

# ÖNEMLİ DUYURU

## Mail Order POS İşlemlerinde Dikkat Etmemiz Gereken Noktalar

Ülkemizde yaşanan sahtecilik olaylarından dolayı, POS üzerinden gerçekleştirilen işlemlerde, ancak bunlarla sınırlı olmamak üzere, özellikle aşağıda belirtilen hususlara dikkatiniz çekmek isteriz.



Siz değerli müşterilerimizin, kart hamili ile yüzyüze gelmeksizin gerçekleştirdiği, özellikle mail order işlemlerde;

İlk defa işlem gerçekleştiren yeni müşteriler,

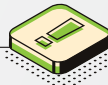
Aynı gün içerisinde acil teslimat isteyen veya doğrudan firmadan teslimat isteyen müşteriler,

Üye işyeri sipariş yoğunluğunda meydana gelen olağandışı hareketler,

Aynı müşteri tarafından kısa süre içerisinde farklı kartlar ile gerçekleştirilen işlemler,

Ret işlem denemeleri sonrasında onay alan bağlantılı işlemler,

Riskli işlemler ve müşteriler olarak değerlendirilmekte ve Uluslararası Kartlı Sistem Kuruluşları'nın belirlediği kurallar çerçevesinde charge back riski yüksek işlem ve müşteriler olarak sınıflandırılmaktadır.



Bu tip müşteri ve işlemlere dikkat etmeniz önem arz etmektedir.

Böyle bir durumla karşılaşmanız halinde alınacak aksiyonlara [www.garantilisler.com.tr](http://www.garantilisler.com.tr) adresinde yer alan Sanal POS ve Mail Order Sahteciliklerinden Korunma Yöntemleri sayfamızdan ulaşabilirsiniz.



Değerli üye işyerimiz,

# CHARGEBACK VE SAHTECİLİĞE KARŞI DİKKAT

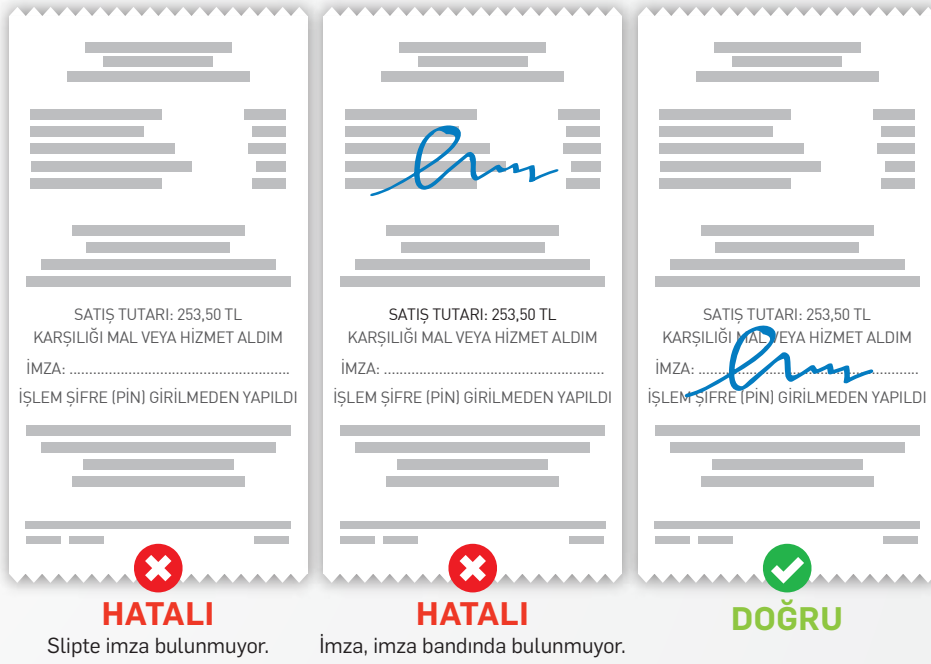
Kartın fiziki olarak kullanılması yoluyla gerçekleştiren işlemlerde aşağıdaki hususlara dikkat etmeniz önem arz etmektedir.

Kartın fiziki olarak kullanılması yoluyla gerçekleştirilen harcamalara kart hamillerinin itirazı söz konusu olabilmekte ve işyerlerimizden işleme/işlemlere ait belgelerin sunulması talep edilebilmektedir.

Bunun temel nedeni, kart hamillerinin "bana ait değil", "işlemi tanımiyorum", "işlemi hatırlamıyorum", "ürün/hizmet teslim almadım" vb. nedenlerle işlemlere itiraz etmeleridir.

