Bankacılık Düzenleme ve Denetleme Kurumundan: (Taslak)
Görüş ve önerileriniz için: kartmevzuat@bddk.org.tr

BANKA VE KREDİ KARTI İŞLEMLERİNDE KULLANILAN BİLGİ SİSTEMLERİNİN YÖNETİMİ HAKKINDA TEBLİĞ TASLAĞI

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1 – (1) Bu Tebliğin amacı, banka ve kredi kartları ile gerçekleştirilen işlemler kapsamındaki faaliyetlerin yürütülmesinde kullanılan bilgi sistemlerinin yönetimine ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 – (1) Kartlı sistem kuran, kart çıkaran, üye işyeri anlaşması yapan kuruluşlar, üye işyerleri ve dış hizmet sağlayıcılar bu Tebliğ kapsamındadır.

Dayanak

MADDE 3 – (1) Bu Tebliğ, 10/3/2007 tarihli ve 26458 sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmeliğin 27/A maddesi hükümlerine dayanılarak düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 4 – (1) Bu Tebliğde yer alan;

a) Asimetrik şifreleme: Gizli anahtar ve açık anahtar olmak üzere iki anahtarın kullanıldığı, anahtarlardan birisinin şifrelediği verinin ancak diğer anahtar aracılığıyla açıldığı ve sadece açık anahtar bilgisi kullanılarak gizli anahtara ulaşmanın mümkün olmadığı şifreleme algoritmalarını,

b) BIN: "Bank Identification Number", kart numarasının, kart çıkaran kuruluşu tekil olarak tanımlayan alt kümesini,

c) BSDHY: 13/1/2010 tarihli ve 27461 sayılı Resmi Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliği,

ç) CNP: "Card Not Present", CP dışında kalan kartlı işlemleri,

d) CP: "Card Present", kartın ve kart hamilinin işlemin gerçekleştiği ortamda fiziksel olarak yer aldığı kartlı işlemleri,

e) Denetim izi: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtları,

f) Dış hizmet sağlayıcı: Kartlı işlem altyapısı kullanılan ya da kart ile ilişkilendirilen işlemlere ilişkin veya kart verisi saklama, işleme, iletme amacıyla kart kuruluşlarına veya üye işyerlerine hizmet veren kişileri,

g) EFT-POS: "Electronic Funds Transfer At Point Of Sale", kart kullanılarak elektronik fon transferi ile ödeme yapmaya yarayan satış terminalini,

ğ) GİB: Türkiye Cumhuriyeti Gelir İdaresi Başkanlığı'nı,

h) Güvenli şifreleme: Kimlik doğrulama, veri bütünlüğünü sağlama, gizlilik ve mahremiyeti temin etme veya inkâr edememe amaçlarıyla kullanılabilen, literatürde kabul görmüş ve güvenilirliğini yitirmemiş güçlü bir algoritma ile yeterli uzunlukta ve güvenliği kriptografik anahtar yönetimi süreci ile sağlanmış anahtarlar kullanılarak gerçekleştirilen, anahtar kullanılmaksızın şifrelenmemiş verinin elde edilmesi teorik olarak mümkün olsa bile pratikte gerektirdiği zaman ve kaynaklar dikkate alındığında uygulanabilir olmayan şifreleme faaliyetlerini,

ı) Hassas kart verisi: Kart numarasının ilk 6 ve son 4 hanesi haricinde kalan kısmı, PIN/PIN blokları, kart doğrulama kodu ve kart hamili adına finansal işlem yapılabilmesi için gerekli diğer veriler ile bu verilerin alt kümesi olan, bu verileri içeren ve herhangi bir işlemden geçirilmesi durumunda bu verilere ulaşılabilecek her türlü veriyi,

i) Hassas veri: Hassas kart verisi ile hassas kart verisini simetrik şifrelemede kullanılan anahtarlar, hassas kart verisini asimetrik şifrelemede kullanılan gizli anahtarlar ve hassas kart verisiyle ilişkili anahtarları şifrelemede kullanılan anahtarlar gibi hassas kart verisinin güvenliğine ilişkin verileri,

j) İkincil merkez: Kanun ve ilgili alt düzenlemelerinde, kuruluş için tanımlanan tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan yedek sistemlerin kullanıma hazır olacak şekilde tesis edildiği, herhangi bir kesinti durumunda kartlı işlemlere ilişkin faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesine ve personelin çalışmasına imkân tanıyacak ve kuruluşun faaliyetleri sürdürmede kullandığı asıl sistemlerin tesis edildiği yapı ile aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı,

k) İlkeler Tebliği: 14/9/2007 tarihli ve 26643 sayılı Resmî Gazete'de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliği,

l) Kanun: 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanununu,

m) Kart: Kanunda düzenlenen banka kartlarını ve kredi kartlarını,

n) Kart çıkaran kuruluş: Banka kartı veya kredi kartı düzenleme yetkisini haiz bankalar ile diğer kuruluşları,

o) Kart doğrulama kodu: Kartın üzerinde manyetik, elektronik veya basılı halde yer alan, verinin bütünlüğünü korumayı, kartın bir kart çıkaran kuruluş tarafından üretilip üretilmediğini ve kart üzerindeki verinin değiştirilip değiştirilmediğini anlamayı amaçlayan kartın güvenliğine ilişkin kodu,

ö) Kart hamili bilgisi: Kimliği belirli veya kimliği belirlenebilir kart hamillerine ilişkin, kart verisi haricinde kalan ve anonim olmayan bütün bilgileri,

p) Kart kuruluşu: Kartlı sistem kuruluşu, kart çıkaran kuruluş ve üye işyeri anlaşması yapan kuruluşları,

r) Kart verisi: Kartta manyetik, elektronik veya basılı halde yer alan veriler ile bu veriler kullanılarak üretilmiş verileri,

s) Kartlı sistem kuruluşu: Banka kartı veya kredi kartı sistemi kuran ve bu sisteme göre kart çıkarma veya üye işyeri anlaşması yapma yetkisi veren kuruluşları,

ş) Korunaklı sistem: Bünyesindeki hassas verilere fiziksel ve yazılımsal olarak erişimi kısıtlayan, şifreleme anahtarlarının korunmasını ve yönetimini sağlayan, yetkisiz erişimleri fark eden ve tepki veren, birimlerinin yetkisiz olarak değiştirilmesi ve çıkarılması ile yeni birim

eklenmesi faaliyetlerini algılamaya ve bunlara tepki vermeye yönelik kontroller barındıran, çevresel ve operasyonel şartların değiştirilmesi, normal çalışma şartlarının dışına çıkarılması veya yazılımsal anormallikler oluşturulması dolayısıyla sağladığı güvenlik seviyesinin azalmayacağına ilişkin makul güvence sunan sistemleri,

t) Kriptografik anahtar yönetimi süreci: Anahtarın ve başlangıç vektörleri, sayaçlar gibi ilgili diğer güvenlik parametrelerinin oluşturulması, dağıtımı, saklanması, yüklenmesi ve kullanılması, ömrünü tamamlamasının ardından veya güvenliği zedelendiğinde yeni bir anahtar oluşturularak eski anahtarın imhası veya arşivlenmesinin yazılı ve etkin bir biçimde yönetildiği süreci,

u) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

ü) Kuruluş: Kart kuruluşları, dış hizmet sağlayıcıları ile CNP ödeme kabul eden üye işyerlerini,

v) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

y) ÖKC: Ödeme Kaydedici Cihazı,

z) ÖKC üreticisi: Maliye Bakanlığı'ndan onay alan ve yeni nesil ÖKC ile TSM'lerden sorumlu olan ödeme kaydedici cihaz üreticisi ve ithalatçısı firmayı,

aa) PCI DSS: "Payment Card Industry Data Security Standard", PCI SSC tarafından yayımlanan Veri Güvenliği Standardını,

bb) PCI SSC: "Payment Card Industry Security Standards Council", Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyini,

cc) POI: "Point of Interaction", banka kartları ve kredi kartları ile ödeme gerçekleştirmesine imkân veren, donanım ve yazılımdan oluşan EFT-POS özelliği barındıran cihazı,

çç) POI bileşenleri: POI'nin tek bir gövdeden oluşmadığı durumlarda, POI'nin kartlı işlemlere ilişkin fonksiyonlarını gerçekleştirebilmesi için gerekli olan ve farklı gövdelerde yer alan PIN giriş aygıtı, kart okuyucu gibi cihazları,

dd) PIN: "Personal Identification Number", kart hamilinin kimliğini doğrulama amaçlı kullanılan, sadece kart hamilinin bildiği, en az dört rakamdan oluşan değeri,

ee) Sanal POS: CNP işlemlerde ödemeyi sağlayan ve kart hamillerinden alınan kart bilgileri ile kartın hesabından tahsilâta aracılık eden yazılımı,

ff) Sızma testi: Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amaçlı gerçekleştirilen testleri,

gg) Simetrik şifreleme: Hem veriyi şifrelemek hem de şifreli veriyi açmak için aynı anahtarın kullanıldığı şifreleme algoritmalarını,

ğğ) SMS: "Short Message Service", kısa mesajı,

hh) Tekrar eden ödemeler: Taksitli kredi kartı işlemlerinden farklı olarak, ödenecek toplam tutarın kredi kartının kullanılabilir limitini azaltmadığı, kart hamili ile yapılmış bir sözleşmeye istinaden tekrar eder şekilde satın alınan mal veya hizmetlere ilişkin ödemeleri,

ıı) TSM: "Trusted Service Manager", ÖKC üreticisi tarafından yeni nesil ÖKC'leri yönetmede, yazılım güncellemede, parametre yüklemede ve EFT-POS özelliği olan yeni nesil ÖKC'nin üye işyeri anlaşması yapan kuruluşlar ile iletişiminde kullanılan terminal yönetim sistemini,

ii) Üye işyeri anlaşması yapan kuruluş: Banka kartı veya kredi kartı kabulünü sağlamak amacıyla işyerleriyle anlaşma yapan bankaları ya da kuruluşları,

jj) Yeni nesil ÖKC: GİB ile ve EFT-POS özelliği bulunması halinde üye işyeri anlaşması yapan kuruluşlarla çevrimiçi çalışabilen yeni nesil ödeme kaydedici cihazı

ifade eder.

