FİNANSAL KİRALAMA, FAKTORİNG, FİNANSMAN VE TASARRUF FİNANSMAN ŞİRKETLERİNCE KULLANILACAK UZAKTAN KİMLİK TESPİTİ YÖNTEMLERİNE VE ELEKTRONİK ORTAMDA SÖZLEŞME İLİŞKİSİNİN KURULMASINA İLİŞKİN YÖNETMELİK

BİRİNCİ BÖLÜM
Amaç ve Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 –(1) Bu Yönetmeliğin amacı, finansal kiralama, faktoring, finansman ve tasarruf finansman şirketleri tarafından yeni müşteri kazanımında kullanılabilecek uzaktan kimlik tespiti yöntemlerine ve müşteri kimliğinin tespit edilmesini müteakip sunulacak hizmetlere yönelik olarak mesafeli olsun olmasın bir bilişim veya elektronik haberleşme cihazı üzerinden yazılı şeklin yerine geçecek şekilde ya da mesafeli olarak sözleşme ilişkisinin kurulmasına yönelik usul ve esasları düzenlemektir.

(2) Uzaktan kimlik tespiti yöntemi, 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bu Kanunlarla ilgili mevzuatta yer alan yükümlülükler saklı kalmak kaydıyla uygulanır.

Dayanak

MADDE 2 –(1) Bu Yönetmelik, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanununun 22 nci maddesinin birinci fıkrası, 38 inci maddesinin ikinci fıkrası, 39 uncu maddesinin üçüncü fıkrası ve 39/A maddesinin ikinci fıkrasına dayanılarak düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 3 – (1) Bu Yönetmelikte yer alan;

a) Açık rıza: Kişisel Verilerin Korunması Kanununda tanımlanan açık rızayı,

b) Beyaz ışık: Gün ışığı gibi görünürde renksiz olan ışığı,

c) Bilgi Sistemleri Tebliği: 6/4/2019 tarihli ve 30737 sayılı Resmî Gazete'de yayımlanan Finansal Kiralama,Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliği,

ç) Elektronik imza: 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanan elektronik imzayı,

d) Güvenlik ögeleri: Kimlik belgesinde yer alan giyoş, gökkuşağı baskı, optik değişken mürekkep, gizli görüntü, hologram ve mikro yazıyı,

e) Kimlik belgesi: 3/12/2019 tarihli ve 30967 sayılı Resmî Gazete'de yayımlanan Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliğinde tanımlanan kimlik kartını,

f) Kimlik Paylaşımı Sistemi:20/8/2020 tarihli ve 2837 sayılı Cumhurbaşkanı Kararıyla yürürlüğe konulan Kimlik Paylaşımı Sistemi Yönetmeliğinde tanımlanan Kimlik Paylaşımı Sistemini,

g) Kişi: Uzaktan kimlik tespiti yapılacak gerçek kişiyi veya gerçek kişi taciri,

ğ) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

h) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

ı) MRZ: Optik karakter okuma yöntemlerini kullanarak makine okuması için biçimlendirilmiş, zorunlu ve isteğe bağlı verileri kapsayan, kimlik belgesi üzerinde yer alan sabit boyutlu alanı,

i) Müşteri temsilcisi: Kişinin uzaktan kimlik tespitini yapacak şirket personelini ya da dış hizmet alımı yoluyla istihdam edilen personeli,

j) SMS OTP: Elektronik haberleşme işletmecilerinin sunduğu kısa mesaj servisi aracılığıyla iletilen tek kullanımlık parolayı,

k) Şirket: 6361 sayılı Kanunun 3 üncü maddesinde tanımlanan şirketi,

l) Yakın alan iletişimi: Elektronik cihazların güvenilir, temassız işlem yapabilmesini ve sayısal içeriğe ve/veya elektronik cihazlara erişimini mümkün kılan, veri okuma ve yazmakta kullanılan kısa menzilli kablosuz teknolojiyi,

ifade eder.