Siz değerli müşterilerimizin, kartın fiziki olarak kullanılması yoluyla gerçekleştiren işlemlerde Uluslararası Chargeback kuralları çerçevesinde zarara uğramamak adına aşağıdaki hususlara dikkat etmeniz önem arz etmektedir.

- Şifresiz işlemlerde, slip nüshalarında (üye işyeri nüshası) yer alan imza bandına mutlaka kart hamili imzasının alınması
- Slip (üye işyeri nüshası), fatura ve ürün/hizmet teslim belgesi gibi söz konusu işleme ait tüm belgelerin işlem tarihinden itibaren 10 (on) yıl süreyle muhafaza edilmesi ve Banka tarafından talebi halinde 7 (yedi) iş günü içerisinde paylaşılması
- Şifresiz işlemlerde, gerekli görülen durumlarda kimlik kontrolü yapılması
- Kartın fiziksel güvenlik özelliklerinin kontrol edilmesi (Chip (çip), Hologram, İmza Paneli, Güvenlik Kodu, Hemzemin Rakam, Son Kullanım Tarihi, vb)
- Şifresiz işlemlerde, kartın ön yüzündeki kart numarası ile slip üzerinde yer alan kart numarasının kontrolünün yapılması
- Şifresiz işlemlerde, kartın arkasındaki yer alan imza panelindeki imza ile slipte yer alan imzanın karşılaştırılması



Detaylı bilgi için [garantilisler.com.tr/kart-guvenligi](http://garantilisler.com.tr/kart-guvenligi) web sayfamızı ziyaret edebilirsiniz.

Mail Order ve Sanal POS üzerinden gerçekleştirilen işlemlerde aşağıdaki hususlara dikkat etmeniz önem arz etmektedir.

## Sanal ve Mail Order POS'larda riskli görülen işlemler

- Aynı gün içerisinde acil teslimat isteyen ve ilk defa işlem gerçekleştiren yeni müşteriler,
- Adrese teslimat istemeyip, ürünlerin firmadan farklı kişi/kişiler aracılığı ile alınmasını talep eden müşteriler,
- Teslimatın ısrarla kargo şirketine yapılmasını talep eden müşteriler,
- Teslimat günü sürekli arayarak teslimat süreci ile ilgili bilgi talep eden müşteriler,
- Üye işyeri sipariş yoğunluğunda meydana gelen olağandışı hareketler,
- Kolay nakde çevrilebilir (kuyum, elektronik, telefon) ürün siparişlerinde meydana gelen yoğunlaşmalar,
- Belirli bir ürün ya da hizmet üzerindeki olağandışı yoğunlaşmalar,
- Kayıp çalıntı, sahte kart, CVV ve vade tarihi hatası gibi riskli ret işlem denemelerindeki yoğunlaşmalar,
- Yurtdışı bankalara ait kartlarla gerçekleştirilen yüksek tutarlı işlemler,
- Yukarıda belirtilen riskli ret işlem denemeleri sonrasında onay alan bağlantılı işlemler,
- Aynı müşteri tarafından kısa süre içerisinde farklı kartlar ile gerçekleştirilen işlemler,
- Farklı müşterilere ait siparişlerin tek bir teslimat adresinde yoğunlaştığı durumlar,
- Sanal POS üzerinden verilen siparişlerde aynı IP numarasından farklı müşteriler adına kısa süre içerisinde gerçekleştirilen işlemler

## Sahtecilik işlemlerini tespit etmeye yönelik sorular

- Satışa konu ürünler firmanızdan mı teslim alınmak isteniyor?
- Sipariş veren kişi telefonla mı bağlantıya geçiyor?
- Satış çok kolay mı gerçekleşti? Müşteriniz yeni bir müşteri mi?
- Sipariş verilen mal çok değerli ve nakde dönüştürülebilir mi?
- Sipariş ortalama aldığınız siparişlerin üzerinde mi?
- Aynı müşteri birden fazla kredi kartı ile farklı siparişler mi veriyor?
- Müşteri birden çok mu sipariş veriyor?
- Verilen siparişler diğer satışlarınıza göre olağandışı mı?
- Müşteri başkasına ait bir kredi kartının bilgilerini mi vermek istiyor?
- Verilen adres bilgileri şüpheli mi? Aynı veya benzer adresler daha önce de kullanıldı mı?

## Üye işyerlerimiz tarafından dikkat edilmesi gereken hususlar ve riskli görülen durumlarda alınması gereken aksiyonlar nelerdir?