İKİNCİ BÖLÜM
Bilgi Sistemlerinin Yönetimi

Genel ilkeler

MADDE 5 – (1) Kuruluş, İlkeler Tebliğinin "Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi" başlıklı 7 nci, "Kimlik doğrulama" başlıklı 9 uncu, "Görevler ayrılığı prensibi" başlıklı 11 inci, "Yetkilendirme" başlıklı 12 nci, "İşlemlerin, kayıtların ve verilerin bütünlüğü" başlıklı 13 üncü ve "Veri gizliliği" başlıklı 15 inci maddelerinde yer verilen hükümlere tabidir. Bu maddelerde geçen "banka" ifadesi kuruluş; "destek hizmeti" ifadesi dış hizmet; "destek hizmeti kuruluşu" ifadesi dış hizmet sağlayıcı; "müşteri" ifadesi kart hamili olarak uygulanır.

(2) CNP ödeme kabul eden üye işyerleri, bu maddenin birinci fıkrasından muaf olmakla birlikte İlkeler Tebliğinin "Veri gizliliği" başlıklı 15 inci maddesinde yer verilen hükümlere tabidir.

Risk yönetimi

MADDE 6 – (1) Kuruluş, kartlı işlem altyapısını kullanılan ya da kart ile ilişkilendirilen işlemlere dair faaliyetlerinin ifasında kullandığı bilgi sistemlerine ilişkin riskleri tespit etmek, analiz etmek, ölçmek, izlemek, kontrol etmek ve raporlamak üzere kapsamlı bir risk yönetim planı oluşturur. Kartlı işlem altyapısının bir parçası olan veya herhangi bir noktada kart verisini işleyen, ileten veya saklayan donanım ve yazılımlar risk yönetim planına dâhil edilir.

(2) Kuruluş, uyguladığı risk yönetim planı çerçevesinde, dış hizmet sağlayıcılarından kaynaklanabilecek riskleri de dikkate alarak faaliyetlerinde kullandığı bilgi teknolojisi varlıklarının risk analizini gerçekleştirir; bu kapsamda varlık envanteri hazırlanır, varlıklara yönelik tehditler, tehditlerin risk seviyeleri ve uygulanacak eylemler belirlenir, yazılı hale getirilir ve uygulanma durumu üst yönetim tarafından izlenir. Bilgi sistemlerine ilişkin risk analizleri, hizmetleri etkileyen önemli güvenlik olayları sonrasında, önemli bir değişiklik öncesinde ve yeni tehditlerin tespiti halinde gözden geçirilir ve yılda en az bir defa olmak üzere güncellenir.

Denetim izlerinin oluşturulması

MADDE 7 – (1) Kuruluş, kart hamili bilgisine, hassas veriye ve bu verilerin saklandığı, işlendiği veya iletildiği sistemlere ve yazılımlara gerçekleştirilen mantıksal veya fiziksel erişimlere, kartlı işlem altyapısını kullanılan ya da kart ile ilişkilendirilen işlemlere ve yetkisiz erişim teşebbüslerine ilişkin etkin bir denetim izi mekanizması tesis eder.

(2) Denetim izi, kullanıcılara sorumluluk atayan, yeterli detay içeren ve şüpheli bir olayı izleme imkânı sunan nitelikte tutulur.

(3) Denetim izleri asgari olarak aşağıdaki bilgileri içerir:

a) İşlemi gerçekleştiren uygulama,

b) İşlemi gerçekleştiren ve varsa onaylayan kişiler,

c) İşlemin açıklaması,

ç) Yapılan işlemin zaman bilgisi,

d) İşlemin olumlu veya olumsuz sonucu,

e) Etkilenen veri ve sistemlerin bilgisi,

f) Finansal sonuç doğuran işlemlerde, işleme konu tutar bilgisi,

g) Bir kart hamiline ilişkin veriye yapılan erişimlerde, kart hamiline dair tanımlayıcı bir bilgi,

ğ) Kartlı işlem seçeneklerini değiştiren işlemlerde, kartlı işlem seçeneklerinin değişiklikten önceki ve sonraki halleri.

(4) Denetim izleri asgari 3 yıl süreyle denetime hazır bulundurulacak şekilde saklanır.

(5) Denetim izlerinin bütünlüğünün sağlanması ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır. Denetim izleri yetkisiz değiştirilmeye karşı korunur. Ayrıca denetim izleri, ayrıcalıklı yetkiye sahip kullanıcıların kendi faaliyetlerine ilişkin denetim izlerine müdahale edemeyeceği şeklide korunur.

(6) Denetim izi mekanizmalarının geçici veya sürekli olarak durdurulmasını önlemeye ve durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(7) Denetim izlerinin yeterli güvenlik seviyesi bulunan ortamlarda saklanması, yedeklerinin alınması ve olası bir mücbir sebep ya da olağanüstü hal sonrasında erişilebilirliği temin edilir.

(8) Bilgi sistemleri faaliyetleri kapsamında dış hizmet alınıyor olması durumunda kuruluş, dış hizmet sağlayıcı tarafından tutulan denetim izlerinin kendi standartlarına uygunluğunu ve kendisinin bu denetim izlerine erişebilirliğini temin eder.

(9) Kuruluş, denetim izlerinin düzenli olarak gözden geçirilmesine, değerlendirilmesine ve raporlanmasına ilişkin iç süreçlerini oluşturur.

Değişiklik yönetimi

MADDE 8 – (1) Kuruluş, bünyesindeki bilgi sistemleri üzerinde gerçekleştirilen ve kart verisi işleyen, ileten ya da saklayan donanım ve yazılımlara ilişkin her türlü bakım, yama ve değişikliğin uygun bir şekilde planlanmasını, yetkilendirilmesini, test edilmesini, gerçekleştirilmesini, belgelendirilmesini ve sonrasında denetlenebilirliğini sağlayacak, yazılı ve etkin bir değişiklik yönetimi süreci işletir.

(2) Kuruluş, kart verisi işleyen, ileten ya da saklayan yazılımlar için, yazılım geliştirilen ortamların ve geliştirilen yazılımların canlı ortama aktarılmadan önce test edildiği ortamların, canlı ortamlardan ayrılmasını ve bu ortamların herhangi birinde değişiklik yapma yetkisine sahip personelin diğerlerinde değişiklik yapma yetkisinin bulunmamasını sağlar. Bununla birlikte, test ve geliştirme ortamlarında kullanılan verilerin canlı ortam verileri ile eşleştirilemeyecek nitelikte olmasını temin eder.

(3) Kuruluş, kart verisi işleyen, ileten veya saklayan sistemlere ilişkin değişikliklerde etki analizi yapılmasını, değişikliğin yetkili kişi veya kişilerce onaylanmasını ve değişikliği geri çekme prosedürünün oluşturulmasını sağlar.

(4) CNP ödeme kabul eden üye işyerleri bu maddenin ikinci ve üçüncü fıkralarına tabi değildir.

Dinamik kimlik doğrulama

MADDE 9 – (1) Dinamik kimlik doğrulama, kimlik doğrulama verisinin en az iki bileşenden oluştuğu ve bu bileşenlerden birinin ele geçirilmesi durumunda diğerinin güvenliğinin azalmadığı kimlik doğrulama mekanizmasıdır

(2) CP işlemlerde kullanılacak dinamik kimlik doğrulamada, kimlik doğrulama bileşenleri, kişinin "bildiği", "sahip olduğu" veya "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olacak şekilde seçilir.

(3) CNP işlemlerde kullanılacak dinamik kimlik doğrulamada, kimlik doğrulama amacıyla kullanılan veri kümesi her bir kullanım için tekillik arz eder, bir kez kimlik doğrulama gerçekleştirilen veri kümesi ile ikinci bir kimlik doğrulama gerçekleştirilemez. Dinamik kimlik doğrulama kapsamında, kimlik doğrulamayı üye işyeriyle ve işlem tutarıyla ilişkilendiren kimlik doğrulama mekanizması kullanılır.

(4) Dinamik kimlik doğrulama bileşenlerinden birisinin tek kullanımlık şifre olması halinde, üçüncü fıkra kapsamında, tek kullanımlık şifrenin yetkilendirilmekte olan işlem haricinde herhangi başka bir işlem için geçerli olmaması sağlanır.

(5) Tekrar eden ödemeler için uygulanacak dinamik kimlik doğrulama mekanizması, ilk işlem esnasında, ödenen tutarın değişmesi durumunda ve uzun süreli işlemlerde asgari olarak yılda bir kez; kimlik doğrulama amacıyla kullanılan veri kümesinin her bir kullanım için tekillik arz ettiği, bir kez kimlik doğrulama gerçekleştirilen veri kümesi ile ikinci bir kimlik doğrulamanın gerçekleştirilemediği kimlik doğrulamayı ve ödemenin ne sıklıkla gerçekleşeceği, kaç kez tekrar edeceği ve her bir tekrarda ödenecek tutar hususlarında kart hamilinin SMS, e-posta gibi bir yöntemle bilgilendirilmesini içerir. Bunlar haricindeki tekrarlarda kart hamilinin kimliğinin doğrulanması zorunlu değildir. Bilgilendirme, sözleşme aşamasında belirlenen şekilde işleme ilişkin tutarın kart hamilinin hesabına işlenmesi öncesinde veya işlenmesinin hemen ardından gerçekleştirilir.

İşleme ilişkin verilerin korunması

MADDE 10 – (1) Hassas kart verisi tutan, işleyen veya ileten gerçek ve tüzel kişiler ile münferit sistemler, hassas kart verisinin güvenliğine ilişkin uygun kontrolleri işletir.

a) Hassas kart verisi herhangi bir sisteme kart hamili haricinde bir kişi tarafından manüel girilemez.

b) Hassas verilerin iletimi güvenli şifreleme ile gerçekleştirilir ve iletişim öncesinde iletişimi gerçekleştirecek taraflar birbirlerinin kimliğini güvenli şifreleme metotlarından faydalanarak doğrular.

c) Kart numarasının ilk 6 ve son 4 hanesi haricinde kalan kısmı, şifrelenmiş olsa dahi kart kuruluşları ve bu kuruluşlara hizmet veren dış hizmet sağlayıcılar haricinde hiçbir gerçek veya tüzel kişi tarafından tutulamaz.

