MOROĞLU ARSEVEN

With the Communiqué Amending the Financial Crimes Investigation Board General Communiqué (Sequence No: 19), Banks and Legal Entities will be able to Perform Remote Identity Detection.

15 Aug 2023

On 11 August 2023, the Communiqué (Serial No: 24) concerning Amendments to the General Communiqué of the Financial Crimes Investigation Board (Serial No: 19) was officially published in the Official Gazette numbered 32276. Thus, revisions have been introduced to the General Communiqué of Financial Crimes Investigation Board (Serial No: 19), which governs the protocols and principles pertaining to remote identity verification methods employed for the verification of customer identities. These revisions now grant banks the capacity to conduct remote identity verification for legal entities as well.

Regulation Amending the Regulation on Remote Identity Verification Methods to be Used by Banks and the Establishment of Contractual Relations in the Electronic Environment ("**Amendment Regulation**") was published in the Official Gazette numbered 21201 dated 25 May 25 2023, and is set to come into effect on 1 June 2023. *You can access the Amendment Regulation prepared for these changes here.* Furthermore, as a continuation of these amendments, significant revisions have been introduced in the Communiqué (Serial No: 19) of the Financial Crimes Investigation Board ("**Communiqué**"), originally published in the Official Gazette numbered 31470 dated 30 April 2021, through the Communiqué (Serial Number: 24) regarding Amendments to the General Communiqué of the Financial Crimes Investigation Board (Serial No: 19) ("**Amendment Communiqué**") concerning the remote identity verification processes.

The important provisions introduced by the Amendment Communiqué can be listed as follows:

- In the cCommuniqué, under Article 3 entitled "Definitions," a customer was originally defined as "*a Turkish national individual or individual trader on whom remote identity verification is to be conducted*." With the Amendment Communiqué; however, the definition of a customer was expanded to include "*an individual, individual trader, or a legal entity registered in the trade registry*,"; thus, broadening the scope of customer identification to encompass not only individuals and individual traders but also legal entities, allowing banks, within the framework of the Financial Crimes Investigation Board ("**MASAK**"), to conduct remote identity verification for legal entity customers.
- Furthermore, within the Amendment Communiqué, definitions for "security features" and "near-field communication" have been added to the definitions section:
- *Security features* include visual security elements on the identification document that can be visually distinguished under white light, such as guilloche, rainbow printing, optical variable ink, hidden image, hologram, and microprinting, as well as visual security elements comprising a photograph and signature.
- *Near-field communication* is defined as a short-range wireless technology that enables electronic devices to conduct reliable, contactless transactions and allows access to digital content and/or

electronic devices for data reading and writing.

- As per Article 4, titled "General Principles for Remote Identity Verification" in the Amendment Communiqué, the following provisions have been stipulated:
- In remote identity verification, the process must be conducted online, continuously, with video, and in real-time, and the entire remote identity verification process must be recorded and stored in a manner that includes all steps and allows for auditability.
- In cases where remote identity verification is partially or entirely outsourced to service providers, these service providers are now required to have the TS EN ISO/IEC 27001 Information Security Management System certification.
- Detailed explanations have been added regarding the key considerations for artificial intelligence-based applications to be used in remote identity verification processes.
- Within the continuation of the article on general principles for remote identity verification, a distinction has been made between "*general principles for remote identity verification in natural persons*" and "*general principles for remote identity verification in legal entities registered in the trade registry*". This separation allows for a detailed examination of the specific principles and procedures that apply to remote identity verification processes for both natural persons and legal entities. It ensures that the regulatory framework addresses the unique requirements and considerations associated with each category.
- The information required for the remote identification of natural persons or individual traders can also be submitted electronically through channels such as internet websites, online banking portals, or mobile applications by filling out electronic forms. During the verification process, an identity card must be used, and the address and identity information obtained as part of the identity verification process should be cross-verified by querying the database of the Ministry of Interior, General Directorate of Population and Citizenship Affairs through the identity sharing system. To ensure the accuracy of the identity document and verify the identity of the individual in question, precautions should be taken. The verification process should include measures to validate the authenticity of the identity document, ascertain the person's vitality, and confirm the consistency between the identity document and the individual. Additionally, technical methods such as near-field communication or biometric comparison should be employed to verify the accuracy of the identity document. Unique one-time passwords should be sent for the identity verification process, and the verification of these passwords should also confirm the associated mobile phone number.
- The information required for the remote identification of legal entities can also be submitted electronically through channels such as internet websites, online banking portals, or mobile applications by means of forms filled out in electronic format. Regarding the information pertaining to legal entities, the legal entity's name, trade registry number, business activity, and address must be verified through the Central Registration System (MERSIS) and the Turkey Trade Registry Gazette, while the tax identification number should be confirmed based on the up-to-date information in the database of the Revenue Administration. In the event that the individual authorized to represent the legal entity is already a customer of the same obligor, they may submit their request to establish a continuous business relationship with the represented legal entity through the open-access online banking portal or mobile application. During this process, the information provided on the signature circular presented by the authorized representative should be documented with photographs or screen captures, and the sample signature on the signature circular should be compared to the individual's identification document or the signature on their MERSIS registration. Additionally, the existence of the signature circular should be confirmed with the date and serial number provided on it.

You can access the Amendment Regulation in Turkish through this link.

Related Practices

- Financial Markets and Services

- Privacy and Data Protection