Marmara Üniversitesi Öneri Dergisi • Cilt 16, Sayı 55, Ocak 2021, ISSN 2147-5377, ss. 185-220
DO1: 10.14783/maruoneri.770525

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

HAVAYOLU SEKTÖRÜNDE ÖDEME SİSTEMLERİ YOLUYLA YAPILAN DOLANDIRICILIK İŞLEMLERİNİN SEKTÖRE OLAN ETKİSİNİN DEĞERLENDİRİLMESİ, DENETLENMESİ VE ÖNLENMESİNE YÖNELİK ÖNERİLER

SUGGESTIONS ON ASSESSMENT OF EFFECTS OF FRAUDULENT TRANSACTIONS MADE THROUGH PAYMENT SYSTEMS ON AVIATION SECTOR AS WELL AS INSPECTION AND PREVENTION OF SUCH TRANSACTIONS

Zekeriya DEMİR*

Öz

Havayolu sektörü hem sağladığı istihdam hem de ekonomik büyüklük ve katma değer açısından, dünya ekonomisi için büyük bir öneme sahiptir. IATA'nın verilerine göre, 2018 yılında sektörün cirosu 885 milyar ve sektördeki dolandırıcılık tutarı da yaklaşık 850 milyon Amerikan doları gibi ciddi bir tutara ulaşmıştır. Sektörde bu ciro artışına paralel olarak, kullanılan finansal enstrümanlar ve ödeme sistemleri değişmiş ve bu durum beraberinde yeni dolandırıcılık risklerini de getirmiştir. Çalışmanın odak noktası, artan bu dolandırıcılık risklerine karşı sektörde yapılan çalışmaların incelenmesi ve bu risklerin önlenmesi için öneriler getirilmesidir. Çalışma bu haliyle, havacılık sektöründeki dolandırıcılıkları inceleyen ve alınacak önlemlere yer veren ilk çalışma olup, özgünlüğü buradan kaynaklanmaktadır. Yapılan çalışma sonunda, dijital ekonomideki gelişmelere paralel olarak, satış kanallarında ve ödeme sistemlerinde ortaya çıkan gelişmelerin havayollarına büyük avantajlar sağlamakla beraber, ciddi anlamda güvenlik ve dolandırıcılık risklerini de beraberinde getirmiş olduğu ve bu riskleri önlemeye yönelik işlemlerin önemli oranda manuel olarak yürütülmekte olduğu ve eski kural setlerinin uygulandığı yönündedir.

Anahtar Kelimeler: Dolandırıcılık, Ödeme Yöntemleri, Denetim, Önleme

* THY Anonim Ortaklığı, Muhasebe ve Mali Kontrol Başkanlığı, zdemir55@gmail.com, ORCID: 0000-0001-8390-2031

Makale Gönderim Tarihi: 16.07.2020
Yayına Kabul Tarihi: 23.10.2020

Abstract

The aviation sector is greatly important for the world economy thanks to the employment and the economic magnitude and value-added it provides. According to the IATA data, the sector produced a turnover of 850 billion dollars and the amount of fraud in the sector reached a serious amount of approximately 850 million U.S. dollars in the year 2018. In parallel with this increase in turnover in the sector, the financial instruments and payment systems have changed, and this situation has brought new fraud risks with it. The focus of the study is to examine the work done in the sector against these increasing fraud risks and to make suggestions to prevent these risks. The study, in its current form, is the first study that examines frauds in the aviation sector and includes measures to be taken, and its originality stems from this. At the end of the study, in parallel with the developments in the digital economy, the developments in sales channels and payment systems have brought great advantages to airlines, as well as serious security and fraud risks, and that the transactions to prevent these risks are carried out manually and the old rule sets are applied.

