Remote Identity Verification

Remote identity verification and electronic agreements became legally possible for **banks, financial leasing, factoring, financing and saving financing companies, intermediary institutions and portfolio management companies** with the regulations and communiqués published in the Official Gazettes dated 1 April 2021, 11 January 2022, and 8 February2022.

Conditions Regarding Customer Representatives: Customer representatives must be specifically trained for remote identity verification, and further they must be trained on personal data protection at least once a year, and afterwards, for every amendment in the legislation.

Remote Identity Verification Method: Since remote identification is considered as a «critical transaction» as per the legislation, it must be designed and operated in a way that does not allow a call to be initiated, approved, and completed by the IT or the customer representative alone.

The remote identity verification process should begin with **an electronic form filled by the customer**. Sensitive personal data of the customer other than her/his **biometric data** cannot be processed. A **specific consent** must be taken from the customer for the processing her/his personal data and such consent **must be kept electronically**.

The video call should be done in **real-time and without any interruption**. During the call, **image and sound quality must be sufficient**. Documentations submitted by the customer **must be presented under white light and be undamaged.**

Centrally generated SMS OTP must be transmitted in order to verify the customer's mobile phone.

Tansel

Remote Identity Verification

Security Measures: Adequate security measures should be taken to ensure the call is conducted safely. During the process, an **identity document that has visually distinguishable security elements**, **a photograph**, **and signature should be presented under white light**. Furthermore, **additional precautions should be taken regarding the risks associated with fake face technology**.

The entire process must be recorded and stored in accordance with the information and document retention requirements in the legislation and must be available for audit.

The institution performing the identity verification must minimize the risk of misidentifying the person. Thus, **additional security and control methods must be applied depending on the type and amount of the transaction.**

Termination of the Interview: If the appropriate conditions cannot be met during the interview or if there are doubts about the accuracy of the documents presented, the interview must be terminated.

Electronic Contract: The customer's declaration of intent **must be received after at least a two-factor authentication mechanism has been implemented**. Such factors must be under at least two different categories of information: information that the customer «knows», «has» or «has biometric characteristics».

In order for the contract to be concluded between the parties, all the terms of the contract must be sent to the client through online or mobile service channels in a form that the client can read, and the client must sign the contract with her/his own encrypted passcode.

Remote Identity Verification

Use of Artificial Intelligence: Legislation allows financial leasing, factoring, financing, and savings finance companies to use artificial intelligence for remote identity verification procedures during transactions under TRY 7.500. Banking Regulation and Supervision Agency will determine the applicable principles. In any case, the institutions shall get the opinion of Financial Crimes Investigation Board regarding using artificial intelligence for remote identity verification.