KARTLI İŞLEMLER SAHTECİLİK(FRAUD) ÖNLEME PROSEDÜRÜ

Doküman No:	RY07
Doküman Sahibi:	Risk Yönetim Müdürü
Dokümanı Onaylayan:	Yönetim Kurulu
İlk Yayın Tarihi:	20.11.2025
Gözden Geçirme Tarihi	-
Revizyon No:	-
Revizyon Tarihi:	-
Hazırlayan Bölüm:	Risk Yönetim Müdürlüğü

İÇİNDEKİLER

1. GİRİŞ

Fraud Yönetimi Sistemi, kartlı işlemlerden şüpheli / riskli olanları izlemeye yarayan kural tabanlı bir programdır. Işlemler online olarak yansımaktadır. Her bir case, oluşum nedenine göre belirli bir risk içermektedir.
Senaryolar riskli işlem önceliğine göre Skor puan ile tanımlanır. Skor puanı yüksek kurala takılan işlemler İşlem Havuzu ekranına öncelikli olarak yansır. Case incelenmek için Kart İzleme ekranı kullanılır ve işlemler skor puan sıralamasına göre kullanıcıların ekranına otomatik düşer. Kontrol edilen işlemler için hemen aksiyon alınmalıdır. Maksimum 30 dakika içerisinde işlemler kapatılmalıdır.
Sonuç olarak, Fraud Yönetimi Sistemi tarafından üretilen alarmların hızlı ve doğru bir şekilde aksiyon alınarak kapatılması önemlidir. Burada amaç, doğru aksiyonlar alarak riski etkin bir şekilde yönetmek ve fraud işlem kaçırmamaktır.

1.1. Amaç

Bu dökümanın amacı, Fraud Yönetimi ekranında kartlı ödeme sistemleri üzerinden geçen işlemlerini incelerken, doğru şekilde aksiyon alınmasını sağlamak ve alarm inceleme standardı oluşturmaktadır.

1.2. Kapsam

Bu doküman, Fraud Yönetimi Sistemi –Kart İzleme – İşlem Havuzu ekranındaki her kurala ait işlemlerin inceleme adımlarını içermektedir.

2. FRAUD RİSK YÖNETİMİ

2.1. PAYGUARD – YÖNETİM – SENARYO TANIMI

Senaryo, kurallar bütünüdür. Senaryo bir kuraldan oluşabileceği gibi birden fazla kuraldan da oluşabilir. 3 farklı tipte senaryo tanımı yapılabilmektedir.

Online Senaryo: İşlem onayını etkileyen senaryo tipidir. Girilen senaryo adet ve tutarlarına göre işleme otorizasyon sürecinde ret cevabı verilir.

Offline Senaryo: İlgili işlem için skor üreterek, Kart İzleme Ekranı'nda kullanıcının önüne alarm olarak gelir. Kullanıcı tarafından aksiyon alınmasını sağlayan senaryolardır.

Gizli (Simülasyon) Senaryo: Kullanıcının izlemediği fakat işlemi yapan kişinin bilgilendirilebildiği senaryo tipidir.

3. AKSİYON AKIŞLARI

Şirket tarafından belirlenen senaryolara göre;

Cevap Evet ise;

- ✓ İşlem "Normal" Statü ile kapatılır ve süreç sonlanır.

Cevap Hayır ise;

- ✓ Müşteri aranır.

- ✓ Ulaşıldı- İşlem teyidi alınır.
- ✓ Yükleme yapılan kredi kartı bilgileri talep edilir. Bu konuda gerekli incelemeler tamamlanır.
- ✓ İşlem "Normal" Statü ile kapatılır ve süreç sonlanır.
- ✓ Ulaşılmadı- Kartı Blokeye alınır. Aksiyon kapatılırken gerekli memo kaydı girilir.
- ✓ Kart sahibi kurumun Fraud Ekibi'ne mail ile bilgilendirme yapılır.

4. MÜŞTERİ İLE YAPILAN TELEFON GÖRÜŞME İŞ AKIŞLARI

Müşteri telefonu cevapladığında;

- İyi Günler, (İlgili kurum adı) kart ürününüz için arıyorum. İsmim **** görüşmelerimiz kalite standartları gereği kayıt altına alınmaktadır. Hitap etmek amacıyla isminizi rica edebilir miyim?

(Müşteri ismini vermek istemiyorsa çağrıya devam edilebilir)

- Son dört hanesi **** olan kartınızdan gerçekleştirilen işlem / işlemlerin teyidi için aramıştım. İşlem tarihi/saati/işyeri ismi/işlem tutarı bilginiz dahilinde midir?

Cevap Evet ise;

- Kart yükleme işlemleri kontrol edilir ve yükleme kaynağına göre sorgulama yapılır. Yüklemenin hangi bankaya ait kredi kartı ile yapıldığı, kartın ilk 6 hanesi ve kart sahibinin ad/soyad bilgileri sorulur?

Cevaplar şüpheli ise;

- Müşterinin kartının blokede olduğu ve yükleme yapılan kredi kartına ilişkin teyit süreçleri tamamlandığında kartın kullanıma açılabileceği bilgisi verilir.
- Müşterinin dolandırıcı olduğu net ise kart/kartlar ilgili statüsü kullanıma kapatılır ve ilgili kurumun Fraud Ekibi'ne mail ile bilgi verilir.

Cevaplar şüpheli değilse;

- İşlem teyidine istinaden aksiyon Normal olarak kapatılır ve müşteriye bilgi verilir.

5. KART FRAUD STATÜLERİ

Riskli işlem kontrollerinde yapılan tespitler neticesinde, ilgili kurum ya da diğer kurum/bankalardan gelen Fraud bildirimlerinde aşağıda belirtilen kart statüsü ve kart alt statüsü kullanılmalıdır.

1. Müşteriye ulaşılamaması durumunda;

   T-Geçici Kapalı- TT-Geçici Blokeli

2. Müşterinin kartını kaybettiği/çaldırdığını ilettiği durumlarda;

   S-Çalıntı / L-Kayıp

3. Kart kopyalama vakalarında;
   F-Fraud Sahte Kart- FF-Fraud Sahte Kart

4. Müşterinin kartını kötü niyetli kullandığı durumlarda;
   F-Sahte Kart - FD-Fraud Data

5. Sahte başvuruya konu olan durumlarda
   F-Sahte Kart - MS-Fraud Sahte Müracaat

6. SENARYO GÜNCELLEME

Fraud Yönetimi Sistemi' nde yer alan senaryolar yaşanan dolandırıcılık vakalarına göre anlık olarak güncellenir. Dolandırıcılık amaçlı işlemlere aracı olduğu düşünülen işyerleri için işlem kesici senaryo tanımı yapılır ve otorizasyonda tüm işlemleri reddedilir.