Keywords: Fraud, Payment Methods**,** Audit, Prevention

1. Giriş

Dolandırıcılık sadece bugüne ve belli sektörlere yönelik bir olgu olmayıp, zamana ve zemine göre gelişmekte ve değişmektedir. Yılmaz (2015)'ın da belirttiği üzere, 1920'lerin başında Charles Ponzi'nin, geri gönderim pullarından para kazandığını iddia ederek halkı dolandırmasının yerini, bugün foreks yatırımları, hacmi milyarlarca dolarlara varan sahte tahvil ve sahte hedge fonları, sanal para birimleri, internet üzerinden daha geniş kitlelere yayılan yüksek getirili yatırım programları gibi yöntemler almıştır. Örneğin İngiltere'de, NFA (2013) Annual Fraud Indicator Raporuna göre, 25, ABD'de Federal Trade Commission (2014) Raporuna göre, 30 farklı dolandırıcılık türü tespit edilmiştir. Yılmaz (2015) Türkiye'de, 2010 – 2014 yılları arasında Jandarma bölgesinde meydana gelen dolandırıcılık olaylarını incelemiş ve bu olayların yaklaşık %2'sinin ödeme sistemleri yoluyla işlendiğini tespit etmiştir. Türkiye'de, ödeme sistemleri, 1990'lardan bu tarafa hızlı bir şekilde gelişmektedir. Bu gelişimin ana nedenlerinden biri mevduat hesabındaki paraların istenilen yerden çekilmesine imkân veren banka kartlarının çıkarılması ve e-ticaretin gelişmeye başlamasıdır (Alponat, 2006; Diker & Varol, 2013). Bu gelişme, TÜİK tarafından 2011-2019 yılları için yayınlanan, e-ticaret verilerinden de anlaşılmaktadır. Bu yıllar arasında, satın alınan tatil konaklama işlemleri %7,3'ten %14'8'e, seyahatle ilgili diğer faaliyetler (bilet, araç kiralama vb.) %15,2'den %31,7'ye çıkmıştır. Bu artışa paralel olarak, 2011-2017 yılları arasında, e-ticarette yaşanan sorunlar (dolandırıcılık dâhil) yaklaşık 3 kat artarak, %7,4'ten %21,5'e çıkmıştır. Görüleceği üzere, ödeme sistemleri ve e-ticaretin artışına paralel olarak bu alandaki sorunlar ve yönetilmesi gereken riskler de artmaktadır. Kredi ve banka kartlı işlemlerdeki genel artışa paralel olarak, havayolu sektöründe kullanılan kart sayıları ve işlem hacimleri de, aşağıdaki tablodan da görüleceği üzere yaklaşık üç katına çıkmıştır.

Tablo 1. 2015-2019 Banka ve Kredi Kartı Gelişimi

Yıllar	İşlem Adedi		İşlem Tutarı (Milyon TL)	
	Banka Kartı	Kredi Kartı	Banka Kartı	Kredi Kartı
2015	1.873.880	26.020.029	1.144	9.158
2016	2.341.572	26.170.384	1.367	9.460
2017	3.360.585	26.264.159	2.428	11.888
2018	4.647.738	23.170.586	5.074	15.549
2019	5.830.224	22.791.496	7.673	21.335

Kaynak: BKM, Seçilen Sektöre Göre Aylık Gelişim (Havayolu Sektör Verileri, 03.06.2020)

Dolandırıcılık yukarıda da ifade edildiği üzere, sadece havayolu sektörüne özgü bir olgu olmayıp tüm sektörleri etkilemekte ve ciddi finansal kayıplara neden olmaktadır. ACFE (2020) Hile Raporu'nda, çalışanlar tarafından yapılan hile ve dolandırıcılıkların tutarının 3,6 milyar USD olduğu, işletmelerin yıllık gelirlerinin yaklaşık %5'inin hile ve yolsuzluklar nedeniyle kaybedildiği ve bunun dünya ekonomisine yıllık maliyetinin yaklaşık 4,5 trilyon dolar olduğu tahmin edilmektedir. Havayolu sektörüne yönelik olarak, Cybersource (2018) tarafından yapılan çalışmada, global havayolu sektöründe 2014'te dolandırıcılık şüphesi nedeniyle iptal edilen rezervasyonların oranı %3.4'ten 2018'de %3.8'e ve bu işlemlerden kaynaklı gelir kaybı da, %1'den %1,2'ye çıkmıştır. IATA (2016)'ya göre, havayolu sektöründe sahte işlem nedeniyle yıllık 858 milyon USD tutarında finansal kayıp meydana geldiği tahmin edilmektedir. Kijek (2017)'e göre, perakende ve bankacılıktan sonra sahte işlemler nedeniyle en fazla kayba uğrayan sektör havayolu olup, bu kayıpların, 2020 yılında tüm sektör için 1,5 milyar dolar seviyesine ulaşması öngörülmektedir. Ortalama karlılığın %3'ler civarında olduğu bir sektör için dolandırıcılık yoluyla ortaya çıkan kayıpların mali tablo etkisinin ne kadar önemli olduğu aşikârdır. Çünkü dolandırıcılık yoluyla elde edilemeyen gelirler bir taraftan bilançoda nakit ve nakit benzeri varlıkları azaltırken, diğer taraftan gelir tablosunda da, rezervasyon kayıpları nedeniyle satış gelirlerini azaltarak faaliyet karını etkilemektedir.