İKİNCİ BÖLÜM
Uzaktan Kimlik Tespiti Sürecine İlişkin Şartlar

Süreç başlatılmadan önce uyulması gereken genel ilkeler

MADDE 4 – (1) Uzaktan kimlik tespiti, müşteri temsilcisi ile kişinin; fiziksel olarak aynı ortamda bulunmasına gerek olmadan, çevrim içi olarak görüntülü görüşmesi ve birbiriyle iletişim kurması ile yapılır.

(2) Uzaktan kimlik tespiti yöntemi bu Yönetmelikte belirtilen şartlar dâhilinde uygulanır. Uygulanacak yöntem, yüz yüze yapılan kimlik tespiti yöntemine benzer ve asgari seviyede risk ihtiva edecek şekilde tasarlanır.

(3) Uzaktan kimlik tespitinde kullanılacak görüntülü görüşme yönteminde olası teknolojik, operasyonel ve benzeri riskler dikkate alınarak yeterli seviyede güvenlik önlemleri alınır.

(4) Uzaktan kimlik tespiti işlemi, kritik bir işlem olarak değerlendirilir ve işlemin bilgi teknolojileri veya müşteri temsilcisi tarafından tek başına başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir. Sürecin kişi tarafından başlatılması, bilgi teknolojileri tarafından uygulanan kontroller ile devam ettirilmesi ve müşteri temsilcisi tarafından yapılacak onaylama ve ek kontroller ile tamamlanması sağlanır. Müşteri temsilcisi tarafından yapılan kontrollerde işlemin riskli bulunması halinde işlem ikinci bir onaya gönderilir veya sonlandırılır.

(5) Uzaktan kimlik tespitine ilişkin kullanılacak süreç, sistem, ürün ve hizmetlerin Türkiye'de üretilmesi veya üreticilerinin ar-ge merkezlerinin Türkiye'de bulunması için azami özen gösterilir ve dış hizmet alımında önemli bir kriter olarak değerlendirilir. Bu tür sağlayıcıların ve üreticilerin Türkiye'de müdahale ekiplerinin bulunması şarttır.

(6) Kimlik tespiti sırasında kullanılacak belgelere, bu belgelerde var olan doğrulanabilir özelliklere ve doğrulamanın yapılması sırasında kullanılacak kriterlere ilişkin detaylı dokümanlar oluşturulur.

(7) Şirketin belirlediği uzaktan kimlik tespiti sürecinin uygulanmasından önce, süreç dokümanları oluşturulur ve sürecin etkinliği test edilerek sonuçları yazılı hale getirilir. Test sonuçlarının başarılı bulunmaması durumunda süreçte gerekli güncellemeler yapılır ve sürecin etkinliği ve yeterliliği sağlanmadıkça süreç uygulanmaz.

(8) Uzaktan kimlik tespiti süreci yılda en az bir defa gözden geçirilir. Güvenlik ihlallerinin tespit edilmesi veya gerçekleşmesi, ilgili mevzuatta değişiklik yapılması, şirketin muhtemel dolandırıcılık veya sahtecilik teşkil edebilecek eylemlerden haberdar olması ve kullanılan uzaktan kimlik tespiti yöntemine ilişkin zayıflıkların ortaya çıkması gibi durumlarda teknolojik gelişmeler ve uygulamada kazanılan deneyimler dikkate alınarak sürecin ayrıca gözden geçirilmesi sağlanır ve gerekli güncellemeler yapılır.

Uzaktan kimlik tespitini yapacak müşteri temsilcisi ve çalışma ortamı

MADDE 5 – (1) Uzaktan kimlik tespitinin görüntülü görüşme aşaması, bu konuda eğitim almış müşteri temsilcisi tarafından gerçekleştirilir.

(2) Müşteri temsilcisinin, kimlik tespitinde kullanılabilecek belgelerin özelliklerini ve bu belgeler için uygulanan geçerli doğrulama yöntemlerini öğrenmesi ve dolandırıcılık veya sahtecilik teşkil edebilecek eylemlere, bu Yönetmelikte ve ilgili diğer mevzuatta yer alan yükümlülüklere ilişkin bilgi sahibi olması sağlanır.

