

Regulation on Remote Identity Verification and Remote Contract Execution of Banks Published in Official Gazette

15 Apr 2021

The Regulation on Remote Identification Methods to be Used by Banks and Establishment of Contractual Relations in Electronic Environment ("**Regulation**") was published in the Official Gazette numbered 31441, on 1 April 2021. With the regulation, it became possible to perform identity verification transactions by video calling online without the need for the customer representative and the customer to be physically present at the same environment. In addition, after identity verification was made remotely or through branches, it became possible to establish remote banking contracts. The Regulation will become effective as of 1 May 2021.

The important provisions included in the Regulation are briefly as follows:

- Remote identification process is considered as a critical operation and systems to be used for remote identification are considered as critical information systems.
- In the remote identification process to be implemented within the scope of the Regulation, only the biometric data among the special categories of personal data can be used, and in this case the explicit consent of the customer is recorded electronically.
- The video call phase of remote identification is done in real time and without interruption. The image quality must allow the examination of security elements to visually verify the submitted document under white light and to check that the presented document has not been worn or tampered with.
- In the remote identification process, an identification document with security elements, photograph and signature that can be visually distinguished under white light is used.
- When the identity information on the chip of the ID document is verified by using near field communication, the necessary match is considered to be provided for identification of the customer.
- If verification cannot be possible using near field communication for any reason, it is ensured that at least four of the visual security elements of the ID document are verified in terms of form and content. In cases where only visual security elements are verified, the bank additionally requires that the first financial transaction be made from the account of the person in another bank, where the principles of recognition of the customer are applied, before establishing a permanent business relationship with the person.
- In the video call stage of remote identification, methods to detect the vitality of the person must be used. The bank must take additional measures to prevent the risks associated with deepfake technology.
- In the process of remote identification, biometric comparison of the person's face with the photo (i) on the chip if it can be taken from the identity document using near field communication, (ii) and if not, the photo on the identity card, is compared.
- At the end of the video call stage of remote identification, the process is completed by informing the person about the banking services to be provided and verbal confirmation that he / she accepts to be a bank customer.

- The bank must monitor the persons identified by remote identification in a different risk profile. Additional security and control methods must be applied depending on the type and amount of the transaction made by these persons. In the event of an objection to transactions that cause liability to individuals or a third party, the burden of proof lies with the bank.
- Following the remote identification or face-to-face identification of the customer through branches; in case the contractual relationship is established at a distance from internet banking or mobile banking distribution channels, the declaration of will of the customer must be received through the said distribution channels after identity verification.
- In order to establish a contractual relationship that can replace the written form via an information or communication device for the transactions requested by the customers, (i) the Bank must provide all the terms of the contract to the customer through internet banking or mobile banking distribution channels (ii) together with the contract communicated to the customer, the declaration of will of the customer establishing the contract must be signed with the customer-specific encryption secret key and transmitted to the bank, (iii) measures must be taken to ensure that the customer is signed the contract that is aligned with the information provided to the customer.

You can find the full Turkish text of the Regulation published in Official Gazette dated 1 April 2021, and numbered 31441, at this [link](#). (Only available in Turkish.)

Related Practices

- [Financial Markets and Services](#)
- [Privacy and Data Protection](#)

Related Attorneys

- [BURCU TUZCU ERSİN, LL.M.](#)