ç) Kart doğrulama kodu, şifrelenmiş olsa dahi kartın dışında tutulamaz. Kart çıkaran kuruluş, kart doğrulama kodu hesaplamada kullanılan anahtarları ve diğer kritik verileri sadece korunaklı sistem bünyesinde saklayabilir.

d) PIN bilgisi, PIN bilgisi kullanılarak üretilmiş veri veya herhangi bir işlemden geçirilmesi halinde PIN bilgisine ulaşılacak veri, kart çıkaran kuruluş ve bu kuruluşa hizmet veren dış hizmet sağlayıcılar haricinde hiçbir gerçek veya tüzel kişi tarafından tutulamaz.

e) Bu Tebliğ ile hassas kart verilerini saklaması uygun görülenler, veriyi ya güvenli şifreleme ile şifrelenmiş olarak ya da korunaklı sistemlerde saklayabilir.

f) Hassas kart verilerini işlemesi Kanun veya alt düzenlemeleri kapsamında uygun görülenler, veriyi korunaklı sistemlerde işleyebilir. Kart numarasını kullanarak, herhangi bir işlemden geçirilmesi halinde hassas kart verisine ulaşılamayacak veri üretme işlemlerinin ve hassas kart verisini iletmek üzere şifreleme işlemlerinin, kullanıcıların kart verilerine müdahalesine müsaade etmeyen bir sistem tarafından gerçekleştirilmesi, bu hükmün uygulanmasında hassas kart verisinin işlenmesi kapsamında değerlendirilmez.

g) Hassas kart verisi, kart hamili kontrolündeki bir cihazda ancak cihazın kart verisini saklayan biriminin korunaklı sistem özelliklerini barındırması ve cihazın diğer birimlerinden fiziksel veya yazılımsal olarak ayrı olması durumunda tutulabilir.

ğ) Hassas veri taşıyan cihazların ömürlerini tamamlamasının ardından, cihaz bünyesindeki hassas veri geri döndürülemeyecek şekilde silinerek güvenli imhası gerçekleştirilir.

h) Hassas kart verisi denetim izlerinde tutulamaz, hiçbir yazılı belgede yer alamaz.

(2) Kart verisi tutan, işleyen veya ileten gerçek ve tüzel kişiler ile münferit sistemler, asgari olarak PCI SSC tarafından yayımlanan ilgili standardın/standartların güncel versiyonu ile kartlı sistem kuruluşlarının tanımlamış oldukları süre çerçevesinde uyumlu hale gelir ve bu durumu kartlı sistem kuruluşlarının ve PCI SSC'nin tanımlamış olduğu belgeler ile ispatlar.

(3) PCI SSC tarafından yayımlanan ilgili standardın/standartların güncel versiyonu ile uyumlu olduğunu yerinde denetimler ile ispatlaması gereken tarafların denetimi, PCI SSC tarafından yetkilendirilmiş ve yurtiçinde kurulmuş denetçi kuruluşlar tarafından gerçekleştirilir. Denetlenen ile denetimi gerçekleştirecek kuruluşların karşılıklı yükümlülükleri, BSDHY'de yer verilen ilkeler ile uyumlu olacak şekilde taraflar arasında imzalanan sözleşmelerle belirlenir.

ÜÇÜNCÜ BÖLÜM
Kart Çıkaran Kuruluşlar

Kart hamilinin kimliğinin doğrulanması ve işlemin onaylanması

MADDE 11 – (1) Yurtiçinde kurulu bir üye işyeri anlaşması yapan kuruluş aracılığıyla gerçekleşen işlemlerde, kart hamilinin kimliğinin doğrulanması için dinamik kimlik doğrulama haricinde bir mekanizma kullanılmış ise, kart çıkaran kuruluşlar bu işlemleri onaylamaz ve işleme ilişkin tutarı kart hamilinin hesabına işlemez. Yurtdışında gerçekleştirilen işlemlerde ve yurtdışına gerçekleşen ödemelerde altyapının teknik özelliklerinin uygun olduğu kartlı işlemlerde, kart hamilinin kimliğinin doğrulanması için dinamik kimlik doğrulama kullanılmasına yönelik kart üzerinde gerekli kısıtlama yapılır ve kart çıkaran kuruluş bünyesinde gerekli izleme faaliyetleri gerçekleştirilir. Çevrimdışı temassız işlemler ve telefon üzerinden gerçekleştirilen ödemeler bu hükmün kapsamı dışındadır.

(2) Kart hamili adresi, telefon numarası, kart limiti, risk kısıtlama tercihleri gibi doğası gereği sabit olması beklenen bilgilere ilişkin değişiklik taleplerinde, kart çıkaran kuruluş, talep sahibinin kimliğini doğrular ve talebin iletildiği kanal haricindeki bir iletişim kanalı kullanarak değişikliğe dair kart hamilini bilgilendirir.

(3) Tekrar eden ödemelerde işlemin yurt dışında kurulu bir üye işyeri anlaşması yapan kuruluş üzerinden gerçekleşmesi halinde, süreç kartlı sistem kuruluşları tarafından belirlenen kurallar çerçevesinde gerçekleşir; ancak kart çıkaran kuruluş işleme ilişkin tutarı kart hamilinin

hesabına işlemesi öncesinde veya işlemesinin hemen ardından kart hamilini bilgilendirir. Üye işyeri anlaşması yapan kuruluşun kurulu olduğu ülkeden bağımsız olarak, kart hamili üye işyerine veya kart çıkaran kuruluşa ödemeyi durdurma talebini iletmesi halinde ödeme devam ettirilemez.

Kartlı işlem seçenekleri

MADDE 12 – (1) Kart çıkaran kuruluş, kart hamillerine işlem sınırlama seçenekleri sunar. Bu seçenekler asgari olarak;

a) Kartın CNP ödemelere kapatılabilmesi,

b) Kartın internet üzerinden gerçekleşen ödemeler haricindeki CNP ödemelere kapatılabilmesi,

c) Kart hamilinin kart verisini üye işyerine vermesini gerektirmeyen bir yöntemin kullanılması haricinde kartın CNP ödemelere kapatılabilmesi,

ç) Kartın yurtdışında kullanıma kapatılabilmesi,

d) Kartın yurtdışına yapılan CNP ödemelere kapatılabilmesi,

e) Kartın kredi kartı hesabından gerçekleştirilecek nakit çekim işlemine kapatılabilmesi,

f) Kartın yurt dışında nakit çekim işlemine kapatılabilmesi,

g) Kartın manyetik şeridinde hassas kart verisi bulunması

hususlarını içerir. Kart hamili tarafından belirlenen seçeneklere aykırılık teşkil eden işlemlere ilişkin kart hamili sorumlu tutulamaz.

(2) Kart çıkaran kuruluş, kart hamillerine işlem limitlerine ilişkin asgari olarak;

a) Kartın CNP ödemelerde,

b) Kartın yurtdışında kullanımında,

c) Kart ile yurtdışına yapılan CNP ödemelerde

tek bir işleme veya hesap dönemi içerisindeki toplam işlemlere ilişkin işlem üst tutarının belirlenebilmesi seçeneklerini sunar. Kart hamili, belirlediği üst tutara aykırılık teşkil eden işlemlere ilişkin, belirlemiş olduğu üst tutar haricinde sorumlu tutulamaz.

(3) Kart çıkaran kuruluş, ikinci fıkradaki işlemlere ilişkin kart hamillerine bilgilendirme seçenekleri de sunar. Bilgilendirme, işleme ilişkin tutarın kart hamilinin hesabına işlenmesi öncesinde veya işlenmesinin hemen ardından gerçekleştirilir.

(4) Kart çıkaran kuruluş, çıkardığı CNP ödeme yapabilen kartlar için kart hamillerine sanal kart hizmeti de sunar.

(5) Kart çıkaran kuruluş, kartlı işlem seçeneklerinin tanımlanması ve değiştirilmesi için doğrudan başvuru imkânının yanı sıra; kart hamili sayısını dikkate alarak, internet bankacılığı ve mobil bankacılık gibi güvenli bir ortam üzerinden de imkân sunabilir.

(6) Hesap özetlerinde, harcamaların sektörel dağılımları yer alır, CNP olarak gerçekleştirilen ödemeler, tekrar eden ödemeler, yurtdışında gerçekleştirilen işlemler ve yurtdışına yapılan ödemeler vurgulanır.

(7) Kart çıkaran kuruluş, kartlarını CNP ödemelere ve yurtdışında kullanıma kapalı olarak müşterilerine sunar. Kartın CNP ödemelerde ve yurtdışında kullanılabilir olması ancak müşterinin bilgilendirilmesi ve açık onayının alınması halinde mümkün olur. Kartlarda gerçekleşecek yenileme işlemi için bu hüküm aranmaz.

(8) Kart çıkaran kuruluş, her bir kart için, kart kullanılarak bir gün içinde çekilebilecek nakde ilişkin üst sınır belirler.

Kartın güvenliği

MADDE 13 – (1) Kart çıkaran kuruluş, bir karta ilişkin başarısız kimlik doğrulama teşebbüslerinin belirli bir sayıyı aşması halinde, kartı sürekli veya geçici olarak kullanıma kapatır ve kart hamilinin yapılan kapatma işlemi ve kapatılan servislerin güvenli bir şekilde aktifleştirilmesi ile ilgili olarak bilgilendirilmesini temin eder.

(2) Kart çıkaran kuruluş, kart hamili ile yapacağı sözleşmede, güvenlik kaygısı ile tek bir işlemi engelleyebileceğine veya kartı sürekli veya geçici olarak kullanıma kapatabileceğine, kullanıma kapatmaya ilişkin kart hamili ile nasıl temasa geçileceğine ve kartın kullanıma nasıl yeniden açılacağına ilişkin hükümlere yer verir. Kart çıkaran kuruluş, yalnızca geçerli bir gerekçe ile kartı sürekli veya geçici şekilde kullanıma kapatabilir.