Hile ve yolsuzlukların önlenmesi açısından teknolojinin bütün imkânları kullanılmasına ve bu kapsamda her türlü güvenlik önlemleri alınmasına rağmen, usulsüz ve sahte işlemlerin gerçekleştirilmesine ilişkin yöntemler de buna ayak uydurmakta ve değişmektedir. Özellikle dijital ekonomideki gelişmelere paralel olarak, satış kanalları ve ödeme sistemlerinde ortaya çıkan çeşitlilik havayolları ve seyahat acenteleri için getirmiş olduğu çok büyük avantajların yanında ciddi güvenlik ve dolandırıcılık risklerini de beraberinde getirmektedir. Bu nedenle havayollarının bu riskleri yönetebilmek ve dolandırıcılık maliyetlerini minimize edebilmek için, risk önleme ve denetim sistemlerine daha fazla yatırım yapmaları zorunlu hale gelmiştir. Ancak, kurulacak olan risk ve denetim sistemleri için belirlenecek olan güvenlik önlemlerinin hem yolculara iyi bir satın alma deneyimi sağlayacak hem de sahte (fraud) işlemleri etkin bir şekilde tespit edecek şekilde tasarlanması büyük önem taşımaktadır. Aksi takdirde müşteri memnuniyetsizliği nedeniyle oluşacak kayıp, engellenen sahte işlemlerden elde edilen tutardan çok daha yüksek olabilir.

Tüm sektörlerde olduğu gibi, havayolu sektöründe de çok ciddi boyutlarda hileli işlemler oluşmakta ve bu işlemlerden dolayı sektörde milyar dolarlara varan kayıplar oluşmaktadır. Ancak ulaştığı boyutlar açısından bakıldığında, havayolu sektöründe yapılan hile ve yolsuzluklara ilişkin literatürde yeteri kadar çalışma yapılmadığı tespit edilmiş ve bu durum konunun seçiminde etkili olmuştur. Bu yanıyla çalışmanın literatüre ve sektöre önemli bir katkısının olacağı düşünülmektedir. Buradan hareketle, çalışmanın odak noktası, artan dolandırıcılık risklerine karşı sektörde yapılan çalışmaların incelenmesi, sektöre olan etkisi ve bu risklerin önlenmesi için öneriler getirilmesidir. Çalışmanın birinci bölümünde, havayolu sektöründe dolandırıcılıkların önlenmesi konusunda, IATA, ACTA, Europol, Interpol, Visa gibi kurumların yaptıkları çalışmalara yer verilmiştir. İkinci bölümde, ödeme sistemlerinin tanımı yapılmakta ve havayolu sektöründe yaygın olarak kullanılan ödeme sistemlerine yer verilmektedir. Üçüncü bölümde, havayolu sektöründe ödeme sistemleri yoluyla ne tür dolandırıcılıklar yapıldığı ve nasıl yapıldığına ilişkin açıklamalar yapılacak ve örnekler verilecektir. Dördüncü bölümde, havayolu sektöründe ödeme sistemi dolandırıcılıklarının önlenmesine yönelik önerilere yer verilecek ve sonuç bölümünde de, dünyada önemli bir yeri olan ve hızla gelişen sektörde, dolandırıcılık risklerinin yönetilmesi, önlenmesi ve denetlenmesi konusunda ulaşılan sonuçlar paylaşılmıştır.