Sipariş teslimi öncesinde üye işyeri bankasından teyit alınmalıdır.

Sanal POS yönetim ekranları aracılığıyla tutar, adet, BIN, riskli ret kodları detaylı incelenmelidir.

Yeni müşterilere ait işlemler detaylı olarak incelenmeli, sipariş bilgilerinin doğruluğu araştırılmalıdır.

Kredi kartı BIN kontrolü yapılarak yurtdışı bankalara ait kartlarla verilen siparişler daha dikkatli incelenmelidir.

Kargo/kuryelerin bayi adreslerine talep edilen siparişler detaylı olarak incelenmelidir. Sipariş bilgilerinin teyit edilemediği durumlarda gerekirse üye işyeri bankasına bilgi verilmelidir.

Kart hamili tarafından talep edilen iade işlemleri mutlaka işlemin gerçekleştirildiği karta yapılmalıdır.



Burada değinilen hususlar bilgilendirme amaçlı verilmiş olup, tüm bu hususların yerine getirilmesi, işyerinizin karşı karşıya kalabileceği geri ödeme risklerini asgari düzeye indirecektir.

**İşbirliğiniz ve hassasiyetiniz için şimdiden teşekkür ederiz.**

# VERİ GÜVENLİĞİ

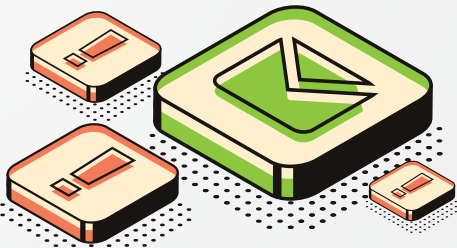
Üye İşyerleri, kart ve kart hamili verilerinin güvenliğini sağlamakla yükümlüdür

Kart verilerinin üye işyerlerinden çalınması, sızması, kopyalanması gibi durumlarda, kart kuruluşları tarafından bir takım **cezai yaptırımlar uygulanmaktadır**.

Üye işyerleri, sabit parasal cezaların yanı sıra, kart hamili bankalarının uğradıkları zararı tazmin etmek zorunda kalmakta, kart kabul yetkileri kısmen ya da tamamen kısıtlanabilmekte ve bunun sonucunda, **büyük ölçüde para ve itibar kaybına uğrayabilmektedirler**.

Müşteri verilerinin güvenliğinin sağlanması, verilerin sızması ve veri çalınması riskinin azaltılması amacıyla uluslararası kartlı ödeme sistemleri kuruluşları tarafından, **Kartlı Ödeme Sektörü Veri Güvenlik Standartları (PCI DSS)** geliştirilmiştir. Bu düzenlemenin temel amacı kart hamili bilgisi (kart numarası, kart hamili ismi, servis kodu, son kullanım tarihi) ve kritik doğrulama bilgisinin (manyetik şerit bilgileri, çip bilgileri, güvenlik kodu ve şifre) güvenliğini sağlamaktır.

**On iki koşuldan oluşan Veri Güvenlik Standartları, temelde bu bilgilerden hangilerinin saklanabileceği ve saklanırken nasıl korunacağına dair kuralları içermektedir:**



## E-POSTA İLE DOLANDIRICILIK

Dünyada ve ülkemizde yurt içi veya yurt dışında faaliyet gösteren ve firmalara yabancı para transferi gerçekleştiren şirketlere yönelik olarak **e-posta ele geçirilmesi** veya **taklit edilmesi** yoluyla gerçekleştirilmeye çalışılan **dolandırıcılık** girişimleriyle sıklıkla karşılaşılmaktadır.

İş ilişkisi içerisinde bulunduğunuz alıcı firma ile **e-posta üzerinden** görüşüyorsanız firmanın e-posta adresi **dolandırıcılar tarafından ele geçirilmiş olabilir**.

Dolandırıcılığa maruz kalmamanız açısından;

**İlk defa transfer** yapacağınız bir hesap numarası size **e-posta üzerinden** gönderiliyorsa **şüpheyle yaklaşmanızı** ve alıcı taraftan **telefon yolu ile IBAN/hesap numarasını ve işlemi teyit etmeniz gerektiğini önemle hatırlatmak isteriz**.

Sahte e-postalar hakkında detaylı bilgi edinmek için [www.garanti.com.tr](http://www.garanti.com.tr)'de yer alan **güvenlik sayfasını** ziyaret edebilirsiniz.