(3) Kart çıkaran kuruluş, kartın ve PIN'in üretilmesi de dâhil olmak üzere, kartın veya PIN'in kart hamiline iletilmesinde ya da kart hamili tarafından PIN oluşturma işleminde kullanılan bütün yöntemler için, bilgilerin gizliliğini sağlayacak uygun kontrol ortamını tesis etmek ve olabilecek her türlü suistimal olayına karşı gerekli önlemleri almakla yükümlüdür.

(4) Kart çıkaran kuruluş, kendi bünyesinde meydana gelen veya başka bir kuruluş nezdinde meydana gelip kart çıkaran kuruluşa bilgisi iletilmiş olan suistimal olaylarına ilişkin, etkilenmesi muhtemel kart hamillerine almaları gereken önlemler konusunda bilgi verir.

(5) Kart verisi saklayan, işleyen veya ileten sistemlerin ya da bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğini olumsuz etkileyen ve bununla birlikte kart hamilini muhtemel finansal zarara uğratabilecek olaylar suistimal olayı olarak kabul edilir.

Dış hizmet alımı

MADDE 14 – (1) Kart çıkaran kuruluş, hizmet aldığı dış hizmet sağlayıcıların bu Tebliğ ve PCI DSS ile uyumluluk durumlarını izler ve sundukları hizmete ilişkin herhangi bir kapsam kısıtlamasına gitmeksizin standart ile uyumlu olduklarını yılda bir kez belgelediklerinden emin olur. Kart çıkaran kuruluş, dış hizmet sağlayıcıların bu Tebliğ ile uyumlu olduklarına ve kartlı işlem altyapısının güvenliğini azaltmadıklarına ilişkin, dış hizmet sağlayıcı nezdinde gerçekleştirdiği denetimlerle veya başka taraflarca gerçekleştirilen yerinde denetimler sonucunda oluşturulan raporlardan faydalanarak makul güvence oluşturur.

(2) Kart çıkaran kuruluş, dış hizmet sağlayıcı nezdinde tespit edilen bulgulardan kartlı işlem altyapısını önemli oranda etkileyebilecek veya kart hamillerinin finansal kayba uğramasına yol açabilecek olanlarını diğer kart çıkaran kuruluşlara duyurur. Duyuru, tespite ilişkin dış hizmet sağlayıcının görüşünün alınmasından itibaren en geç 7 gün ve herhalde tespitin yapıldığı günden itibaren en geç 30 gün içerisinde gerçekleştirilir.

DÖRDÜNCÜ BÖLÜM
Üye İşyeri Anlaşması Yapan Kuruluşlar

Üye işyerleri ile sözleşmeler

MADDE 15 – (1) Üye işyeri anlaşması yapan kuruluş, üye işyerleri ile yaptığı sözleşmelerde, sunulan ödeme hizmetlerinin taşıdığı riskler çerçevesinde;

a) Üye işyerlerinin kart ve kart hamili ile ilgili bilgilerin gizliliğinin sağlanması için uygulaması gereken asgari güvenlik kontrollerine,

b) Üye işyerlerinin, hassas kart verisini, hiçbir nedenle saklamayacağına, kopyalamayacağına, açıklamayacağına ve üye işyeri anlaşması yapan kuruluş ile bu kuruluşun yetkilendirdiği dış hizmet sağlayıcıları dışında herhangi bir yere göndermeyeceğine,

c) Üye işyerinin, kart hamili bilgisini ancak kart hamilinin rızası alınması neticesinde paylaşabileceğine,

ç) Üye işyerinin kendisine ait satış işlemini başka iş yerinin POI'sinden veya başka iş yerinin satış işlemini kendi POI'sinden yapmayacağına,

d) Ödemeye ilişkin verilere, POI'ye veya kartlı işlem altyapısına etki edebilecek tüm güvenlik olaylarını üye işyeri anlaşması yapan kuruluşa bildireceğine,

e) Üye işyerinin suistimal işlem yaptığını tespit etmesi halinde, üye işyeri anlaşması yapan kuruluşun bu durumu diğer üye işyeri anlaşması yapan kuruluşlar ile paylaşacağına,

f) Üye işyeri kaynaklı suistimal işlem şüphesi ya da tespiti halinde, işyeri hesaplarına üye işyeri anlaşması yapan kuruluş tarafından ihtiyaç duyulacak sürelerde bloke konabileceğine,

g) Üye işyerine hizmet veren dış hizmet sağlayıcının süreç veya sistemlerinde, kartlı işlem altyapısını önemli oranda etkileyebilecek ya da kart hamillerinin finansal kayba uğramasına yol açabilecek önemli bulguların tespit edilmesini gerekçe göstererek; üye işyeri anlaşması yapan kuruluşun üye işyerinden dış hizmet alımını durdurmasını talep etmesi halinde, üye işyerinin makul bir süre içerisinde dış hizmet alımını durduracağına,

ğ) Tarafların bu Tebliğ hükümlerine uygun hareket edeceğine,

h) Üye işyerinin, bu Tebliğ hükümleri ile uyumluluğunun, Kurum ve üye işyeri anlaşması yapan kuruluş tarafından denetlenebileceğine

ilişkin olarak uyulması gereken hükümlere ve aksi durumlarda uygulanacak para cezaları ve gerekmesi halinde sistemden çıkarma hallerine yer verir.

Kartlı işlem altyapısı

MADDE 16 – (1) Üye işyeri anlaşması yapan kuruluş, kart hamilinin kimliğinin dinamik kimlik doğrulama ile doğrulanarak işlem yapılmasına ilişkin altyapı sunar. Üye işyeri anlaşması yapan kuruluş, sunduğu altyapı üzerinde, yurt içinde kurulu bir kart çıkaran kuruluş tarafından çıkarılmış bir kart ile gerçekleştirilen tüm işlemlerde, kart hamilinin kimliğinin dinamik kimlik doğrulama ile doğrulanmasının sağlanmasına yönelik kısıtlamalar yapar. Çevrimdışı temassız işlemler ve telefon üzerinden gerçekleştirilen ödemeler bu hükmün kapsamı dışındadır.

(2) Üye işyeri anlaşması yapan kuruluş, uygulamasının yüklü olduğu farklı POI'lerde aynı anahtarları kullanmaz, sanal POS'larda kullanılan anahtarların tekil nitelik taşımasını sağlar.

(3) Tekrar eden ödemeler için üye işyeri anlaşması yapan kuruluş tarafından üye işyerlerine sunulan altyapı, ilk işlemde tutar, ödemenin ne sıklıkla gerçekleşeceği ve ne kadar tekrar edeceği bilgilerini üye işyeri anlaşması yapan kuruluşa iletir. Sonrasında ödemenin devam etmesi için üye işyerinden herhangi bir bilgi beklenmez.

(4) Üye işyeri anlaşması yapan kuruluş, telefon üzerinden ödeme kabul edecek üye işyerlerine, hassas kart verisinin otomatik yanıt sistemine kart hamili tarafından tuşlanmasını ve güvenli şifreleme ile sistemsel olarak doğrudan kendisine aktarılmasını sağlayan altyapı sunar ve kullanımını teşvik eder.

(5) Üye işyeri anlaşması yapan kuruluş, üye işyeri adresi, telefon numarası gibi doğası gereği sabit olması beklenen bilgilere ilişkin değişiklik taleplerinde, talebin sahibinin kimliğini

ve bilgideki değişikliği doğrular ve değişiklik talebinin iletildiği kanal haricindeki bir iletişim kanalı kullanarak üye işyerini bilgilendirir.

(6) Üye işyeri anlaşması yapan kuruluş, üye işyerinin unvanını üye işyerinin tabelasında yer alan isimle ilişkili ve anlaşılır şekilde kaydeder, üye işyerinin faaliyet göstermekte olduğu sektörü güncel tutar.

İzleme ve gözetim faaliyetleri

MADDE 17 – (1) Üye işyeri anlaşması yapan kuruluş, kendisinin ve anlaşma yapmış olduğu üye işyerlerinin hizmet aldığı dış hizmet sağlayıcıları ile anlaşma yapmış olduğu üye işyerlerinin, bu Tebliğ ve PCI DSS ile uyumlu olduklarına ve kartlı işlem altyapısının güvenliğini azaltmadıklarına ilişkin, gerçekleştirdiği denetimlerden veya geçerliliğini yitirmemiş denetim raporu, sertifika gibi belgelerden faydalanarak makul güvence oluşturur. Üye işyeri anlaşması yapan kuruluş, kart hamili ile kendisi arasında kart verisi tutan, işleyen veya ileten tüm sistemlerin, herhangi bir kapsam kısıtlamasına gitmeksizin PCI DSS ile uyumlu olduklarını yılda bir kez belgelediklerinden emin olur.

(2) Üye işyeri anlaşması yapan kuruluş, üye işyerleri ve dış hizmet sağlayıcılar nezdinde tespit edilen bulgulardan, kartlı işlem altyapısını önemli oranda etkileyebilecek veya suistimal olayına sebebiyet verebilecek olanlarını diğer üye işyeri anlaşması yapan kuruluşlara duyurur. Duyuru, tespite ilişkin dış hizmet sağlayıcının görüşünün alınmasından itibaren en geç 7 gün ve herhalde tespitin yapıldığı günden itibaren en geç 30 gün içerisinde gerçekleştirilir.

(3) TSM nezdinde tespit edilen bulgulardan, kartlı işlem altyapısını önemli oranda etkileyebilecek veya kart hamillerinin finansal kayba uğramasına yol açabilecek olanlarını, üye işyeri anlaşması yapan kuruluşlar ortak bir raporla Kuruma raporlar.

(4) Üye işyeri anlaşması yapan kuruluş, sahtecilik ve dolandırıcılık faaliyetlerinin önlenmesine yönelik olarak, anlaşması bulunan üye işyerlerine ilişkin takip mekanizmaları tesis eder. Takip edilmekte olan konularda olağan dışı değişiklik meydana gelen üye işyerleri için, gerekli incelemeler gerçekleştirilir ve uygun aksiyonlar alınır.