(3) Müşteri temsilcisinin, uzaktan kimlik tespiti sürecine ilişkin yılda en az bir defa ve her bir güncelleme sonrasında kişisel verilerin korunması

mevzuatı da dâhil olmak üzere eğitim alması sağlanır.

(4) Müşteri temsilcisinin, kişinin şirket müşterisi olma veya şirketin sunduğu hizmetlerden yararlanma isteğini kendi iradesiyle şirketten talep ettiğine dair karar verebilmesi konusunda eğitim alması sağlanır.

(5) Uzaktan kimlik tespiti sürecinde müşteri temsilcisinin, yaşanılabilecek güvenlik zafiyetlerinin ya da suistimallerin engellenmesine yönelik gerekli tedbirlerin alındığı, erişimi sınırlandırılmış ayrı alanlarda çalışması sağlanır.

(6) Kişiye güven vermesi açısından müşteri temsilcisinin şirket adına çalıştığını yansıtacak şekilde uygun bir ortam oluşturulması veya yöntemler kullanılması sağlanır.

(7) Engelli kişilere hizmet verebilmek amacıyla en az bir müşteri temsilcisine gerekli eğitimlerin verilmesi sağlanır.

(8) Dış hizmet alımıyla müşteri temsilcisi istihdam edilmesi durumunda söz konusu müşteri temsilcisinin şirkete özel erişimi sınırlandırılmış ayrı bir alanda çalışması Kurum iznine tabidir.

Sürecin başlatılması ile uyulması gereken genel ilkeler

MADDE 6 –(1) Uzaktan kimlik tespiti sürecinde görüntülü görüşme başlamadan önce kişinin başvurusu uzaktan kimlik tespiti sürecinin işletildiği şirket uygulaması üzerinden elektronik ortamda doldurulan bir form ile alınır, alınan veriler kullanılarak kişi hakkında risk değerlendirmesi gerçekleştirilir. Risk değerlendirmesi sonucunda gerekiyorsa görüntülü görüşme başlatılmadan süreç sonlandırılır.

(2) Bu Yönetmelik kapsamında uygulanacak uzaktan kimlik tespiti sürecinde, kişinin uzaktan kimlik tespitinin yapılması amacıyla özel nitelikli kişisel verilerden sadece biyometrik verisi kullanılabilir ve kişinin buna dair açık rızası elektronik ortamda kayıt altına alınır.

(3) Müşteri temsilcisine uzaktan kimlik tespiti işlemleri atanırken önceden tahmin edilebilir durumlardan kaynaklı suistimal olasılığını azaltmak için gerekli mekanizmalar tesis edilir.

(4) Kişi ile yapılacak görüntülü görüşmeden önce müşteri temsilcisinin soracağı asgari sorular belirlenir ve sorulan soruların sırası ve/veya türü değişkenlik arz eder.

(5) Uzaktan kimlik tespitinin görüntülü görüşme aşaması gerçek zamanlı ve kesintisiz şekilde yapılır. Müşteri temsilcisi ile kişi arasındaki görsel-işitsel iletişimin bütünlüğünün ve gizliliğinin yeterli seviyede olması sağlanır. Bu amaçla, yapılan görüntülü görüşme uçtan uca güvenli iletişim ile gerçekleştirilir.

(6) Gerçekleşen iletişimin görüntü ve ses kalitesinin, bu Yönetmelikte yer alan hükümler ve kontroller çerçevesinde şüpheye yer bırakmayacak ve kimlik tespitinde herhangi bir kısıtlamaya imkân vermeyecek şekilde tüm görüşme esnasında yeterli seviyede olması sağlanır. Görüntü kalitesi, sunulan belgeyi beyaz ışık altında görsel olarak doğrulayabilmeye ve sunulan belgenin yıpranmamış ya da tahrif edilmemiş olduğunu kontrol edebilmeye yönelik güvenlik ögelerinin incelenmesine olanak tanır.

