REGULATION ON REMOTE IDENTIFICATION METHODS TO BE USED BY FINANCIAL LEASING, FACTORING, FINANCING AND SAVINGS FINANCE COMPANIES AND ON THE ESTABLISHMENT OF CONTRACTUAL RELATIONSHIPS IN ELECTRONIC ENVIRONMENT

SECTION ONE
Purpose and Scope, Basis and Definitions

Purpose and Scope

ARTICLE 1-(1) The purpose of this Regulation is to regulate the procedures and principles regarding the remote identification methods that may be used by financial leasing, factoring, financing and savings finance companies for the acquisition of new customers and the services to be provided following the identification of the customer identity, and the procedures and principles for the establishment of a contractual relationship over an information or electronic communication device, whether distance or not, as a substitute for the written form or distance.

(2) The remote identification method shall be applied without prejudice to the Law on the Prevention of Laundering Proceeds of Crime dated 11/10/2006 and numbered 5549 and the Law on the Protection of Personal Data dated 24/3/2016 and numbered 6698 and the obligations set forth in the legislation related to these Laws.

Basis

ARTICLE 2-(1) This Regulation has been issued based on the first paragraph of Article 22, the second paragraph of Article 38, the third paragraph of Article 39, the third paragraph of Article 39 and the second paragraph of Article 39/A of the Law on Financial Leasing, Factoring, Financing and Savings Finance Companies, dated 21/11/2012 and numbered 6361.

Definitions and abbreviations

ARTICLE 3- (1) In this Regulation;

a) Explicit consent: refers to the explicit consent as defined in the Personal Data Protection Law,

b) White light: Light that is apparently colorless, such as daylight,

c) Information Systems Communiqué: Financial Leasing, Factoring and Financing Companies published in the Official Gazette dated 6/4/2019 and numbered 30737 Communiqué on the Management and Audit of Information Systems,

ç) Electronic signature: The electronic signature defined in the Electronic Signature Law dated 15/1/2004 and numbered 5070,

d) Security elements: Identity document with a wearable, rainbow print, optical variable ink, latent image, hologram and micro-lettering.,

e) Identity Card: Identity card as defined in the Republic of Turkey Identity Card Regulation published in the Official Gazette dated 3/12/2019 and numbered 30967,

f) Identity Sharing System: Identity Sharing System defined in the Identity Sharing System Regulation put into force by the Presidential Decree dated 20/8/2020 and numbered 2837,

g) Person: The natural person or natural person merchant to be identified remotely,

ğ) Board: Banking Regulation and Supervision Board,

h) Agency: Banking Regulation and Supervision Agency,

ı) MRZ: A fixed-size area on an identity document containing mandatory and optional data formatted for machine reading using optical character reading methods,

i) Customer representative: Company personnel or personnel employed through outsourced service procurement who will carry out remote identification of the person,

j) SMS OTP: Single-use password transmitted through the short message service provided by electronic communication operators,

k) Company: The company defined in Article 3 of the Law No. 6361,

l) Near field communication: refers to short-range wireless technology used to read and write data, enabling electronic devices to perform reliable, contactless transactions and access digital content and/or electronic devices,

SECTION TWO
Conditions for the Remote Identification Process

General principles to be followed before the process is initiated

ARTICLE 4-(1) Remote identification is done by video calling and communicating with the customer representative online, without the need for the customer representative and the person to be physically present in the same environment.

(2) Remote identification method shall be applied within the conditions specified in this Regulation. The method to be applied is designed to be similar to the face-to-face identification method and to contain a minimum level of risk.

(3) Adequate security measures are taken by taking into account possible technological, operational and similar risks in the video call method to be used in remote identification.

(4) The remote identification process is considered as a critical process and is designed and operated in a way that does not allow the process to be initiated, approved and completed by the information technologies or customer representative alone. It is ensured that the process is initiated by the person, continued with the controls applied by information technologies and completed with the approval and additional controls to be made by the customer representative. If the transaction is found risky in the controls made by the customer representative, the transaction is sent for a second approval or terminated.

(5) Maximum care shall be taken to ensure that the processes, systems, products and services to be used for remote identification are produced in Turkey or that the R&D centers of their producers are located in Turkey, and this shall be considered as an important criterion for outsourcing. Such providers and manufacturers must have response teams in Turkey.

(6) Detailed documents are created on the documents to be used during identification, the verifiable features in these documents and the criteria to be used during verification.

(7) Before the implementation of the remote identification process determined by the company, process documents are created and the effectiveness of the process is tested and the results are written down. If the test results are not successful, necessary updates are made to the process and the process is not implemented unless the effectiveness and adequacy of the process is ensured.