2. Havayolu Sektöründe Dolandırıcılıkların Önlenmesi Konusunda Yapılan Çalışmalar

Bu konuda çalışan kurumların başında IATA gelmekte olup, çalışmalar, IATA Mali Komitesi (FinCom)'ne bağlı olan, Ödeme Yöntemi Çalışma Grubu (PMWG) tarafından yürütülmektedir. IATA (2016) tarafından yapılan çalışmalar sonucunda, Endüstri Sahteciliği Önleme (IFP) projesi yürürlüğe konmuş ve faaliyet alanları belirlenmiştir. IFP, sahtekarlığı tespit etmek, önlemek ve kayıpların azaltılmasını desteklemek için sektördeki en iyi uygulamaları oluşturmak ve standartları belirlemek yanında eğitim faaliyetleri ve iyi uygulama örneklerinin paylaşımı yoluyla sektöre katkı sunmayı amaçlamaktadır. IATA, ödeme sistemleri dolandırıcılıkları kapsamında, ödeme sistemleri kuruluşları ve bankalarla dolandırıcılık tespiti ve önlenmesi konusunda işbirliğini, önemli bir stratejik hedef olarak belirlemiştir. Projenin ilk aşaması, havayolu şirketlerinin doğrudan satış işlemlerinin CNP (Kart-Mevcut Değil) yönlerine ve sık uçan yolcu programları alanındaki bazı temel faaliyetlere odaklanmıştır. Proje, bir yandan yaygın dolandırıcılıkla mücadele çözümlerinin uygulanmasına, diğer yandan da piyasa özelliklerini dikkate alarak, ödeme tedarik zinciri içindeki iletişim ve işbirliğinin esnek bir şekilde güçlendirilmesine imkân tanıyacaktır.

IATA, dolandırıcılığın önlenmesi döngüsünü dört ana kritere göre belirlemiştir. Bu kriterler; dolandırıcılığın ölçülmesi, önlenmesi, algılanması ve yeniden değerlendirilmesidir. IATA (2016), IFP Projesi ile bir endüstri sahtekarlığı önleme stratejisi oluşturmayı amaçlamakla beraber, projenin önemli zorlukları olduğunun da farkındadır. Bu zorluklar;

- Endüstri kriterlerinin yokluğu,

- Havayolu Eylem Günlerine (DoA) havayollarından eksik katılım,
- Havayolları arasındaki sahtekarlık önleme performansındaki eşitsizlikler,
- Sahteciliği önleme destekli araçlar konusunda endüstri konsensüsünün eksikliği,
- Havayolu endüstrisindeki işlemlerin doğası gereği, uzaktan satışlar, büyük miktarlar, artan mobil dolandırıcılıklar olarak belirtilebilir.

IATA, IFP Projesi yanında, IATA Perseuss (2020) platformunu oluşturmuş ve bu platform üzerinden, ticari ve ödeme sektöründeki paydaşlar arasında topluluk temelli paylaşım yoluyla sektörler arası dolandırıcılık verilerine gerçek zamanlı erişim sağlamaktadır. Tüm sektör verilerinin paylaşılmasındaki amaç, sahtekarların faaliyetlerini bir sektör veya bölgeyle sınırlamadıkları gerçeğine dayanmaktadır. Yapılan dolandırıcılık işlemleri analiz edildiğinde, ortalama %35'lik kısmının birbiri ile çakıştığı tespit edilmiştir. Bu sistemle, kullanıcılar, doğrudan veya ödeme servis sağlayıcıları aracılığıyla entegrasyon sağlayarak, Perseuss veri tabanında dolandırıcılık çakışmasını gerçek zamanlı olarak kontrol edebilmektedirler. Bu veri tabanı sayesinde, havayolları artan data büyüklüğü nedeniyle manuel kontrolün neredeyse imkansız hale geldiği bir yükten kurtulmuş ve dolandırıcılık maliyetlerini azaltmış olurlar.

Kanada Seyahat Acenteleri Birliği (ACTA)'de, sektördeki dolandırıcılıkları önlemek amacıyla, Kanada Seyahat Dolandırıcılığını Önleme Grubu (CTFPG)'nu oluşturmuş ve IATA ile bu dolandırıcılık önleme girişiminde çözüm ortağı olmuştur. CTFPG'nin (2016) amacı, gelir kayıplarını önlemek için ortak çözümler geliştirmek ve en iyi uygulamaları geliştirmek üzere sektör temsilcilerini bir araya getirmektir. Bu amaçla 2016 yılında Montreal'de yapılan toplantıda, ters ibrazlarla (chargeback) nasıl başa çıkılacağı, Kanada seyahat endüstrisinde dolandırıcılığın boyutları, türleri, verilerin paylaşımı ve sahtekarlık yönetim araçları gibi konular tartışılmıştır.

