



Turkey: New Regulation on Remote Customer Identification

Authors: Gönenç Gürkaynak, Esq., Nazlı Nil Yukaruç and Büşra Üstüntaş of ELIG Gürkaynak Attorneys-at-law

I. General Overview

The Regulation on Remote Identification Methods to be used by Banks and the Establishment of Contractual Relationships in Electronic Media (“**Regulation**”) was published in the Official Gazette dated April 1, 2021 and numbered 31441 and entered into force after one month as of its publication. The Regulation was prepared based on the Draft Communiqué on Remote Identification Methods to be used by Banks, which was published by the Banking Regulatory and Supervisory Authority (“**BRSA**”) as presented to the public opinion¹.

The provisions of the draft communiqué were mainly reflected to the Regulation in terms of the remote identification method that banks may use for new customers and verification of customer identity. Unlike the draft communiqué, the Regulation also regulates the terms regarding the establishment of contractual relationships in electronic media following remote identification. This article will focus on the significant provisions of the Regulation.

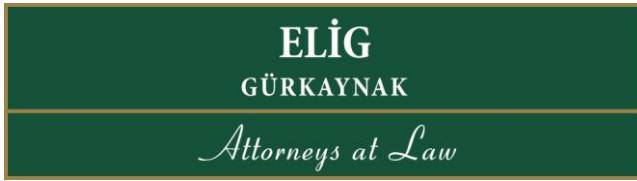
II. General Principles Applied to the Remote Identification

Remote identification process is carried out between the potential customer and customer representative through online video call and without requiring physical presence of the customer.

Before the implementation of the remote identification process, documents related to the process are created and the effectiveness of the process is tested. The process is not implemented unless the efficiency and competence of the process is ensured. Article 4/8 of the Regulation also obliges banks to review the remote identification process at least twice a year and under certain circumstances, such as detection of security breaches and fraudulent activities.

Under Article 5/1 of the Regulation, the video call phase of the remote identification is carried out by a trained customer representative. It must be ensured that the customer representative learns the characteristics of the documents that can be used for identification and the valid verification methods applied for these documents, and is informed about the actions that may

¹ Please see our article on the Draft Communiqué on Remote Identification Methods to be used by Banks: <https://www.mondaq.com/turkey/financial-services/1020694/digital-revolution-remote-customer-identification-in-banking-sector>



constitute fraud or forgery as well as the obligations contained in the Regulation and other relevant legislation.

III. Remote Identification Methods

According to Article 6/1 of the Regulation, the identification process is initiated upon customer completing an electronic form. Risk assessment is performed for the potential customer by using the data obtained and if necessary process is ended before initiating the video call.

During the remote identification process, customer's sensitive personal data, other than their biometric data, cannot be processed and customer's explicit consent must be received for processing such data.

Remote identification via video calls must be made in real time and uninterruptedly. It should also be ensured that the integrity and confidentiality of the audiovisual communication between the customer representative and the potential customer is at an adequate level. For this purpose, the call must be carried out with end-to-end encrypted communication. In addition, banks must adopt certain security measures, such as having sufficient lighting and sending a one-time password delivered through short message service to the customer's mobile phone for confirmation of the customer's identity.

IV. Identity Documents and Verification

Identity cards must be used for identification and the bank must verify if the customers' identity cards have the required security items (*i.e.* rainbow print, optical variable ink, hidden image, hologram micro lettering), photograph and signature.

After verifying the identity card, video call phase starts where the potential customer's liveliness is ensured. Also, customer representative must ensure that the photograph and information on the identity document match with the potential customer. At this stage, the bank must confirm that additional measures are in place to avoid risks related deep-fake technology.

Article 9 of the Regulation states that the remote identification process must be cancelled, if the process is prevented from running as usual due to the issues such as poor lighting conditions or poor image quality, or if any inconsistency, uncertainty or fraud is discovered in the process or in the documents presented by the potential customer. The remote identification process must be recorded and stored, in full and as available for any audits.



V. Execution of the Banking Agreement Electronically

After completion of the remote identification or face-to-face identification at branches, banks are entitled to execute agreements with the customers electronically, except the ones subject to an official form or special procedural requirement.

In order to enter into a banking agreement electronically, following conditions must be met: (i) all conditions of the banking agreement must be sent to the customer via internet banking or mobile banking in a way that may be read by the relevant customer; (ii) the customer's declaration of intention related to execution of the electronic banking agreement as well as the agreement itself must be delivered to the bank with a secret encryption key generated for the customer; and (iii) the content of the electronic agreement sent to the customer under the section (i) above and the agreement executed by the customer under the section (ii) above must be the same.

VI. Conclusion

The BRSA has recently published this regulation on remote identification process enabling the bank to verify potential customer's identity and thereafter entering into electronic banking agreements. These recent technological developments will certainly provide great flexibility for the banking customers on one hand, however, on the other hand puts great responsibility and on the banks to create the bullet-proof identification system.

Article contact: Gönenç Gürkaynak, Esq.

Email: gonenc.gurkaynak@elig.com

(First published by Mondaq on May 14, 2021)