From the Banking Regulation and Supervision Agency:

REGULATION ON REMOTE IDENTIFICATION METHODS TO BE USED BY BANKS AND ESTABLISHMENT OF CONTRACTUAL RELATIONSHIP IN ELECTRONIC ENVIRONMENT

SECTION ONE
Purpose, Scope, Basis and Definitions

Purpose and Scope

ARTICLE 1 – (1) The purpose of this Regulation is to set forth the procedures and principles regarding remote identification methods that banks may use for acquiring new clients and the establishment of contractual relationships through information technology or electronic communication devices in a manner that substitutes written form, whether remotely or not, following the identification of the client. This also includes the provision of banking services subsequent to such identification.

(2) The remote identification method shall be applied without prejudice to the obligations set forth in the Law No. 5549 on the Prevention of Laundering Proceeds of Crime dated October 11, 2006, and the Law No. 6698 on the Protection of Personal Data dated March 24, 2016, as well as the related regulations under these laws.

Basis

ARTICLE 2 – (1) This Regulation has been issued based on the second paragraph of Article 76 and Article 93 of the Banking Law No. 5411 dated October 19, 2005.

Definitions and Abbreviations

ARTICLE 3 – (1) In this Regulation,

a) Explicit Consent; refers to the explicit consent defined in the Law on the Protection of Personal Data.

b) Bank; refers to the banks defined in Article 3 of the Banking Law.

c) White Light; refers to light that appears colorless to the eye, similar to daylight.

ç) BSEBY; refers to the Regulation on the Information Systems of the Banks and Electronic Banking Services, published in the Official Gazette No. 31069 dated March 15, 2020.

d) Security Features; refers to elements on the identity document such as guilloche patterns, rainbow printing, optically variable ink, hidden images, holograms, and microtext.

e) Identity Document; refers to the identity card defined in the Regulation on the Turkish Republic Identity Card, published in the Official Gazette No. 30967 dated December 3, 2019.

f) Identity Sharing System; refers to the Identity Sharing System defined in the Regulation on the Identity Sharing System, enacted by the Presidential Decree No. 2837 dated August 20, 2020.

g) Person; refers to the natural person or natural person merchant for whom remote identification will be conducted.

ğ) Board; refers to the Banking Regulation and Supervision Board.

h) MRZ (Machine Readable Zone); refers to the fixed-size area on the identity document containing mandatory and optional data formatted for machine reading using optical character recognition methods.

ı) Client Representative; refers to the bank personnel responsible for conducting the remote identification of the person.

i) SMS OTP; refers to the SMS One-Time Password as defined in the BSEBY.

j) Near Field Communication (NFC); refers to the short-range wireless technology enabling secure, contactless transactions and access to digital content and/or electronic devices, used for reading and writing data.

SECTION TWO
Conditions for the Remote Identification Process

General Principles to be Followed Before Initiating the Process

ARTICLE 4- (1) Remote identification is carried out through an online video call between the client representative and the person, without the need for them to be physically present in the same location.

(2) The remote identification method is applied under the conditions specified in this Regulation. The method is designed to resemble in-person identification and to involve a minimal level of risk.

(3) Sufficient security measures are taken for the video call method used in remote identification, considering potential technological, operational, and similar risks.

(4) The remote identification process is considered a critical operation and is designed and operated in such a way that it cannot be initiated, approved, or completed solely by information technology systems or the client representative. The process begins with the individual, continues with controls implemented by information technology systems, and concludes with approvals and additional controls conducted by the client representative. If the client representative determines the process to be risky during their checks, the operation is either referred for secondary approval or terminated.

(5) The processes and systems used for remote identification are evaluated as critical information systems under the tenth paragraph of Article 29 of the BSEBY.

(6) Detailed documentation is prepared regarding the documents to be used during identification, the verifiable features of these documents, and the criteria to be used during the verification process.

(7) Before implementing the remote identification process determined by the bank, process documents are prepared, and the effectiveness of the process is tested and documented. If the test results are deemed unsuccessful, necessary updates are made to the process, and it is not implemented until its effectiveness and adequacy are ensured.

(8) The remote identification process is reviewed at least twice a year. In cases such as the detection or occurrence of security breaches, amendments to relevant legislation, the bank becoming aware of potential fraud or forgery attempts, or the emergence of vulnerabilities in the remote identification method, the process is additionally reviewed, considering technological advancements and practical experience, and necessary updates are made.

Client Representative and Work Environment for Conducting Remote Identification

MADDE 5 – (1) The video call stage of remote identification is conducted by a client representative who has received training in this area.