(7) Uzaktan kimlik tespiti sürecinde kişiye yalnızca yapılan kimlik tespiti işlemi için geçerli, merkezi olarak üretilen SMS OTP iletilir. İletilen SMSOTP'nin kişi tarafından çevrim içi olarak uygulama ara yüzü üzerinden geri gönderilmesi sağlanır. Sistemde bu SMSOTP'nin başarılı şekilde onaylanması durumunda kişinin cep telefonu numarası doğrulanmış olur.

Kullanılabilecek kimlik belgesi ve doğrulanması

MADDE 7 –(1) Uzaktan kimlik tespiti sürecinde beyaz ışık altında görsel olarak ayırt edilebilen güvenlik ögelerine, fotoğraf ve ıslak imzaya sahip olan kimlik belgesi kullanılır.

(2) Yakın alan iletişimi kullanılarak kimlik belgesinin yongası üzerinde yer alan kimlik bilgilerinin doğrulanması, kimlik belgesinden kişinin kimliğinin tespit edilmesi için gereken eşleşmenin sağlandığı anlamına gelir. Söz konusu doğrulama;

a) Kullanılan kimlik belgesinin, belgeyi çıkaran yetkili makam tarafından verildiği ve belgenin temassız yongası üzerindeki bilgilerin değiştirilmediği,

b) Kimlik belgesinin temassız yongası üzerindeki anahtarların kopyalanarak oluşturulmadığı,

kontrol edilerek yapılır.

(3) Yakın alan iletişimi kullanılarak ikinci fıkrada geçen doğrulamanın herhangi bir nedenle yapılamaması halinde kimlik belgesinin sahip olduğu bu maddenin birinci fıkrasında ifade edilen görsel güvenlik unsurlarından en az dört adedinin şekil ve içerik bakımından doğrulanması sağlanır. Sadece görsel güvenlik unsurlarının doğrulanması hallerinde şirket ilave olarak kişi ile sürekli iş ilişkisi tesisi öncesinde risk temelli yaklaşım çerçevesinde ilgili mevzuatta geçen sıkılaştırılmış tedbirlerden bir veya birden fazlasını ya da tamamını uygular. Yürütülen işlemlerde 11 inci maddenin birinci fıkrası gereği ispat yükümlülüğü şirkettedir.

(4) Görsel kimlik tespiti esnasında kişinin, kimlik belgesini kameranın önünde yatay veya dikey olarak eğmesi ve müşteri temsilcisinin vereceği talimata göre ilave hareketler yapması sağlanır. Bu amaçla kişiden, kimlik belgesinin güvenlikle ilgili kısımlarından sistem tarafından değişken ve rastgele şekilde belirlenen kısımlarına parmağını koyması istenir.

(5) Müşteri temsilcisi, görüntülü görüşme sürecinde kişiyi ve kişi tarafından sunulan kimlik belgesinin ön ve arka yüzü ile birlikte belgenin üzerindeki bilgileri gösteren fotoğraflar ve/veya ekran görüntüleri oluşturur.

(6) Müşteri temsilcisi, kişinin hareketlerinden alınan, kesilen ve büyütülen tekil görselleri kullanarak, beyaz ışık altında görsel olarak ayırt edilebilen tüm güvenlik ögeleri ile birlikte kimlik belgesinin doğru açıyla tam olarak kapsandığından ve kimlik belgesinin üzerindeki kısımlar arasındaki geçiş noktalarında tahrifatı ve sahteliği gösteren hiçbir yapaylık bulunmadığından emin olur.

