the Rules for providing communication services using the above equipment.

---

[2] Over 500,000 users per day.

[3] The Government's Directive No. 4154-r "On approving the concept of a state system to counter illegal acts committed using information and communication technologies" dated 30 December 2024.

- **VTEs** means a communication tool designed to enable a subscriber to use telecom services, perform switching functions and route traffic within a telecom network.
- **Subscriber traffic gateway terminal** means user equipment (data terminal equipment) that employs software and radio-electronic tools and is designed to route traffic between communication networks and/or data transmission networks, with the opportunity for multiple SIM modules to be used simultaneously.

It is not permitted to use VTEs and SIM boxes in violation of the requirements established by the Law "On communications"[4] or the rules for the supply of communication services.

State Duma deputy Sergey Boyarsky noted on his Telegram channel that the ban on VTEs/SIM boxes being used may not fully tackle the issue of their essence, owing to which further solutions need to be devised.[5]

Restrictions on mass calling

Mass calling is permitted only if a subscriber has provided consent which is "expressed through the actions [of the subscriber] that unequivocally identify the subscriber and reliably confirm their willingness to receive mass calls."

Pepeliaev Group's comment

The Law does not define criteria for what constitutes a mass call. It cannot be ruled out that telecom service providers will interpret the definition differently, potentially leading to disputes with subscribers.

According to the letter of the Law, a subscriber must explicitly consent to receiving mass calls. Otherwise, such calls will be deemed "unlawful", at least in theory. It will be interesting to see how this provision is implemented in practice.

For the ambiguities to be resolved, we anticipate that the Government will draw up relevant regulations. In the absence of those, courts will determine what constitutes 'mass' calls and how a subscriber's consent should be obtained.

[4] Federal Law No. 126-FZ "On communications" dated 7 July 2003
[5] https://t.me/sergeyboyarskiy24/1217

A self-imposed ban on SIM cards being registered remotely

When a contract for communication services is concluded remotely, the service provider will be obliged to verify whether individuals have a self-imposed ban on a SIM card being registered. Individuals may impose the ban via the public service app Gosuslugi or by personally visiting a public service centre.

Prohibiting phone numbers from being transferred to third parties

The Law establishes a prohibition on subscribers' numbers being transferred to third parties, except for family members and/or close relatives, as well as persons a list of whom the Government will determine.

The liability for a subscriber's number being unlawfully used will be imposed the persons who own the number on legal grounds.

The obligation to label a call

A telecom service provider from whose network a call is initiated is obliged to demonstrate details regarding a legal entity or an individual entrepreneur who has initiated the call.

The Ministry has prepared a draft Resolution[6] under which legal entities/ individual entrepreneurs are obliged to enter into a contract with a telecom service provider for the details to be reflected for a person who accepts the call. The contract should specify information regarding the activities of the legal entity/individual entrepreneur, the telephone numbers assigned to them and the category of calls.

Based on the data provided to it, the telecom service provider will transmit the following information to the subscriber's phone:

- the full or abbreviated name or trademark (if any) of the legal entity/individual entrepreneur;
- the category of the telephone call;
- additional information related to the legal entity/sole entrepreneur's activity.

The information will be transmitted to the phone in the format of text limited to 32 characters.

---

[6] The Government's draft Resolution "On approving the Rules, deadlines and format for a telecom service provider from whose network a telephone call to user equipment (data terminal equipment) is initiated to transmit details about the subscriber that is a legal entity or an individual entrepreneur initiating the call, as well as the content of such information. // Draft's ID: 156527 // You can access the draft at: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=156527. The draft is undergoing public discussions.

The legal entity/individual entrepreneur or the service provider from whose network the call is initiated will be obliged to provide the receiving service provider with details regarding the legal entity/individual entrepreneur and regarding the telephone numbers from which calls will be made.

Pepeliaev Group's comment

It cannot be ruled out that the costs on setting up labelling of calls will trigger increased prices for services that will ultimately be passed on to end consumers.

The new development will come into effect on 1 September 2025.

Receiving an SMS only after the call is over

Typically, scammers demand an SMS with a password from the public service portal Gosuslugi during a call. It is considered acceptable that SMS may only be delivered after the call has ended.

Restricting mass messaging

A subscriber may opt out of mass messaging by submitting a relevant application to their service provider.

The new development will come into effect on 1 August 2025.

Security measures connected with the activity of credit institutions

The provisions in this part of the Law will come into effect on 1 September 2025

New rules for cash withdrawals

A bank that has issued a payment card (the 'Bank') will be obliged to verify that the client has voluntarily consented to cash withdrawals from ATMs.

If 'involuntary' consent is detected, the Bank must impose a 48-hour cash withdrawal limit of no more than RUB 50,000 per day. The Bank will notify the client of such a limit.