(2) The client representative is trained to understand the characteristics of documents that can be used for identification, the valid verification methods applied to these documents, and the obligations set forth in this Regulation and other relevant legislation concerning actions that may constitute fraud or forgery.

(3) The client representative is required to undergo training on the remote identification process, including legislation on the protection of personal data, at least once a year and after every update to the process.

(4) The client representative is provided with training to ensure they can determine whether the individual has voluntarily requested to become a bank client or to benefit from banking services.

(5) During the remote identification process, client representatives must work in separate, access-restricted areas where the necessary precautions have been taken to prevent potential security vulnerabilities or abuses.

(6) To instill confidence in the individual, it must be ensured that an appropriate environment or methods are used to reflect that the client representative is working on behalf of the bank.

(7) To serve individuals with disabilities, at least one client representative must be provided with the necessary training.

Principles to be Followed at the Initiation of the Process

ARTICLE 6- (1) Before the video call in the remote identification process begins, the individual's application is received through a form filled out electronically via the bank application where the remote identification process is conducted. A risk assessment is performed based on the data collected. If deemed necessary as a result of the risk assessment, the process is terminated before the video call begins.

(2) In the remote identification process implemented under this Regulation, only the biometric data of the individual, as a special category of personal data, may be used for identification purposes. The individual's explicit consent regarding this is recorded electronically.

(3) Mechanisms are established to minimize the risk of abuse stemming from predictable assignments, such as assigning a specific individual to a specific client representative during remote identification processes.

(4) Before the video call with the individual, a set of minimum questions to be asked by the client representative is determined. The sequence and/or type of questions asked may vary.

(5) The video call stage of remote identification is conducted in real time and without interruption. The integrity and confidentiality of the audiovisual communication between the client representative and the individual are ensured at a sufficient level. For this purpose, the video call is carried out with secure end-to-end communication.

(6) The quality of the video and audio communication during the video call is ensured to be sufficient throughout the call to avoid any doubt or limitations in identification in line with the provisions and controls specified in this Regulation. The video quality allows for visual verification of the document presented under white light and for examining the security elements to ensure that the document is neither worn out nor tampered with.

(7) During the remote identification process, the individual is sent a centrally generated SMS OTP that is valid only for the identification transaction. The system ensures that the SMS OTP is returned by the individual via the online application interface. If the SMS OTP is successfully verified in the system, the individual's mobile phone number is confirmed.

Identification Documents and Verification

ARTICLE 7-(1) During the remote identification process, identification documents that feature security elements distinguishable under white light, as well as a photograph and a signature, are used.

(2) Verification of identity information embedded in the chip of the identification document via near-field communication (NFC) confirms the match necessary to identify the individual based on the document. This verification ensures:

a) That the identification document has been issued by the authorized issuing authority, and the information stored in the contactless chip has not been altered,

b) That the keys in the contactless chip of the identification document have not been duplicated or cloned.

(3) If verification through NFC as described in the second paragraph cannot be performed for any reason, at least four visual security features outlined in the first paragraph must be verified in terms of shape and content. In cases where only visual security features are verified, the bank must also require the initial financial transaction before establishing a continuous business relationship to be made from the individual's account at another bank that applies client identification principles.

(4) During visual identification, the individual is asked to tilt the identification document horizontally or vertically in front of the camera and make additional movements as instructed by the client representative. For this purpose, the individual may be asked to place their finger on randomly determined sections of the security features of the identification document identified by the system.

(5) During the video call process, the client representative captures photographs and/or screenshots showing the individual, the front and back of the identification document, and the information on the document.

(6) Using individual images obtained, cropped, and enlarged from the individual's movements, the client representative ensures that all security elements distinguishable under white light are fully covered at the correct angle and verifies that there is no indication of forgery or tampering at the transition points between sections of the identification document.

(7) Verification of the validity and authenticity of the data and information on the identification document is carried out as part of the remote identification process. Within this scope, at a minimum:

a) The document must exhibit characteristics such as font type, layout, number, size, spacing, and typography as defined by the authorized issuing authority,

b) The identification document must not be damaged, altered, tampered with, or have a photograph affixed to it post-issuance,

c) The document's validity period must conform to the standards associated with the specific type of identification document,

ç) The information in the Machine-Readable Zone (MRZ) of the document must match the information on the identification document,

d) The individual-related information on the identification document must correspond to the information known to the bank, obtained from the Identity Sharing System, and, if applicable, other information accessible to the bank for identification purposes,

e) The serial number on the identification document is verified by having the individual read it out during the video call.