(5) Üye işyeri anlaşması yapan kuruluş, kendi bünyesinde veya anlaşması bulunan üye işyerleri ile hizmet aldığı dış hizmet sağlayıcılar nezdinde meydana gelen suistimal olaylarına ilişkin detaylı bilgiyi diğer üye işyeri anlaşması yapan kuruluşlara ve etkilenmesi muhtemel kart hamili listesini, etkilenmesi muhtemel kart hamillerinin kartlarını çıkaran kuruluşlara bildirir. Bildirim, tespite ilişkin dış hizmet sağlayıcının görüşünün alınmasından itibaren en geç 7 gün ve herhalde tespitin yapıldığı günden itibaren en geç 30 gün içerisinde gerçekleştirilir.

Üye işyeri adına hassas kart verisinin saklanması ve kullanılması

MADDE 18 – (1) Üye işyeri adına, kart hamilinin talebi halinde, bu Tebliğ hükümlerine uygun olarak, sadece üye işyeri anlaşması yapan kuruluş veya üye işyeri anlaşması yapan kuruluşun dış hizmet sağlayıcısı nezdinde kart verisi saklanabilir. Üye işyeri, kart hamilinin talebini, kanıtlanabilir bir şekilde, yazılı veya elektronik olarak alır ve inkâr edilemezliği sağlar.

(2) Kart verisini saklayan kuruluş, adına kart verisi saklanan üye işyeri tarafından saklanmak üzere, kart numarasını, kart hamilini ve üye işyerini temsil eden, belirli bir ömrü olan, herhangi bir işlemden geçirilerek hassas kart verisine ulaşılması mümkün olmayan ve ele geçirilmesi halinde kart hamili adına sahte işlem yapılamayacak referans kodu üretir. Referans kodunun adına kart verisi saklanan üye işyerine özgü olması ve sadece bu üye işyeri tarafından

kart verisini saklayan kuruluşa iletilmesi halinde kart verisinin kullanılabilmesi sağlanır. Kart verisini saklayan kuruluş, referans kodu oluşturulması öncesinde ve referans kodu ile kart verisinin kullanımı sırasında üye iş yerinin kimliğini doğrular ve erişim kontrolleri tesis eder.

(3) Üye işyeri adına kart verisi saklandığı durumlarda, saklanan hassas kart verisi hiçbir biçimde üye işyerine iletilmez. Saklanan kart verileri, yasalarla açıkça yetkili kılınan merciler dışındaki taraflarla paylaşılmaz.

(4) Üye işyeri adına saklanan hassas kart verisi iki yıl boyunca ödeme amaçlı kullanılmazsa iki yıllık sürenin dolduğu tarihi takip eden ayın ilk gününde silinir.

BEŞİNCİ BÖLÜM
Üye İşyerleri

Kartlı işlem altyapısı

MADDE 19 – (1) Üye işyeri, kendi kontrolündeki kartlı işlem altyapısını dinamik kimlik doğrulama mekanizmasını destekleyecek şekilde tesis eder. CNP işlemlerde, sanal kart ile ödemeye ve kart verisinin üye işyerine iletilmesini gerektirmeyen diğer ödeme metotlarından en az bir tanesine destek verir.

(2) Üye işyeri, kartın ve kart hamilinin fiziksel olarak bulunduğu hallerde, sanal POS veya farklı bir yöntem kullanarak, kartın üzerinde yer alan verilerin manüel olarak girilmesi ile ödeme işlemini gerçekleştirmez. Üye işyeri, CP işlemlerde, kartın POI haricinde bir cihaz üzerinden herhangi bir işleme tâbi tutulmamasını sağlayacak altyapıyı tesis eder.

(3) CNP işlemlerde, kart verisinin üye işyeri sistemlerine kadar güvenli akışının sağlanmasından ve üye işyerinde hassas kart verisi tutulmadan üye işyeri anlaşması yapan kuruluşa ait olan bir cihaza veya sisteme verilerin aktarılmasından üye işyeri sorumludur. Posta, e-posta, SMS gibi güvenli şifreleme içermeyen iletişim kanalları üzerinden gerçekleşecek ödemelerde hassas kart verisi kullanılamaz. Telefon üzerinden gerçekleşecek işlemlerde hassas kart verisinin gerekmesi halinde, bu veri bir otomatik yanıt sistemine kart hamili tarafından tuşlanır ve güvenli şifreleme ile şifrelenmesinin ardından veri sistemsel olarak doğrudan üye işyeri anlaşması yapan kuruluşa aktarılır.

(4) Tekrar eden ödemeler için üye işyeri ilk işlem öncesinde, üye işyeri anlaşması yapan kuruluşa tutar bilgisi, ödemenin ne sıklıkla gerçekleşeceği ve ne kadar tekrar edeceği bilgilerini iletir. Sonrasında üye işyeri herhangi bir hassas kart verisi saklamaz ve ödemenin tekrarı için herhangi bir iletimde bulunmaz.

(5) Üye işyeri, kendi bünyesinde meydana gelen suistimal olaylarını tespit etmesinin akabinde bu hususa ilişkin genel bilgiyi ve gerçekleştirilen incelemeyi müteakip detaylı bilgiyi, anlaşması bulunan tüm üye işyeri anlaşması yapan kuruluşlara iletir.

(6) Üye işyeri, kart hamili tarafından PIN'in POI'ye girilmesi esnasında PIN gizliliğinin zarar görmemesi ve kartın üye işyerinin kontrolüne girmeksizin işlemin kart hamili tarafından tamamlanabilmesi için gerekli önlemleri alır, masaüstü tipi POI'yi uygun şekilde konumlandırır.

Kart hamiline ve işleme ilişkin bilgilerin güvenliği

MADDE 20 – (1) Üye işyeri, şifrelenmiş bile olsa hiçbir biçimde hassas kart verisi saklayamaz, hassas kart verisini kâğıt üzerinde veya elektronik ortamda tutan veya işleyen bir sistem kuramaz. Hassas kart verisinin, üye işyeri anlaşması yapan kuruluşa veya üye işyeri

anlaşması yapan kuruluşa hizmet sunan dış hizmet sağlayıcıya iletilmek üzere, kişilerin kart verilerine müdahalesine müsaade etmeyen bir sistem tarafından güvenli şifreleme ile şifrelenmesi, bu maddenin uygulanmasında verinin işlenmesi kapsamında değerlendirilmez.

(2) Üye işyeri, işi gereği kart verisine ihtiyaç duyması halinde, hassas kart verisi haricinde kalan kart verisinden ihtiyaç duyulan minimum veri setine karşılık gelen bölümünü, bu veri setinin yetkisiz kişilerce ele geçirilmesi durumunda gizlilik ihlâline veya haksız menfaat sağlanmasına sebebiyet verilmemesi hususları da göz önünde bulundurulmak kaydıyla, ancak anlaşması bulunan tüm üye işyeri anlaşması yapan kuruluşlar ile yapılacak sözleşmeler çerçevesinde saklayabilir ve işleyebilir. Bunun haricinde üye işyeri herhangi bir kart verisini saklayamaz ve işleyemez. CP işlemler için veri aktarımı, POI'nin dış bağlantı ara yüzleri üzerinden, üye işyeri anlaşması yapan kuruluş ile üye işyeri arasında belirlenecek formatta ve şekilde yapılır.

(3) Üye işyeri, sadece gerçekleşmekte olan ödemenin tamamlanması, teslimat, değiştirme ve iade gibi işlemler için kart hamili bilgisi talep edebilir. Bunun haricinde, kart hamilinden bilgi talep edemez ve kart hamili bilgisi saklayamaz. Kart hamili, kişisel bilgilerinin toplanmasını veya paylaşılmasını mal veya hizmet alımının bir koşulu olarak kabul etmeye zorlanamaz. Üye işyeri tarafından kart hamiline, mal veya hizmet satışından bağımsız olarak kişisel bilgilerinin kullanılmasına izin verme seçeneği sunulabilir. Bu hususta, kart hamiliyle üye işyeri arasında kişisel bilgilerin toplanması hususunda yapılacak sözleşme satış sözleşmesiyle birleştirilemez.

(4) Üye işyeri kart verilerinin işlenmesinde, saklanmasında ve iletilmesinde kullanılan ve kendi kontrolünde bulunan sistemlerin ve kart hamiline ilişkin tuttuğu verilerin güvenliğinin sağlanmasından sorumludur. Bu çerçevede üye işyeri, elektronik ortamda ve fiş, fatura, makbuz gibi fiziki belgelerde yer alan kart hamiline ilişkin verileri saklarken;

a) Veriyi, işin gerektirdiği minimum süre boyunca güvenli bir biçimde saklar,

b) Verinin kendisine ve veriye ilişkin kritik sistem kaynaklarına erişimi işin gerekliliği ile sınırlayarak uygun kimlik doğrulama kontrolleri ile izinsiz fiziksel ve elektronik erişimleri önleyecek ve tespit edecek kontrolleri işletir,

c) Verinin, ağ üzerinden iletilmesi esnasında gerekli güvenlik önlemlerini alır,

d) Sürenin tamamlanmasının ardından verinin güvenli imhasını gerçekleştirir.

(5) Üye işyerinin 20/6/2013 tarihli ve 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" kapsamında elektronik para veya ödeme kuruluşu olması durumunda, bu Tebliğin beşinci maddesinin ikinci fıkrasına, sekizinci maddesinin dördüncü fıkrasına, 10 uncu maddesinin birinci fıkrasının (c) bendine ve 20 nci maddesinin birinci fıkrasına tabi değildir. Bu kuruluş, iş gereği kart numarasının ilk 6 ve son 4 hanesi dışındaki bölümlerini saklaması durumunda, herhangi bir kapsam kısıtlamasına gidilmeden ve işlem sayısından bağımsız olarak, PCI DSS ile uyumlu olduğunu, asgari yılda bir kez, standartları PCI SSC tarafından tanımlanmış olan yerinde denetimler ile ispatlar ve uyumluluğuna ilişkin belgeleri anlaşma yapmış olan tüm üye işyeri anlaşması yapan kuruluşlara iletir.