(7) Sunulan kimlik belgesinde bulunan veri ve bilgilerin geçerliliği ve gerçekliğine ilişkin doğrulama, uzaktan kimlik tespiti sürecinin bir parçası olarak gerçekleştirilir. Bu kapsamda asgari olarak;

a) Kimlik belgesinde bulunması gereken karakterlerin yazı tipi, düzeni, sayısı, büyüklüğü, aralığı ve tipografisi gibi belgeyi çıkaran yetkili makamca tanımlanan özelliklere sahip olduğu,

b) Kimlik belgesinin zarar görmemiş, tahrif edilmemiş, değiştirilmemiş ve özellikle üzerine sonradan fotoğraf yapıştırılmamış olduğu,

c) Kimlik belgesi geçerlilik süresinin söz konusu kimlik belgesinin sahip olduğu standartlara aykırı olmadığı,

ç) Kimlik belgesinin MRZ'sinde yer alan bilgiler ile kimlik belgesine ait bilgilerin uyuştuğu,

d) Kişiye ilişkin kimlik belgesinde yer alan bilgilerin şirket tarafından bilinen, Kimlik Paylaşımı Sisteminden alınan ve varsa kimlik tespiti yapmak amacıyla şirketin erişimine açık olan diğer bilgiler ile eşleştiği,

e) Kimlik belgesinde yer alan seri numarasının görüntülü görüşme sırasında kimlik belgesi üzerinden kişiye okutulması suretiyle seri numarası,

doğrulanır.

Kimliği tespit edilecek kişinin doğrulanması

MADDE 8 –(1) Uzaktan kimlik tespitinin görüntülü görüşme aşamasında kişinin canlılığını tespit edici yöntemler kullanılır. Şirket sahte yüz teknolojisine dair riskleri önlemeye yönelik ilave tedbirler alır.

(2) Uzaktan kimlik tespiti sürecinde kişinin yüzü ile kimlik belgesinden yakın alan iletişimi kullanılarak alınabilmesi halinde temassız yongadaki fotoğrafın, alınamaması halinde ise kimlik belgesi üzerinde yer alan fotoğrafın biyometrik karşılaştırması yapılır.

(3) Müşteri temsilcisi, kullanılan kimlik belgesindeki fotoğrafın ve kişisel bilgilerin kişi ile uyuştuğundan emin olur.

(4) Müşteri temsilcisi, kimlik tespiti sürecinde kişi ile kuracağı diyalog ve yapacağı gözlemler neticesinde kimlik belgesindeki bilgilerin, görüşme esnasında kişi tarafından sağlanan bilgilerin ve belirtilen niyetin inandırıcı ve yeterli olduğuna kanaat getirir. Bu kapsamda kimlik avına, sosyal mühendisliğe, başka bir tarafın zorlamasıyla baskı altında gerçekleşen hareketlere ve benzeri dolandırıcılık yöntemlerine ilişkin riskler göz önünde

bulundurulur.

(5) Uzaktan kimlik tespitinin görüntülü görüşme aşamasının sonunda kişinin şirket tarafından verilecek hizmetler hakkında bilgilendirilmesi ve şirket müşterisi olacağını kabul ettiğine ilişkin sözlü onay alınması ile süreç tamamlanmış olur.

Görüntülü görüşmede sürecin sonlandırılması

MADDE 9 – (1) Zayıf ışık koşulları, düşük görüntü kalitesi ya da iletimi ve benzeri durumlar nedeniyle bu Yönetmelikte belirtildiği şekilde görsel doğrulama yapılmasının ve/veya kişi ile sözlü iletişim kurmanın mümkün olmadığı hallerde uzaktan kimlik tespitinin görüntülü görüşme aşaması sonlandırılır. Süreçte başkaca bir tutarsızlık veya belirsizlik bulunması durumunda da bu hüküm uygulanır.

(2) Uzaktan kimlik tespitinin görüntülü görüşme aşamasında kişi tarafından sunulan belgenin geçerliliği hususunda ya da dolandırıcılık veya sahtecilik teşkil edebilecek eylemlerden şüphe edilmesi durumunda, uzaktan kimlik tespiti süreci sonlandırılır.