(8) The remote identification process is reviewed at least once a year. In cases such as the detection or occurrence of security breaches, changes in the relevant legislation, the company becoming aware of possible fraudulent or fraudulent actions, and the emergence of weaknesses related to the remote identification method used, the process is reviewed separately, taking into account technological developments and experience gained in practice, and necessary updates are made.

Customer representative and working environment for remote identification

ARTICLE 5-(1) The video call stage of remote identification is carried out by a trained customer representative.

(2) It is 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 constitute fraud or forgery and the obligations set forth in this Regulation and other relevant legislation.

(3) It is ensured that the customer representative receives training on the remote identification process at least once a year and after each update, including personal data protection legislation.

(4) It is ensured that the customer representative is trained to be able to decide that the person has voluntarily requested the company to become a customer of the company or to benefit from the services offered by the company.

(5) During the remote identification process, it is ensured that the customer representative works in separate areas with restricted access, where necessary measures are taken to prevent possible security vulnerabilities or abuses.

(6) It is ensured that an appropriate environment is created or methods are used to reflect that the customer representative works on behalf of the company in order to give confidence to the person.

(7) It is ensured that at least one customer representative is provided with the necessary training in order to provide service to persons with disabilities.

(8) In the event that a customer representative is employed through outsourcing, such customer representative working in a separate area with restricted access to the company is subject to the permission of the Authority.

General principles to be followed when initiating the process

ARTICLE 6-(1) Before the video call starts in the remote identification process, the application of the person is received with a form filled in electronically through the company application where the remote identification process is operated, and a risk assessment is carried out about the person using the data received. If necessary as a result of the risk assessment, the process is terminated without starting the video call.

(2) In the remote identification process to be implemented within the scope of this Regulation, only biometric data can be used among the personal data of special nature for the purpose of remote identification of the person and the explicit consent of the person to this is recorded electronically.

(3) When assigning remote identification operations to the customer representative, the necessary mechanisms are put in place to reduce the possibility of abuse due to predictable situations.

(4) Before the video call with the person, the minimum questions to be asked by the customer representative are determined and the order and/or type of questions asked may vary.

(5) The video call phase of remote identification is conducted in real time and without interruption. It is ensured that the integrity and confidentiality of the audio-visual communication between the customer representative and the person is at a sufficient level. For this purpose, the video call is realized with end-to-end secure communication.

(6) It is ensured that the image and sound quality of the communication is at a sufficient level during the entire conversation so as to leave no room for doubt within the framework of the provisions and controls set out in this Regulation and not to allow any restriction in identification. The image quality allows for the examination of

security elements to visually verify the presented document under white light and to check that the presented document has not been worn or tampered with.

(7) During the remote identification process, the person receives a centrally generated SMS OTP that is valid only for the identification process. The SMS OTP is sent back by the person online via the application interface. If this SMS OTP is successfully confirmed in the system, the mobile phone number of the person is verified.

Identification document that can be used and its verification

ARTICLE 7-(1) In the process of remote identification, an identity document with security elements that can be visually distinguished under white light, a photograph and a wet signature is used.

(2) Verification of the credentials on the identity document chip using near field communication means that the match required to identify the person from the identity document has been achieved. Such verification;

a) The identity document used is issued by the competent authority that issued the document and the information on the contactless chip of the document has not been altered,

b) This is done by checking that the keys on the contactless chip of the identity document have not been duplicated.

(3) In the event that the verification referred to in the second paragraph cannot be performed for any reason using near field communication, at least four of the visual security elements of the identity document referred to in the first paragraph of this article shall be verified in terms of form and content. In cases where only visual security elements are verified, the company additionally applies one or more or all of the tightened measures specified in the relevant legislation within the framework of the risk-based approach before establishing a permanent business relationship with the person. In the transactions carried out, the burden of proof is on the company pursuant to the first paragraph of Article 11.

(4) During visual identification, the person is asked to tilt the identity document horizontally or vertically in front of the camera and to make additional movements according to the instructions given by the customer representative. For this purpose, the person is asked to place his/her finger on the security-related parts of the identity document, which are determined by the system in a variable and random manner.

(5) During the video call, the agent creates photographs and/or screenshots showing the person and the front and back of the identity document presented by the person, as well as the information on the document.

(6) Using individual images taken from the person's movements, cropped and enlarged, the agent ensures that the identity document is fully covered at the correct angle, with all security elements visually distinguishable under white light, and that there are no artifacts at the transition points between parts of the identity document that would indicate tampering or forgery.