Havayolu sektöründeki ödeme sistemleri yoluyla yapılan dolandırıcılık işlemlerinin, işin finansal boyutunun yanında ciddi kriminal sonuçları da olabilmektedir. Dolandırıcılar, yasa dışı yollarla ele geçirdikleri kredi kartı, banka kartı, kimlik bilgileri, şifreler vb. ile yasadışı göç, insan kaçakçılığı, uyuşturucu kaçakçılığı gibi suçların işlenmesine doğrudan veya dolaylı olarak imkân vermektedirler. İşin bu kriminal boyutu nedeniyle, bilet sahtekarlığıyla kolaylaştırılan çevrimiçi dolandırıcılık konusunda çalışan kurumlardan biri de Europol'dur. Europol (2016, 2017) tarafından, Beşinci ve Altıncı Küresel Havaalanı Eylem Günleri (GAAD) kapsamında yapılan operasyonlarda, 2016'da 193, 2017'de 153, 2016 UEFA Kupası maçlarında yapılan operasyonlarda da 140 kişi yakalanmış ve gözaltına alınmıştır. Europol Müdürü Rob Wainwright, yapılan operasyonla, hileli olarak alınan biletleri kullanarak seyahat etmeye çalışan suçluların sektör ve kolluk kuvvetlerinin işbirliği ile yakalandığını ifade etmiştir. Yapılan inceleme ve soruşturmada bu kişilerin, çalınan, ele geçirilen veya sahte kredi kartı bilgileriyle satın alınan uçak biletlerini kullanarak uçtuğu anlaşılmıştır. IATA'nın koordinasyonunda yürütülen GAAD ile uçak bileti sahtekarlığı ve seyahat değer zinciri paydaşları arasında etkin bir işbirliği yanında, sahtekârların havayolu işletmeleri ve tüketiciler için seyahat maliyetini artıran

yasadışı faaliyetlerinin önlenmesi amaçlanmaktadır. Europol'e göre, bu dolandırıcılıklar sürekli olarak artmakta olup, sadece uçak bilet alımları değil, fiziksel mal alımları, araç kiralama ve güvenliği ihlal edilmiş kartlarla konaklama satın alımları da AB genelinde önemli bir artış göstermektedir. Ancak, en çok etkilenenler arasında havayolu şirketleri gelmektedir.

Europol'ün yanında, Interpol de bu tür yolsuzluk ve dolandırıcılıklarla ilgili çalışmalar ve operasyonlar yapmaktadır. Interpol (2019)'ünde katıldığı bir operasyonda 79 kişi yakalanmıştır. Interpol Organize ve Gelişen Suç Direktörü Paul Stanfield, para ve hızlı karların organize suçlar için kilit öneme haiz olduğunu ve bu alanda başarılı olabilmek için, uluslararası işbirliği ile güvenli ve gerçek zamanlı bilgi paylaşımının önemli olduğunu belirtmektedir. Interpol uçak bileti sahtekarlığı ile ilgili fiili operasyonlar yanında, kendi internet sitesinde, bu sistemin nasıl işlediği, hangi durumlarda dolandırıcılıktan şüphelenilmesi gerektiği ve dolandırıcılık kurbanı olmamak için güvenli alışverişe ilişkin bilgilendirmelerde yapmaktadır.