Verilerin kaydedilmesi ve saklanması

MADDE 10 –(1) Uzaktan kimlik tespiti sürecinin tamamı, sürecin tüm adımlarını içerecek ve denetlenebilir olmasını sağlayacak şekilde kayıt altına alınır ve saklanır. Bilgi ve belge saklama gerekliliklerine ilişkin ilgili mevzuat hükümleri saklıdır.

Uzaktan kimlik tespitinde sorumluluk

MADDE 11 –(1) Uzaktan kimlik tespiti için kullanılan çözümlerin kişiyi yanlış tespit riskini en aza indirecek şekilde kullanılmasını sağlamak şirketin sorumluluğundadır. Şirket uzaktan kimlik tespiti ile kimlik tespiti yaptığı kişileri farklı bir risk profilinde izler. Bu kişilerce yapılan işlemin türüne ve tutarına bağlı olarak ilave güvenlik ve kontrol yöntemleri uygulanır. Kişilere ya da üçüncü bir tarafa yükümlülük doğuran işlemlerde itiraz halinde ispat yükümlülüğü şirkettedir.

(2) Şirketin Bilgi Sistemleri Tebliğinde ve bu Yönetmelikte yer alan hükümlere uyum durumunun, şikâyetler ile sahtecilik veya dolandırıcılık teşkil edebilecek eylemlerin değerlendirilmesi neticesinde ve gerekli görülen diğer hallerde uzaktan kimlik tespiti kullanımını kısıtlamaya veya durdurmaya Kurul yetkilidir.

ÜÇÜNCÜ BÖLÜM
Elektronik Ortamda Sözleşme İlişkisinin Kurulması

Kimlik doğrulama ve işlem güvenliği

MADDE 12 –(1) Bu Yönetmelikte aksi belirtilmedikçe, müşteri bilgilerinin görüntülenmesi gibi finansal sonuç veya yükümlülük doğurmayan işlemler hariç olmak üzere elektronik ortamda sunulan hizmetler için şirketin müşterilerine birbirinden bağımsız en az iki bileşenden oluşan bir kimlik doğrulama mekanizması uygulaması ve bu bileşenlerin kimlik doğrulama sürecinde kullanılmaları esnasında barındırdıkları kimlik doğrulama verilerinin gizliliğini sağlayacak önlemleri alması esastır. Bu iki bileşen; müşterinin "bildiği", "sahip olduğu" veya "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Bileşenlerin bağımsız olması, bir bileşenin ele geçirilmesinin diğer bileşenin güvenliğini tehlikeye atmamasını ifade eder. Müşterinin sahip olduğu bileşenin müşteriye özgü olması ve taklit edilememesi esastır.

(2) Kimlik doğrulamada T.C. Kimlik Kartının kartPIN'i veya biyometrik veri ile birlikte kullanılması veya elektronik imzanın kullanılması hallerinde birinci fıkranın gerekleri yerine getirilmiş sayılır.

(3) Kurum, birinci fıkranın uygulanmasına ilişkin istisna veya ilave güvenlik önlemleri tanımlamaya veya ilave usul ve esaslar belirlemeye yetkilidir. Birinci fıkraya uygun olmayacak şekilde iki bileşenli kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü şirkete aittir.

(4) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasında kullanılacak bileşenlerin üretim aşamalarından başlayarak kullanıcıya ulaştırılmasına kadar geçen sürecin tamamı boyunca güvenliği sağlanır.

(5) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyen yöntemler barındıracak şekilde müşteri kullanımına sunulur.

(6) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasının, başarısız kimlik doğrulama teşebbüsleri hakkında ilgili kullanıcıya sisteme ilk girdiği anda bilgi vermesi sağlanır. Başarısız teşebbüslerin belirli bir sayıyı aşması halinde müşterinin erişimi için ilave güvenlik önlemleri alınır, başarısız kimlik doğrulama teşebbüslerinin devam etmesi halinde ise ilgili kullanıcının erişimi engellenir.