(7) Verification of the validity and authenticity of the data and information contained in the presented identity document is performed as part of the remote identification process. In this context, at a minimum;

a) The characters required in the identity document have the characteristics defined by the competent authority issuing the document, such as font, layout, number, size, spacing and typography,

b) The identity document has not been damaged, defaced, altered and, in particular, has not had a photograph affixed to it,

c) The validity period of the identity document is not contrary to the standards of the identity document in question,

ç) The information in the MRZ of the identity document matches the information on the identity document,

d) The information contained in the identity document of the person matches with other information known to the company, obtained from the Identity Sharing System and, if any, available to the company for identification purposes,

e) The serial number on the identity document is verified by reading the serial number on the identity document to the person during the video call.

Verification of the person to be identified

ARTICLE 8-(1) During the video call phase of remote identification, methods are used to determine the person's vitality. The Company takes additional measures to prevent risks related to false face technology.

(2) In the process of remote identification, a biometric comparison is made between the face of the person and the photograph on the contactless chip if it can be obtained from the identity document using near field communication, or the photograph on the identity document if it cannot be obtained.

(3) The customer representative ensures that the photo and personal details on the identity document used match the person.

(4) As a result of the dialog and observations to be made with the person during the identification process, the customer representative concludes that the information in the identity document, the information provided by the person during the interview and the stated intentions are convincing and sufficient. In this context, the risks related to phishing, social engineering, actions taken under pressure due to coercion by another party and similar fraud methods are taken into consideration.

(5) At the end of the video call stage of remote identification, the process is completed by informing the person about the services to be provided by the company and obtaining verbal confirmation that the person agrees to become a customer of the company.

Termination of the process in video call

ARTICLE 9- (1) In cases where it is not possible to perform visual verification and/or verbal communication with the person as specified in this Regulation due to poor lighting conditions, poor image quality or transmission and similar situations, the video call phase of remote identification shall be terminated. This provision shall also apply if there is any other inconsistency or uncertainty in the process.

(2) If there is any doubt about the validity of the document presented by the person during the video call phase of remote identification, or if there is any suspicion of acts that may constitute fraud or forgery, the remote identification process is terminated.

Recording and storage of data

ARTICLE 10-(1) The entire remote identification process shall be recorded and stored in a way to include all steps of the process and to ensure that it is auditable. The provisions of the relevant legislation regarding information and document retention requirements are reserved.

Responsibility for remote identification

ARTICLE 11-(1) It is the company's responsibility to ensure that the solutions used for remote identification are used in a way that minimizes the risk of misidentification. The Company monitors the persons identified by remote identification in a different risk profile. Additional security and control methods are applied depending on the type and amount of the transaction made by these persons. In case of objection in transactions that give rise to liability to persons or a third party, the burden of proof is on the company.

(2) The Board is authorized to restrict or suspend the use of remote identification as a result of the evaluation of the Company's compliance with the provisions of the Information Systems Communiqué and this Regulation, complaints and actions that may constitute fraud or forgery, and in other cases deemed necessary.

SECTION THREE
Establishment of Contractual Relationship in Electronic Environment

Authentication and transaction security

ARTICLE 12-(1) Except as otherwise provided in this Regulation, for services provided electronically, except for transactions that do not give rise to financial consequences or obligations, such as the display of customer information, it is essential that the company applies an authentication mechanism consisting of at least two independent components to its customers and takes measures to ensure the confidentiality of the authentication data contained in these components during their use in the authentication process. These two components are selected to belong to two different classes of elements that the customer “knows”, “has” or “has a biometric characteristic of”. Component independence means that compromise of one component does not jeopardize the security of another component. It is essential that the customer-owned component is unique to the customer and cannot be forged.

(2) The requirements of the first paragraph shall be deemed to be fulfilled in cases where the Turkish Republic Identity Card is used together with the card-PIN or biometric data or the electronic signature is used for identity verification.

(3) The Authority is authorized to define exceptions or additional security measures or to determine additional procedures and principles regarding the application of the first paragraph. For any transaction carried out without using two-component authentication in a manner that is not in compliance with the first paragraph, the burden of proof that the transactions were made by the customer shall be on the company.

(4) The security of the components to be used in the authentication mechanism to be applied to the users is ensured throughout the entire process starting from the production stages until they are delivered to the user.

(5) Encryption keys to be used in authentication are made available to customers in a way that minimizes the possibility of these keys being intercepted, ensures their confidentiality, and includes methods that prevent them from being changed and corrupted.

(6) It is ensured that the authentication mechanism to be applied to users informs the relevant user about failed authentication attempts at the first time they enter the system. If the number of failed attempts exceeds a certain number, additional security measures are taken for the customer's access, and if failed authentication attempts continue, the relevant user's access is blocked.

(7) The Company may not send an OTP or verification code via SMS to its customers who have installed and activated the mobile application in order to log in or to verify any transaction in the continuation of the session and may not use this as an authentication element. Sending an OTP or verification code via SMS during the initial installation, activation, reactivation stages of the mobile application or in case the application is unavailable does not constitute a violation of this paragraph.