Verification of the Person Whose Identity is to Be Confirmed

ARTICLE 8-(1) During the video call phase of remote identification, methods to detect the person's liveliness are utilized. The bank takes additional measures to mitigate the risks associated with counterfeit facial technology.

(2) In the remote identification process, the individual's face is biometrically compared either with the photograph retrieved from the contactless chip on the identity document using near-field communication (if retrievable) or, if not, with the photograph on the identity document.

(3) The client representative ensures that the photograph and personal details on the identity document match the individual.

(4) Through dialogue and observations during the identification process, the client representative determines that the information on the identity document, the details provided by the individual during the call, and their stated intent are credible and adequate. Risks related to phishing, social engineering, coercion by a third party, or similar fraudulent methods are taken into consideration within this scope.

(5) The process is finalized by informing the individual about the banking services to be provided and obtaining their verbal confirmation that they accept becoming a bank client at the end of the video call phase of the remote identification.

Termination of the Process During the Video Call

ARTICLE 9- (1) If visual verification or verbal communication with the individual cannot be conducted as specified in this Regulation due to poor lighting conditions, low-quality images or transmissions, or similar circumstances, the video call phase of the remote identification process is terminated. This provision also applies in cases where other inconsistencies or uncertainties arise during the process.

(2) If doubts arise during the video call phase of remote identification regarding the validity of the document presented by the individual or in cases of suspected fraudulent or counterfeit activity, the remote identification process is terminated.

Recording and Storage of Data

ARTICLE 10-(1) The entire remote identification process, including all its steps, is recorded and stored to ensure its auditability. The provisions of relevant legislation regarding the retention of information and documents remain reserved.

Responsibility in Remote Identification

ARTICLE 11-(1) It is the bank's responsibility to ensure that the solutions used for remote identification minimize the risk of incorrect identification. The bank monitors individuals whose identities are verified through remote identification under a different risk profile. Additional security and control measures are applied based on the type and amounts of transactions conducted by these individuals.

In the event of disputes regarding transactions that impose obligations on individuals or third parties, the burden of proof lies with the bank.

(2) When remote identification is conducted in compliance with the conditions set forth in this Regulation, the requirements of the first paragraph of Article 34 of the BSEBY regarding identification are deemed fulfilled.

(3) The Board is authorized to restrict or suspend the use of remote identification by the bank in cases of complaints, actions that may constitute fraud or forgery, or other situations deemed necessary, based on the bank's compliance with the provisions of the BSEBY and this Regulation.

SECTION THREE
Establishing a Contractual Relationship in an Electronic Environment

Establishing a Contractual Relationship Following Identification

ARTICLE 7- (1) Following the remote identification performed in accordance with the conditions set forth in this Regulation or the face-to-face identification of the client conducted through branches, if a contractual relationship for transactions requested by clients is to be established remotely via one of the distribution channels regulated under the BSEBY, such as internet banking or mobile banking, which are accessible to the client, the client's declaration of intent to establish the contract must be obtained through these distribution channels following identification conducted in accordance with the first paragraph of Article 34 of the BSEBY.

(2) Following the remote identification conducted in accordance with the conditions set forth in this Regulation or the face-to-face identification of the client conducted through branches, for the establishment of a contractual relationship in writing through an information or communication device for transactions requested by clients, whether remotely or otherwise:

(a) All terms of the contract must be delivered to the client through internet banking or mobile banking distribution channels in a way that the client can read;

(b) The contract and the client’s declaration of intent to establish the contract, as provided to the client under paragraph (a), must be signed with a unique encryption private key specific to the client as specified in the third paragraph of Article 38 and the first paragraph of Article 39 of the BSEBY and transmitted to the bank;

(c) The information provided to the client as part of the contract content under paragraph (a) must match the information signed by the client under paragraph (b).

(3) For any contract regulating the relationship between the bank and the client regarding banking services to be provided to the client that is not subject to an official form or specific formalities:

(a) If it is established electronically in accordance with the second paragraph, or

(b) If the client's declaration of intent to establish the contract is obtained remotely during the video call phase of the remote identification following verification,

the written form requirement for these contracts shall be deemed fulfilled.

SECTION FOUR
Miscellaneous and Final Provisions

Enforcement

ARTICLE 19- (1) his Regulation shall enter into force on May 1, 2021.

Execution

ARTICLE 20- (1) The provisions of this Regulation shall be executed by the Chairman of the Banking Regulation and Supervision Agency.