(7) Şirket, mobil uygulamasını yükleyerek aktifleştirmiş olan müşterilerine, oturum açma ya da oturumun devamında herhangi bir işlemin doğrulanması için hiçbir şekilde SMS ile OTP ya da doğrulama kodu gönderemez ve bunu bir kimlik doğrulama unsuru olarak kullanamaz. Mobil uygulamanın ilk kurulumu, aktifleştirilmesi, yeniden aktifleştirilmesi aşamalarında ya da uygulamanın kullanılamaz olması durumunda SMS ile OTP ya da doğrulama kodu gönderilmesi bu fıkra hükmüne aykırılık teşkil etmez.

(8) Şirket, SIM kart değişikliği gerçekleştirmiş veya numara taşıma yoluyla elektronik haberleşme işletmecisini değiştirmiş müşterilerini Türkiye'de yerleşik mobil haberleşme işletmeleriyle gerekli entegrasyonu sağlayarak SMS OTP göndermeden önce belirler ve ilgili müşterilere, değişiklikler teyit edilmediği müddetçe, değişikliğin yapıldığı tarihten itibaren 90 gün boyunca elektronik ortamdaki hizmetler sunulurken SIM karta dayalı unsur kimlik doğrulama unsuru olarak kullanılamaz. Değişiklikler teyit edilirken iki bileşenli kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü şirkete aittir.

(9) Müşterilere kimlik ya da işlem doğrulama amacıyla kullandırılacak tek kullanımlık parolaların, tahmin edilmesi zor olacak şekilde yeterli uzunlukta, rastgele, değişken ve eşsiz olarak üretilmesi ve belirli bir süre için geçerli olması sağlanır.

(10) Müşterinin kimliğini tespit etmeye yarayan ve resmî kimlik belgesi yerine geçen belgeler üzerinde yer alan bilgiler ile anne kızlık soyadı, elektronik ortamdaki hizmetlerin sunulması esnasında hiçbir aşamada kimlik doğrulama amacıyla kullanılamaz. Şirketin kimlik doğrulamada müşterinin bildiği unsur olarak bir güvenlik sorusu kullanmak istemesi durumunda, bu güvenlik sorusunun resmî kimlik belgesi yerine geçen belgeler üzerinde yer alan bilgilerden birine ilişkin olmaması ve cevabının müşterinin kendisi tarafından belirleniyor olması gerekir.

(11) Şirketin elektronik ortamda sunulan hizmetlerinde kullanmak üzere müşterilerine sunduğu her türlü yazılım ya da mobil uygulamanın kaynağının, ilgili şirket olduğunun doğrulanabiliyor olması sağlanır. Şirket bu yazılım ya da mobil uygulamaların, müşteri güvenliğini tehlikeye sokacak herhangi bir kod içermemesini sağlamakla, güvenlik açıklarını giderecek gerekli yamaları ve güncellemeleri müşteri kullanımına sunmakla yükümlüdür.

(12) Şirket, akıllı telefonlar gibi birden fazla kimlik doğrulama bileşeninin şirkete iletilmesinde kullanılan mobil cihazlar üzerindeki uygulamaların kullandığı hassas verilerin, aynı mobil cihaz üzerindeki diğer uygulamalar ve çalışmakta olan işlemler tarafından erişilemez olmasını sağlayacak önlemler alır. Şirket, söz konusu mobil cihazların kaybolması ya da çalınması halinde bunlar üzerindeki hassas verilerin yetkisiz kişilerce erişilemez olmasını sağlamak ve mobil cihazların ele geçirilmesi, güvenilirliğinin bozulması, işletim sistemi yazılımının kırılması veya değiştirilmesi gibi hallerden kaynaklanacak risklerin azaltılması amacıyla günün teknolojisine uygun kontroller tesis etmekle yükümlüdür.