Dış hizmet alımı

MADDE 21 – (1) Üye işyeri, hizmet alacağı dış hizmet sağlayıcı kuruluşun adını, ortaklık yapısını, sahip olduğu sertifika ve belgeleri ve alacağı hizmetin kapsamını, talep etmeleri halinde, üye işyeri anlaşması yaptığı kuruluşlara bildirir.

(2) Üye işyeri, hizmet aldığı dış hizmet sağlayıcı ile aldığı hizmet kapsamında kart hamili bilgisi paylaşması gerekli ise, kart hamili ile gerçekleştirdiği satış sözleşmesinde paylaşım sınırlarını açıkça belirtir. Ödeme işleminin yapıldığı ortama göre, kart hamilinin kanıtlanabilir şekilde yazılı veya elektronik onayını alır.

(3) Üye işyeri, İlkeler Tebliğinin "Bilgi sistemlerine ilişkin destek hizmeti alımı sürecinin yönetimi" başlıklı 8 inci maddesinin birinci fıkrasına, üçüncü fıkrasının (a), (ç), (e) ve (g) bentlerine ve dördüncü fıkrasına ilişkin hükümlere tabidir. Bu maddede geçen "banka" ifadesi üye işyeri; "destek hizmeti" ifadesi dış hizmet; "destek hizmeti kuruluşu" ifadesi dış hizmet sağlayıcı olarak uygulanır.

(4) Bir sisteme veya sürece ilişkin dış hizmet alınması, hizmet alınan hususa ilişkin hizmet alanın sorumluluğunu ortadan kaldırmaz.

ALTINCI BÖLÜM
Dış Hizmet Sağlayıcılar

Dış hizmet sağlayıcılar

MADDE 22 – (1) Dış hizmet sağlayıcı, kart çıkaran veya üye işyeri anlaşması yapan kuruluşlara verdiği hizmet kapsamında sakladığı ve işlediği kart verileri haricinde, şifrelenmiş bile olsa hiçbir biçimde hassas kart verisi saklayamaz, hassas kart verisini kâğıt üzerinde veya elektronik ortamda tutan veya işleyen bir sistem kuramaz. Hassas kart verisinin, kart çıkaran veya üye işyeri anlaşması yapan bir kuruluşa iletilmek üzere, kişilerin kart verilerine müdahalesine müsaade etmeyen bir sistem tarafından güvenli şifreleme ile şifrelenmesi, bu maddenin uygulanmasında verinin işlenmesi kapsamında değerlendirilmez.

(2) Dış hizmet sağlayıcı, kartlı işlemler kapsamında sunduğu dış hizmetlere ilişkin, hizmet alan kart kuruluşu veya üye işyeri ile imzaladığı sözleşmeler ile belirlenmiş olan kapsam dâhilinde, yine bu sözleşmelerde yer verilmiş olan kuruluşlardan hizmet alabilir. Bunun haricinde sunduğu hizmete ilişkin başka bir kuruluştan hizmet almaz. Dış hizmet sağlayıcılara kartlı işlemler ile ilişkili hizmet sunan kuruluşlar, dış hizmet sağlayıcının tabi olduğu hükümlere tabidir.

(3) Dış hizmet sağlayıcı, kart hamiline ilişkin bilgileri, ilgili mevzuatla ve sözleşmelerle tanımlanmış olan amaçlar dışında kullanamaz, yasalarla açıkça yetkili kılınan merciler dışındaki kişilerle paylaşamaz, satamaz, satın alamaz ve takas edemez.

(4) Dış hizmet sağlayıcının, yurtiçinde kurulmuş olması ve kartlı işlemlere yönelik faaliyetlerinin yürütülmesi ve ilgili düzenlemelerde tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan her türlü donanım, yazılım ve veriyi yurt içinde bulundurması zorunludur.

(5) Dış hizmet sağlayıcı, kendi bünyesinde meydana gelen suistimal olaylarının tespitinin akabinde bu hususa ilişkin genel bilgiyi ve gerçekleştirilen incelemeyi müteakip detaylı bilgiyi, kendilerinin veya hizmet verdiği üye işyerlerinin anlaşma yapmış olduğu tüm üye işyeri anlaşması yapan kuruluşlara ve hizmet verdiği kart çıkaran kuruluşlara iletir.

(6) Kart verisi saklayan dış hizmet sağlayıcı, herhangi bir kapsam kısıtlamasına gidilmeden ve işlem sayısından bağımsız olarak, PCI DSS ile uyumlu olduğunu, asgari yılda bir kez, standartları PCI SSC tarafından tanımlanmış olan yerinde denetimler ile ispatlar.

(7) Dış hizmet sağlayıcı, PCI DSS ile uyumluluğuna ilişkin belgeleri, hizmeti alan kuruluşa ve hizmeti alan kuruluş üye işyeri ise üye işyeri ile anlaşma yapmış olan tüm üye işyeri anlaşması yapan kuruluşlara iletir.

YEDİNCİ BÖLÜM
POI'ler, TSM'ler ve ÖKC Üreticileri

POI'ler

MADDE 23 – (1) POI, yeni nesil ÖKC'lerden EFT-POS özelliği olanları ve doğrudan üye işyeri anlaşması yapan kuruluşla bağlantısı olan EFT-POS cihazları kapsar.

(2) POI ve bileşenleri korunaklı sistem özelliği sunar ve herhangi bir tehdide karşı en az iki güvenlik mekanizması barındırır.

(3) İşlem esnasında, hassas kart verisi üye işyeri anlaşması yapan kuruluşa iletilirse hassas kart verisi POI bünyesinde tutulmaz. İşlem esnasında hassas kart verisinin üye işyeri anlaşması yapan kuruluşa iletilmediği durumda, POI'de sadece üye işyeri anlaşması yapan kuruluşun açabileceği bir mekanizma ile şifreli olarak tutulur, uygun olan ilk anda iletim gerçekleştirilir ve hemen sonrasında POI bünyesinden hassas kart verisi silinir. İşlemlerin süre aşımına uğradığı durumlarda da otomatik olarak tüm belleklerden hassas kart verisi temizlenir. Gün sonu veya başka herhangi bir amaçla hassas kart verisi tutulamaz.

(4) PIN ve PIN blokları şifrelenmiş olsa dahi denetim izlerinde veya herhangi bir kayıtta bulundurulmaz. PIN sadece yetkilendirme işlemi için gerekli olan minimum süre boyunca tutulabilir.

(5) POI, işlem esnasında veya sonrasında hassas verileri güvenli şifreleme gerçekleştirmeden cihaz dışına göndermez.

(6) POI bileşenleri arasındaki iletişim güvenli şifreleme ile gerçekleşir.

(7) POI tarafından gönderilen veya POI'ye gönderilen verilerin bütünlüğü ve gizliliği, ağ üzerinde yetkisiz erişime ve değiştirilmeye karşı güvenli şifreleme yöntemleriyle korunur.

(8) Üye işyeri anlaşması yapan kuruluşlarca, güvenlik altyapısının daha kolay tesisi, operasyonel zorlukların en aza indirilmesi, kaynakların verimli kullanımı gibi hususlar yanında, kullanılan POI'lerin teknolojik olanakları, kapasiteleri ve kesintisiz hizmet verilmesi kriterlerine göre, taraflar arasında yapılacak sözleşme hükümleri saklı kalmak kaydıyla, aynı POI üzerinde maksimum sayıda üye işyeri anlaşması yapan kuruluş uygulamasının veya parametrelerinin çalışmasını sağlayacak bir yapı oluşturulur. Bir POI üzerinde birden fazla üye işyeri anlaşması yapan kuruluş uygulaması bulunması halinde, bu kuruluşlara iletilecek verinin şifrelenmesinde kullanılan anahtarların birbirinden farklı olması sağlanır.

(9) POI'deki ödeme uygulamalarının güvenliğinin diğer uygulamalardan etkilenmemesi ve izole şekilde çalışması sağlanır. Hiçbir uygulamanın bir diğerinin verisine yetkisiz erişmemesine yönelik kontroller tesis edilir.

(10) POI'lere sadece ÖKC üreticisi tarafından yetkilendirilen servis müdahale edebilir. Arızalanan POI'lere müdahale edilmeden önce, ÖKC üreticileri veya üye işyeri anlaşması yapan kuruluşlar, üye işyerlerine önceden bilgi vermek ve olay kaydı oluşturmakla yükümlüdür. Yetkili servis personeli, sadece kendi adına atanmış olay kaydı ile ilişkilendirilen POI'ye müdahale edebilir. Yetkili servis kimlik doğrulaması "bildiği", "sahip olduğu" veya "biyometrik bir karakteristiği olan" unsurlardan birbirinden bağımsız iki bileşen ile sağlanır.

(11) Üye işyeri anlaşması yapan kuruluş POI'nin sahibi ise bu kuruluş, POI'ler üzerindeki işletim sistemi, bellenim ve yazılımların yüklenmesine ve güncellenebilmesine ilişkin yazılı ve denetlenebilir bir süreç oluşturur, sürecin işleyişine ve cihazının fonksiyonelitelerine ilişkin yeterli detayda dokümantasyon tutar, yüklenmiş yazılımlarda gizlenmiş, yetkilendirilmemiş veya yazılı olarak kayda alınmamış fonksiyonların cihazda barındırılmadığına ilişkin güvence oluşturacak düzeyde belgelendirme yapar. POI'nin EFT-POS özelliği olan yeni nesil ÖKC olması durumunda bu sorumluluk ÖKC üreticisine, diğer durumlarda ise POI sahibi merci tarafından belirlenecek üye işyeri anlaşması yapan kuruluşa aittir.