Ödeme sistemleri ile yapılan dolandırıcılıkları önlemeye çalışan kurumlar arasında kredi kartı kuruluşlarını da saymak gerekir. Bu kuruluşlardan biri olan Visa (2014) dolandırıcılıkları önlemek amacıyla; kartı düzenleyen kuruluşu, kart sahipleri tarafından izinsiz olarak gerçekleştiği iddia edilen her işlemi araştırmakla yükümlü tutmaktadır. Yapılan incelemede, gerçekten sahtekarlık ve dolandırıcılık tespit edilmesi halinde, bu sahtekarlıkla ilgili bütün ayrıntıları TC40 üzerinden Visa'ya göndermelerini zorunlu tutmaktadır. Visa, bu TC40 mesajlarını harmanlamakta, doğrulamakta ve minimum standartları karşılamayanları reddetmektedir. Daha sonra toplanan bu TC40 datalarını;

- Yeni sistem ve altyapı yatırımlarını desteklemek
- İş modellerindeki değişiklikleri desteklemek
- Uygun uyum programlarını sürdürmek ve işletmek
- Visa Avrupa Kurulunu sahtekarlık performansı hakkında güncellemek
- Visa Europe için öncelikleri belirlemek
- Ödeme sistemindeki tüm taraflar için dolandırıcılığı minimize etmek
- Kart sahiplerine ve işletmelere en iyi işlem onay oranları sağlamak
- Tüm tarafların maruz kaldığı dolandırıcılık riski yönetimi maliyetlerini minimize etmek
- Dolandırıcılık kalıplarını belirlemekte kullanarak kredi kartı dolandırıcılıklarını minimize etmek.

Visa Europe'ta dolandırıcılık temel bir iş ölçütü olarak kullanılmakta olup, Eylül 2013 itibariyle, genel dolandırıcılık oranı 4,5 baz puan yani toplam satışların %0,045'ine veya harcanan her 100 Euro'da 0,045 Euro'dur.

3. Ödeme Sistemleri ve Havayolu Sektöründe Kullanılan Ödeme Sistemleri

3.1. Ödeme Sistemleri

Merkez Bankası (2014) ödeme sistemlerini şu şekilde tanımlamaktadır: Ödeme sistemi, ekonomik birimler arasında mal ve hizmetlerin değişimini kolaylaştıran araçları, yasal düzenleme ve standartları, kurumsal ve örgütsel çatıyı, işletim süreçlerini ve haberleşme ağını kapsamaktadır. Genel kabul görmüş tanıma göre, üç veya daha fazla katılımcı arasındaki transfer emirlerinden kaynaklanan fon veya menkul kıymet aktarımlarının gerçekleştirilmesini sağlamak amacıyla yapılan takas ya da mutabakat işlemleri için gerekli altyapıyı sunan ve ortak kuralları olan yapı "ödeme sistemi" olarak adlandırılmaktadır.

Havayollarının, hem pazardan daha iyi bir pay almaları hem de gittikçe artan ödeme sistemi dolandırıcılık risklerinden korunmaları için (pazarda yaygın ve güvenlik riski düşük) uygun ödeme sistemi kullanmaları önemli bir gereklilik olarak ortaya çıkmaktadır. Aşağıda, havayolu sektöründe genel olarak kabul edilen ödeme sistemleri hakkında bilgi verilmektedir.

3.2. Havayolu Sektöründe Kullanılan Ödeme Sistemleri

Havayolu sektöründe müşteriye doğru satış kanalından ulaşmak ne kadar önemli ise doğru ödeme sistemi alternatiflerinin sunulması da bir o kadar önemlidir. Cybersource Raporu'na (2018) göre havayolu sektöründe kullanılan satış kanalları, %31 ile havayolu web siteleri, %27 ile seyahat acenteleri, tur operatörleri ve konsolidatörler, %19 Online seyahat acenteleri (OTA), %9 havayolu çağrı merkezleri, %7 mobil ve %7 havaalanları bilet satış noktaları ve kiosklar şeklindedir. Bu kanallarda kabul edilen ödeme yöntemlerine baktığımızda %99 gibi çok yüksek bir oranla dünya çapındaki kredi ve banka kartları, %58'i Paypal ve diğer elektronik cüzdanlar ve bunları sırasıyla, UATP, banka havaleleri, ülke ve bölge bazlı kredi kartları, teslimde nakit, cep telefonu ödemesi, Elektronik çek, ACH veya otomatik ödeme, hediye kartları, Western Union olarak sıralanmaktadır. Burada dikkat çekici bir şekilde, PayPal ve diğer elektronik cüzdanlar üzerinden yapılan ödemelerin kabulü, 2014 yılında %32 iken 2018 yılına gelindiğinde yaklaşık iki katına %62'ye çıkmıştır. Bu durum alternatif ödeme yöntemlerinin hızla artan önemini göstermektedir. Benzer şekilde, Orta Doğu ve Asya Pasifik'teki havayollarında da, Alipay ve WeChat Pay kullanımı önemli ölçüde artmaktadır. Bu artışı destekleyen unsurların başında güvenlik gelmekte olup, kredi ve banka kartlarındaki dolandırıcılık riski ile mukayese edildiğinde bu kartlardaki dolandırıcılık oranları çok düşük kalmaktadır. Örneğin, banka ve kredi kartlarında dolandırıcılık oranı ortalama %27, ülke ve bölge bazlı kartlarda %7, cep telefonu ödemelerinde %5 iken bu kartlarda %3 düzeyindedir. Bu nedenle, kredi ve banka kartına göre neredeyse dokuz kat daha düşük dolandırıcılık riski, bu kartları daha güvenli seçenekler arasına yerleştirmekte ve hızla gelişmelerine neden olmaktadır.