(13) Elektronik ortamda sunulan hizmetlerde birinci fıkraya göre gerçekleştirilecek kimlik doğrulama işlemi için müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanacak şekilde tek kullanımlık bir doğrulama kodu üretilir. Doğrulama kodu aracılığıyla birinci fıkrada belirtilen kimlik doğrulama unsurlarından hiçbiri hakkında bilgi edinilememesi, bilinen bir doğrulama kodu ile geçerli başka doğrulama kodlarının türetilememesi, doğrulama kodlarının taklit edilememesi sağlanır. Müşteriye atanmış bir şifreleme gizli anahtarı ile doğrulama kodunun imzalanmasının mümkün olmadığı hallerde, yedinci fıkra hükmü saklı kalmak kaydıyla SMS yoluyla müşteriye doğrulama kodu iletilebilir.

(14) Elektronik ortamda sunulan hizmetin mobil uygulama vasıtasıyla verilmesi durumunda, uygulama PIN'inin veya müşteriye ait bir biyometrik kimlik doğrulama bileşeninin müşteriye özgü bir şifreleme anahtarına erişmek üzere kullanılması ve bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin şirket nezdinde çevrimiçi olarak doğrulanması halinde, birinci fıkrada belirtilen iki bileşenli kimlik doğrulama yerine

getirilmiş kabul edilir.

Kimlik tespitini müteakip sözleşme ilişkisinin kurulması

MADDE 13 –(1) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da müşteri kimliğinin yüz yüze tespit edilmesini müteakiben, müşterilerce gerçekleştirilmek istenen işlemlere yönelik sözleşme ilişkisinin internet veya mobil hizmet kanalları üzerinden mesafeli olarak kurulması durumunda, müşterinin sözleşmeyi kuran irade beyanının aynı kanallar üzerinden 12 nci maddenin birinci fıkrasına uygun olarak gerçekleştirilmiş bir kimlik doğrulama sonrasında alınması şarttır.

(2) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da müşteri kimliğinin yüz yüze tespit edilmesini müteakiben, mesafeli olsun olmasın, müşterilerce gerçekleştirilmek istenen işlemlere yönelik olarak bir bilişim veya haberleşme cihazı üzerinden yazılı şeklin yerine geçecek nitelikte bir sözleşme ilişkisi kurulabilmesi için;

a) Söz konusu sözleşmenin bütün şartlarının, müşterinin okuyabileceği şekilde internet veya mobil hizmet kanalları üzerinden müşteriye iletilmesi,

b) (a) bendine göre müşteriye iletilen sözleşme ve bu sözleşme ile birlikte müşterinin sözleşmeyi kuran irade beyanının, 12 nci maddenin on üçüncü fıkrası ile on dördüncü fıkrasında belirtilen müşteriye özgü şifreleme gizli anahtarı ile imzalanarak şirkete iletilmesi,

c) (a) bendine göre iletilen sözleşmede müşteriye sözleşme içeriği olarak hangi bilgiler gösterilmiş ise (b) bendine göre müşteri tarafından yalnızca o bilgilerin imzalanmasının sağlanması,

şarttır.

(3) Müşteriye sunulacak hizmetlere yönelik olarak şirket ile müşteri arasındaki ilişkileri düzenleyen ve resmî şekle veya özel bir merasime tabi olmayan her türlü sözleşme ilişkisinin;

a) İkinci fıkraya uygun olarak elektronik ortamda kurulması ya da

b) Müşterinin sözleşmeyi kuran irade beyanının uzaktan kimlik tespitinin görüntülü görüşme aşamasında kimlik tespitini müteakip alınması suretiyle mesafeli olarak kurulması,

hallerinde bu sözleşmeler için yazılı şekil şartı gerçekleşmiş sayılır.

DÖRDÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Yapay zekâ temelli uygulamalar

MADDE 14 –(1) 7.500 TL tutarını aşmayan işlemlerde bu Yönetmelikte ifade edilen müşteri temsilcisinin yapacağı işlemlerin yapay zekâ temelli yöntemler ile yapılabilmesine ilişkin esasları belirlemeye Kurul yetkilidir.

Yürürlük

MADDE 15 – (1) Bu Yönetmelik yayımı tarihinden bir ay sonra yürürlüğe girer.

Yürütme

MADDE 16 – (1) Bu Yönetmelik hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.