(12) Yurt içinde kurulu bir kart çıkaran kuruluş tarafından çıkarılmış bir kart ile yurt içinde gerçekleşen ve temassız olmayan tüm CP işlemlerde, kart hamilinin kimliğinin dinamik kimlik doğrulama ile doğrulanmasının sağlanması için; POI'lere yurt içinde kurulu kart çıkaran kuruluşlara ait BIN bilgileri tanıtılarak, bu BIN değerlerine sahip kartlar için POI'de gerekli kısıtlamalar tanımlanır.

(13) POI, güvenlik ile ilgili herhangi bir işlem veya olaydan sorumlu kullanıcıların tespit edilebilmesi için yeterli denetim izi tutar.

(14) POI'ler için, herhangi bir kapsam kısıtlamasına gidilmeksizin cihazın tamamı kapsanacak şekilde; PCI SSC tarafından yayınlanmış olan ilgili güvenlik prensiplerinin güncel versiyonunun gerekleri kartlı sistem kuruluşlarının tanımlamış oldukları süre içerisinde yerine getirilerek, "PIN Transaction Security (PTS) Point of Interaction (POI)" cihaz onayı alınır.

(15) Kart hamilinden PIN bilgisi istenirken, POI ekranında veya POI'nin PIN girilen bileşeninin ekranında ödemeye ilişkin tutar gösterilir. POI, PIN bilgi istemi gerçekleşmeden önce PIN girilen bileşeninin klavyesi üzerinden girdi kabul etmez.

(16) POI'nin işletim sistemi, sadece amacı doğrultusundaki servislerin ve özelliklerin gerektirdiği servisleri barındırır ve çalıştırır, konfigürasyonu buna göre yapılır.

(17) Üye işyeri anlaşması yapan kuruluşların yazılımlarının veya parametrelerinin güncelleme mekanizması asgari olarak gizlilik, bütünlük ve kaynağın doğrulanması hususlarına ilişkin kontrolleri barındırır. POI, bütünlüğünü, kaynağını ve geçerliliğini güvenli şifreleme yöntemleriyle doğrulamadığı güncellemeleri işleme almadan siler.

(18) Üretim aşamasında veya sahadaki POI'lere üye işyeri anlaşması yapan kuruluşların uygulamalarının ve anahtarlarının güvenli yöntemlerle yüklenmesi sağlanır. Anahtar yükleme işlemleri ve POI bütünlüğünün bozulduğu işlemler, sahada gerçekleştirilmez. Uzaktan ve güvenli biçimde anahtarların yüklendiği mekanizmalar bu kapsamda ele alınmaz.

(19) POI bünyesindeki anahtarlar ve uygulamalar, yetkisiz değiştirilmeye karşı korunaklı bir biçimde saklanır ve kullanılır. Cihazdaki anahtarlar kendileri için tanımlanmış amacın dışında kullanılamaz.

(20) POI, üzerindeki öntanımlı parolanın, üye işyeri tarafından ilk kullanım öncesinde değiştirilmesini zorunlu kılar.

(21) Sanal POS'lar için, bu maddenin 3 üncü, 5 inci, 7 nci, 11 inci, 12 nci, 13 üncü ve 17 nci fıkralarında yer verilmiş olan hükümler, "POI" ve "cihaz" ifadeleri "sanal POS" olarak uygulanır.

TSM'ler

MADDE 24 – (1) Hassas kart verisi ve kart hamili bilgisi, POI'den üye işyeri anlaşması yapan kuruluşa kadar, TSM'nin açamayacağı şekilde güvenli şifrelenmiş olarak iletilir ve TSM bünyesinde hiçbir şekilde saklanmaz. Bu veriler dışında veri tutulması, üye işyeri anlaşması yapan kuruluşlar ile yapılan sözleşmelerle düzenlenir.

(2) ÖKC üreticileri, sundukları hizmete ilişkin tüm bileşenleri kapsayan sızma testini icrai görevi bulunmayan bağımsız ekiplere yılda en az bir defa yaptırır, tespit edilen açıkları ivedilikle giderir, güvenlik alanındaki güncel gelişmeleri ve yeni açıkları takip eder, gerekli yazılım güncellemeleri yapar, gerekli yamaları uygular.

(3) ÖKC üreticileri, verecekleri hizmetlerden doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptırırlar.

(4) TSM, herhangi bir kapsam kısıtlamasına gidilmeden ve işlem sayısından bağımsız olarak, PCI DSS ile uyumlu olduğunu, asgari yılda bir kez, standartları PCI SSC tarafından tanımlanmış olan yerinde denetimler ile ispatlar.

(5) Dördüncü fıkra kapsamında TSM'de yerinde denetim gerçekleştiren kuruluş, denetimlerinde TSM'nin bu Tebliğin hükümlerine uyum durumunun tespit edilmesi amacıyla, karta veya kart hamiline ilişkin veriye erişen veya veriyi saklayan, işleyen veya ileten kişiler, süreçler, yazılımlar ve donanımlar ile bu kapsamda tesis edilen iç kontrolleri de değerlendirir, söz konusu iç kontrollerin etkinliğini, yeterliliğini ve uyumluluğunu denetler.

(6) TSM ile denetimi gerçekleştirecek kuruluşun karşılıklı yükümlülükleri, BSDHY'de yer verilen ilkeler ile uyumlu olacak şekilde taraflar arasında imzalanan sözleşmelerle belirlenir.

(7) TSM, gerçekleştirilen denetim sonucunda oluşturulan raporları ve diğer çıktıları, hizmet verdiği tüm üye işyeri anlaşması yapan kuruluşlar ile paylaşır.

ÖKC üreticileri iş sürekliliği yönetimi

MADDE 25 – (1) ÖKC üreticisi, POI üzerinden sundukları hizmetin sürekliliğini ve kesinti halinde faaliyetlerinin sürdürülebilmesini amaçlayan üst yönetim tarafından onaylanmış iş sürekliliği yönetim süreci tesis eder. Bu kapsamda, iş sürekliliği planı ve planının bir parçası olan bilgi sistemleri süreklilik planı hazırlar.

(2) İş sürekliliği planlamasına yönelik olarak iş etki analizi yapılır ve kurtarma stratejileri belirlenir. Bu kapsamda, iç ve dış bağımlılıklar belirlenir ve meydana gelebilecek bir kesinti durumunda gereken faaliyet düzeyini ortaya koymak üzere operasyonlar önem düzeyi açısından sınıflandırılır. Farklı kesinti senaryolarının faaliyetler üzerinde yaratabileceği muhtemel riskler ve bunların potansiyel etkileri değerlendirilir.

(3) İş sürekliliği yönetimi sürecinde, bilgi sistemleri varlıklarının ve tutulan verilerin önem düzeyleri dikkate alınarak iş etki analizi çerçevesinde kabul edilebilir kesinti süreleri belirlenir ve bu süreler içinde servislerin tekrar erişime açılabilmesini sağlamak amacıyla, alternatifli kurtarma prosedürleri ile yetki ve sorumlukları içeren iletişim prosedürleri geliştirilir. Süreç kapsamında, performans takip teknikleri kullanılır, kapasite planlaması yapılır, işlem hacmi tahminleri doğrultusunda stres testleri gerçekleştirilir, ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif kanallar oluşturulur. Ayrıca, servis dışı bırakma atakları göz önünde bulundurulur ve buna karşı gerekli önlemler alınır.

(4) ÖKC üreticisi tarafından, süreç kapsamında yurtiçinde ikincil merkez tesis edilir, veri ve sistem yedekleri ikincil merkezde kullanıma hazır bulundurulur.

(5) ÖKC üreticisi, bilgi sistemleri sürekliliğini etkileyecek olay ya da değişikliklerden sonra iş sürekliliği planını gözden geçirir ve günceller. Mevcut planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir kez bir günlük operasyonlarının tamamını ikincil merkez üzerinden gerçekleştirecek şekilde testler yapar, test sonuçlarını ve hizmet sürekliliğini etkileyen olayları üst yönetime aktarmak için raporlama süreci işletir.

(6) ÖKC üreticisi, bilgi sistemlerine ilişkin beklenmedik olayları yönetmek ve bunların etkilerini en aza indirmek üzere acil ve beklenmedik durum planı oluşturarak gerekli önlemleri alır, faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci ile beklenmedik olayları erken haber almayı sağlayacak mekanizmaları tesis eder. Acil ve beklenmedik durum planı kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulmayı sağlama, hasarı tespit etme, olayın potansiyel boyutunu ve etkisini gösterme, yetkili yönetim birimine ulaştırılmasını sağlama ve etkilenen müşterileri tespit etme süreçleri ele alınır. Bilgi sistemlerine ilişkin beklenmedik olayların sonradan incelenmesine imkân tanıyacak, yetkili merciler tarafından talep edildiğinde kullanılabilecek nitelikte kayıt ve bilgileri toplayan bir mekanizma oluşturulur.

(7) ÖKC üreticisi, POI üzerinden sundukları hizmete ilişkin üye işyeri anlaşması yapan kuruluşlara sözleşmelerde taahhüt ettiği düzeyde servis sürekliliği sağlar ve bu kuruluşların servis sürekliliğini doğrudan ve anlık olarak takip edebilecekleri altyapı sunar.

(8) ÖKC üreticisi, TSM bilgi sistemleri servislerinin, yılda azami 2 saat kesinti ile hizmet sunmasını temin edecek şekilde, mimari tasarımının ve testlerin yapıldığına dair güvence sunar.

(9) POI üzerinden sunulan hizmette, POI'nin bozulmasından veya başka bir sebepten ötürü 24 saatten fazla kesinti öngörülürse ya da üye işyeri tarafından sorunun ÖKC üreticisine veya yetkili servise iletilmesinden itibaren 24 saat geçmiş ise üye işyeri anlaşması yapan kuruluş, üye işyerine EFT-POS cihazı temin edebilir. Bu durumda, EFT-POS cihazının kullanım süresi yeni nesil ÖKC'nin tamiri için GİB tarafından ÖKC üreticilerine tanınmış süreden daha uzun olamaz ve EFT-POS cihazı bu sürenin aşılmadığını sistemsel olarak kontrol eder. Kesinti giderildiğinde, EFT-POS cihazında gerçekleştirilen tüm işlemler GİB'in beklediği formatta yeni nesil ÖKC cihazına aktarılır.