Additionally, the Bank will limit ATM cash withdrawals by a client to no more than RUB 100,000 per month if it receives information from the Bank of Russia that the client and/or their means of payment are listed in its database of money transfers performed or attempted without the client's voluntary consent.[7] The limitation will remain in place until the relevant data is removed from the Bank of Russia's database.

[7] The Bank of Russia will maintain the above database under article 27(5) of Federal Law No. 161-FZ "On the national payment system" dated 27 June 2011.

The Law also makes more specific the procedure for cash withdrawals by a client through a proxy: when a power of attorney to withdraw cash on behalf of a client is presented, the Bank must record the fact of it being presented and arrange for a copy of the power of attorney to be kept for 5 years from the date on which it was presented or the cash was withdrawn.

Pepeliaev Group's comment

The concept of 'voluntary consent of the client' is not new to Russian legislation.

Operators of money transfers, of payment systems and of electronic platforms as well as service providers of payment infrastructure are obliged to implement measures to counter money transfers in the absence of a client's voluntary consent (article 27(4) of Federal Law No. 161-FZ). The Bank of Russia has set out detailed information on how the above countermeasures will be implemented in its Instruction No. 5371-U dated 19 August 2024 as well as the indicators of unauthorised money transfers in its Order No. OD-1027 dated 27 June 2024.

It can be anticipated that the Bank of Russia will introduce similar regulation for cash withdrawals.

Persons authorised to carry out banking transactions

The Law introduces the concept of a person authorised to carry out banking transactions (the 'Authorised Person'), whom a client may select to oversee transactions in their accounts.

An Authorised Person cannot be a person who has been included in the list of companies and individuals who are known to be involved in extremist or terrorist activities. The Law does not impose any other restrictions.

Banks are obliged to publish on their websites and in their mobile applications information on whether clients may use the services of authorised persons. Banks may also publish details of the procedures of how a person may be assigned the status of an Authorised Person or have it taken away, the requirements for an Authorised Person and the terms and conditions on which an Authorised Person will carry out their mandate.

The essence of legal relationships involving an Authorised Person is as follows:

- Before the Bank executes a transaction to transfer client's money or to dispense cash to the client (including via ATMs), it must seek confirmation of such transactions from the Authorised Person.
- The Bank must simultaneously notify the client of such a request.

- The Bank should receive such confirmation (or rejection) no later than 12 hours after the relevant request was forwarded to the Authorised Person.

- Based on the response of the Authorised Person, the Bank will either proceed or decline the client's transaction.

The client has a right to individually select which transactions and bank accounts (deposits) require confirmation from the Authorised Person. The new procedure, however, does not apply to transactions that involve using electronic money.

The Bank is obliged to:

- Suspend all transactions to transfer client's money until it receives confirmation from the Authorised Person.

- Decline to carry out transactions involving payment cards, the Bank of Russia's Faster Payments System or cash withdrawals if such transactions are subject to a regime requiring that confirmation be obtained from the Authorised Person.

The Authorised Person's powers will be defined in a special agreement between the Bank, the client and the Authorised Person, specifying, among other things, the fees of the credit institution for notifying the Authorised Person and the list of transactions to be confirmed.

The Authorised Person will be deprived of their status on the next day after the Bank's client submits a notice to this effect to the Bank.

Other security measures

A ban on using foreign messaging apps

Scammers frequently use messaging apps to interact with their victims. The Law prohibits telecom service providers, credit institutions, government bodies and other persons from using foreign messaging apps when dealing with citizens.

The ban will come into effect on 1 June 2025.

Using biometrics

Services that publish advertisements may impose a requirement that an individual's identity be verified by way of biometrics. For those opting for biometric verification via the public services portal Gosuslugi, the service will have to arrange for such option.

The new development will come into effect on 1 March 2026.

What to think about and what to do

It is essential to monitor how the Government draws up and adopts regulations governing the supply of communication services using VTEs and SIM boxes and the submission of data to the SIS, as well as establishing criteria for defining mass calls. Business processes should be adjusted in good time to comply with the new requirements.

Credit institutions handling transactions in individuals' accounts should also prepare to fulfil the new obligations.

Help from your adviser

Pepeliaev Group's specialists have significant experience of advising telecom service providers, credit and other institutions on legal matters.

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

- determining the risks in connection with the Law being passed;
- developing a legal position in relation to contentious matters that arise in connection with the Law being applied;
- drafting internal regulations and devising procedures that are required to comply with the new requirements;
- representing clients in disputes with governmental authorities and subscribers.

Contact details

Natalia Kovalenko
Partner

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

Lidia Gorshkova
Head of Banking & Finance Practice

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