(8) The Company shall identify the customers who have changed their SIM card or changed their electronic communication operator through number porting before sending SMS OTPs by ensuring the necessary integration with the mobile communication operators established in Turkey, and the SIM card-based element cannot be used as an authentication element when providing electronic services to the relevant customers for 90 days from the date of the change, unless the changes are confirmed. For any transactions carried out without the use of two-component

authentication when confirming changes, the burden of proof is on the company to prove that the transactions were carried out by the customer.

(9) It is ensured that one-time passwords to be used by customers for identity or transaction verification purposes are generated randomly, variably and uniquely, of sufficient length to be difficult to guess, and are valid for a certain period of time.

(10) The information contained on the documents that serve to identify the identity of the customer and substitute for official identity documents and the mother's maiden name may not be used for authentication purposes at any stage during the provision of services in the electronic environment. In the event that the company wishes to use a security question as an element known to the customer in authentication, this security question must not be related to one of the information on the documents that replace the official identity document and the answer must be determined by the customer itself.

(11) It is ensured that the source of any software or mobile application offered by the Company to its customers for use in its services provided in electronic environment can be verified as the relevant company. The Company is obliged to ensure that these software or mobile applications do not contain any code that may jeopardize customer security, and to make the necessary patches and updates to eliminate security vulnerabilities available to customers.

(12) The Company takes measures to ensure that sensitive data used by applications on mobile devices used to transmit multiple authentication components to the Company, such as smartphones, are inaccessible to other applications and running processes on the same mobile device. The Company is obliged to ensure that sensitive data on these mobile devices are inaccessible to unauthorized persons in case of loss or theft of such mobile devices and to establish controls in accordance with the current technology in order to reduce the risks arising from situations such as seizure of mobile devices, deterioration of reliability, cracking or modification of operating system software.

(13) For the authentication process to be performed in accordance with the first paragraph for services provided in electronic environment, a single-use verification code shall be generated to be signed with an encryption secret key assigned to the customer. It shall be ensured that no information can be obtained about any of the authentication elements specified in the first paragraph through the verification code, no other valid verification codes can be derived from a known verification code, and verification codes cannot be forged. In cases where it is not possible to sign the verification code with a cryptographic secret key assigned to the customer, the verification code may be transmitted to the customer via SMS, without prejudice to the provision of the seventh paragraph.

(14) In case the electronic service is provided through a mobile application, if the application PIN or a biometric authentication component of the customer is used to access a customer-specific encryption key and through this encryption key a unique information related to the customer is verified online with the company, instead of the two-component authentication referred to in the first paragraph
is considered to have been brought.

Establishment of the contractual relationship following identification

ARTICLE 13-(1) In the event that the contractual relationship for the transactions intended to be performed by the customers is established at a distance through internet or mobile service channels following remote identification within the conditions set forth in this Regulation or face-to-face identification of the customer's identity, the customer's declaration of will establishing the contract must be received after an identity verification performed in accordance with the first paragraph of Article 12 through the same channels.

(2) In order to establish a contractual relationship that will replace the written form through an information or communication device for the transactions desired to be performed by the customers, whether distance or not, following the remote identification or face-to-face identification of the customer identity within the conditions specified in this Regulation;

a) All terms and conditions of the said agreement are communicated to the customer via internet or mobile service channels in a way that the customer can read,

b) The contract transmitted to the customer according to subparagraph (a) and the customer's declaration of will establishing the contract together with this contract are signed with the customer-specific encryption secret key specified in paragraph thirteen and paragraph fourteen of Article 12 and transmitted to the company,

c) In accordance with subparagraph (a), if the customer has been provided with the information specified as the content of the contract in the transmitted contract, only that information must be signed by the customer in accordance with subparagraph (b).

(3) Any contractual relationship that regulates the relations between the company and the customer for the services to be provided to the customer and is not subject to an official form or a special ceremony;

a) Established electronically in accordance with the second paragraph or

b) Establishment of the customer's declaration of will establishing the contract at a distance by receiving the customer's declaration of will following the remote identification during the video call phase,
in such cases, the written form requirement for these agreements shall be deemed to have been fulfilled.

SECTION FOUR
Miscellaneous and Final Provisions

Artificial intelligence based applications

ARTICLE 14-(1) For transactions not exceeding TRY 7,500, the Board is authorized to determine the principles regarding the transactions to be performed by the customer representative as referred to in this Regulation with artificial intelligence-based methods.

Enforcement

ARTICLE 15-(1) This Regulation shall enter into force one month after its publication.

Execution

ARTICLE 16-(1) The provisions of this Regulation shall be executed by the Chairman of the Banking Regulation and Supervision Agency.