SEKİZİNCİ BÖLÜM
Çeşitli ve Son Hükümler

Sorumluluklar

MADDE 26 – (1) İlgili mevzuat ve bu Tebliğ ile faaliyetlerin yürütülmesinde kullandığı sistemleri yurtiçinde bulundurmalarına ilişkin zorunluluk bulunmayan kuruluşların, sunucularını yurtdışına taşıması veya yurtdışında kurulu bir kuruluştan hizmet alması, bu Tebliğ ile tanımlanan sorumluluklarını ortadan kaldırmaz.

(2) Kartın manyetik şeridi aracı kılınarak gerçekleşen suistimal ve dolandırıcılıklara ilişkin olarak; kartın manyetik şeridinde hassas kart verisi varsa, kart hamili manyetik şeritte hassas kart verisi bulunmasını talep etmemişse ve kart hamilinin menfaat elde etmek amacıyla kötü niyetli hareket ettiği ispat edilemezse, gerçekleşen işlemlerden dolayı kart hamilinin herhangi bir sorumluluğu bulunmaz.

(3) Dinamik kimlik doğrulama olmayan kimlik doğrulama mekanizması, kart hamilinin işlemi gerçekleştirdiğini ispatlamaya yeterli sayılmaz.

(4) Kart hamilinin bilgisi haricinde gerçekleşen işlemlere ilişkin olarak; kart hamili kartını kaybetmemişse, kart hamilinin kimliğini doğrulamak için dinamik kimlik doğrulama kullanılmamışsa ve kart hamilinin menfaat elde etmek amacıyla kötü niyetli hareket ettiği veya kimlik doğrulama verisini korumada gerekli özeni göstermediği ispat edilemezse, kart hamili sorumlu tutulamaz. Yurtdışında kurulu bir üye işyeri anlaşması yapan kuruluş üzerinden gerçekleşen işlemler, yurtdışında kurulu bir kart çıkaran kuruluş tarafından çıkarılmış bir kart ile gerçekleşen işlemler, ikinci fıkra kapsamındaki işlemler ve çevrim dışı temassız işlemler bu fıkra kapsamı dışındadır.

(5) Kart hamilinin bilgisi haricinde gerçekleşen işlemlerde, kart hamilinin kimliği dinamik kimlik doğrulama ile doğrulanmışsa ve üye işyerinin herhangi bir ihmali, menfaat elde etmek amacıyla kötü niyetli hareket ettiği veya mevzuat uyumsuzluğunun bulunduğu ispat edilemezse, işleme ilişkin üye işyeri sorumlu tutulamaz.

(6) Kart hamilinin işlemi devam ettirmeye, yenilemeye veya tekrarlamaya ilişkin işyerine açık bir beyanı bulunmamasına rağmen kart hamilini borçlandırmaya devam eden işlemlerden dolayı kart hamili sorumlu tutulamaz. Üye işyerinin veya üye işyeri anlaşması yapan kuruluşun yurtdışında kurulu olması bu hükmün uygulanmasında bir değişikliğe yol açmaz. Kart hamili, bu fıkra kapsamındaki itirazını, borcun muaccel olduğu andan itibaren üç ay içerisinde gerçekleştirebilir.

(7) Dış hizmet sağlayıcı, verdiği hizmete ilişkin mevzuatın gereklerini yerine getirmekle yükümlüdür. Bu yükümlülük, üye işyeri anlaşması yapan ve kart çıkaran kuruluşların dolandırıcılık olaylarını izleme ve önlem alma sorumluluklarını ortadan kaldırmaz. Dış hizmet sağlayıcının, mevzuat uyumsuzluğunun bulunmadığının ve işin gerektirdiği özeni gösterdiğini ispatlaması halinde, kart hamilinin bilgisi haricinde gerçekleşen işleme ilişkin herhangi bir yükümlülüğü yoktur.

Muafiyet ve istisnalar

MADDE 27 – (1) Bu Tebliğde yer verilmiş olan kuruluş ve sistemlerden;

a) Kart çıkaran kuruluşlar, bu Tebliğin sadece “Bilgi Sistemlerinin Yönetimi” başlıklı ikinci ve “Kart Çıkaran Kuruluşlar” başlıklı üçüncü bölümlerine ilişkin hükümlerine,

b) Üye işyeri anlaşması yapan kuruluşlar, bu Tebliğin sadece “Bilgi Sistemlerinin Yönetimi” başlıklı ikinci ve “Üye İşyeri Anlaşması Yapan Kuruluşlar” başlıklı dördüncü bölümleri ile “POI’ler” başlıklı 23 üncü maddesine ilişkin hükümlerine,

c) POI’ler ve sanal POS’lar, bu Tebliğin sadece “Bilgi Sistemlerinin Yönetimi” başlıklı ikinci bölümü ile “POI’ler” başlıklı 23 üncü maddesine ilişkin hükümlerine;

ç) ÖKC üreticileri ve TSM’ler bu Tebliğin sadece “Bilgi Sistemlerinin Yönetimi” başlıklı ikinci, “Dış Hizmet Sağlayıcıları” başlıklı altıncı ve “POI’ler, TSM’ler ve ÖKC Üreticileri” başlıklı yedinci bölümlerine ilişkin hükümlerine;

d) Diğer dış hizmet sağlayıcıları, bu Tebliğin sadece “Bilgi Sistemlerinin Yönetimi” başlıklı ikinci ve “Dış Hizmet Sağlayıcıları” başlıklı altıncı bölümlerine ilişkin hükümlerine,

e) Kart verisi saklamayan veya adına kart verisi saklanmayan, sadece POI üzerinden CP ödeme kabul eden ve kart hamili bilgisi saklamayan üye işyerleri, bu Tebliğin sadece “Üye İşyerleri” başlıklı beşinci bölümü ile “İşleme ilişkin verilerin korunması” başlıklı 10 uncu maddesine ilişkin hükümlerine,

f) Diğer üye işyerleri, bu Tebliğin sadece "Bilgi Sistemlerinin Yönetimi" başlıklı ikinci ve "Üye İşyerleri" başlıklı beşinci bölümlerine ilişkin hükümlerine

tabidir.

(2) Bu Tebliğde yer verilmiş olan tüm kuruluş ve sistemler, bu Tebliğin "Çeşitli ve Son Hükümler" başlıklı sekizinci bölümünde yer verilmiş olan hükümlere tabidir.

Diğer Hükümler

MADDE 28 – (1) Bu Tebliğde hüküm bulunmayan hallerde, kartlı işlem altyapısının güvenliğine ve etkinliğine dair kart çıkaran ve üye işyeri anlaşması yapan kuruluşlar bir araya gelerek mutabakat ile karar alabilir. Aldıkları kararları Kuruma iletmelerinden itibaren bir ay içerisinde Kurumun olumsuz görüş bildirmemesi ve etkilediği paydaşlar ile var olan sözleşmelere aykırılık teşkil etmemesi durumunda bu kararlar uygulanır.

(2) Bu Tebliğde yer alan bilgi sistemlerinin yönetimine ilişkin hükümler, bankalar için, İlkeler Tebliğinde belirtilen hükümler aynen geçerli olmak kaydıyla, ilave hükümler olarak değerlendirilir. Dış hizmet alımına ve dış hizmet sağlayıcılara yönelik hükümler, bankalar için, 5/11/2011 tarihli ve 28106 sayılı Resmî Gazete'de yayımlanan "Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik"te ve İlkeler Tebliğinde belirtilen hükümler aynen geçerli olmak kaydıyla, ilave hükümler olarak değerlendirilir.

(3) Bu Tebliğde yer alan bilgi sistemlerinin yönetimine ilişkin hükümler, bilgi alışverişi, takas ve mahsuplaşma kuruluşları için, 4/12/2013 tarihli ve 28841 sayılı Resmî Gazete'de yayımlanan "Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ"de belirtilen hükümler aynen geçerli olmak kaydıyla, ilave hükümler olarak değerlendirilir.

(4) Üye işyerinin elektronik para veya ödeme kuruluşu olması ve iş gereği kart numarasının ilk 6 ve son 4 hanesi dışındaki bölümlerini saklaması durumunda, bu Tebliğin "Bilgi Sistemlerinin Yönetimi" başlıklı ikinci ve "Üye İşyerleri" başlıklı beşinci bölümlerinde yer verilen hükümler, bu kuruluşlar için, 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" ve alt düzenlemelerinde belirtilen hükümler aynen geçerli olmak kaydıyla, ilave hükümler olarak değerlendirilir.

İntibak

GEÇİCİ MADDE 1 – (1) Tebliğ yürürlük tarihinden sonra mevcut çipli kartlar ile gerçekleştirilen ve müşterinin kimliğinin doğrulanmasını gerektiren ödeme, para çekme, para yatırma gibi işlemler için bu Tebliğin 11 inci maddesinin birinci fıkrasında yer verilmiş hükümlere uyulması zorunludur. Ancak halihazırda çip barındırmayan kartlar ile gerçekleştirilen işlemler için bu hüküm 1/1/2017 tarihinden sonra gerçekleştirilecek işlemlerde aranır.

(2) Kart çıkaran kuruluşlar, kart hamillerinin mevcut kartlarının bu Tebliğin 12 nci maddesinin yedinci fıkrasında yer verilen hükümlere uyumluluğunu sağlamak üzere, Tebliğ yürürlük tarihinden itibaren, son bir yıl içerisinde en az bir kez CNP ödemelerde kullanılmış kartların CNP ödemelerde kullanımına, son iki yıl içerisinde en az bir kez yurtdışında kullanılmış kartların da yurtdışında kullanımına ilişkin kart hamili onayı alınmış sayılır. Kart

çıkaran kuruluş, bu kapsama girmeyen kartları CNP ödemelerde ve/veya yurtdışında kullanıma kapatır ve kart hamillerini bilgilendirir.

Yürürlük

MADDE 29 – (1) Bu Tebliğ 1/1/2016 tarihinde yürürlüğe girer.

Yürütme

MADDE 30 – (1) Bu Tebliğ hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.