Sonuç olarak, alternatif ödeme yöntemlerinin yükselişi yeni fırsatlar sunmakla beraber, aynı zamanda havayolları için yeni riskler de oluşturabilir. Çünkü zamanla artan kullanıma bağlı olarak bu yöntemler, dolandırıcıların dikkatini çekecek ve bu alana yönelmelerine neden olacaktır.

3.2.1. Kartlı Ödeme Sistemleri

Özcan (2016)'a göre, nakit dışında pek çok noktada kabul gören ve tercih edilen ödeme yöntemlerinin başında gelmekte olan kartlı ödeme yöntemleri, kredi kartı, banka kartı ve ön ödemeli kart olarak belirtilebilir. Bu ödeme yöntemleri, bir kart ağına (Visa, MasterCard, AMEX vb.) bağlantılı olarak, yetkili finansal kuruluşlar tarafından çıkartılan, kullanıcısına bir limit belirlemek veya mevcut banka hesabındaki bakiyeye dayalı olarak, ödeme yapmasına imkan tanıyan sistemlerdir. Yalnızca yerel finansal altyapıya bağlanmak suretiyle, sadece o ülke içerisinde kabul edilen kartlı ödeme yöntemleri de mevcuttur. Genel olarak, havayolları ve acenteler, uluslararası geçerliliği olan kredi kartları ve banka kartlarını kabul etmektedirler. Bunun yanında havayolları uçuş ağlarının yaygınlığına ve ödeme yönteminin ilgili pazardaki kullanım oranlarına bağlı olarak yerel kart tiplerini de (Örn. Rusya pazarında MIR kart, Türkiye'de TROY) kabul etmektedirler.

3.2.2. Elektronik Cüzdan (e-Wallet) Sistemleri

Her ne kadar arka planında bir kartlı ödeme yöntemi veya banka hesabı çalışıyor olsa da, e-cüzdanlar, özellikle mobil satış kanallarında kullanım kolaylığı ile öne çıkmaktadır. Özellikle e-ticaret işlemlerinde fazlasıyla karşılaşılan, kart bilgilerinin ele geçirilmesi gibi güvenlik riskleri nedeniyle tercih edilmektedir. Buna ilave olarak, tek tıkla alışveriş imkanı sunması, kart bilgilerinin sürekli girilmesinin gerekmemesi ve başarılı işlem oranları gibi kullanım kolaylıkları da, bu yöntemin tercih edilmesini yaygınlaştırmaktadır. PSM (2014)'e göre, ülkemizde BKM tarafından 2012 yılında kullanıma sunulan e-cüzdan uygulaması BKM Ekspress, e-cüzdan uygulamalarının başarılı örneklerinden biri olarak gösterilebilir. Yalçın (2018)' a göre, Google Pay, Apple Pay, PayPal, Square Cash, Facebook Messenger, Skril, Jaxx, Alipay, LevelUp, Qkr, Zelle ve Venmo gibi elektronik cüzdan uygulamaları uluslararası alanda ön plana çıkmakta ve hızlı bir gelişim göstermektedir. E-cüzdan işlem hacimlerinin, 2020 yılında yaklaşık 410,5 milyar Amerikan dolarına ulaşması beklenmektedir. Havayolları, kullanım kolaylıkları ve mobil işlemlerdeki artışa bağlı olarak, hem yerel hem de uluslararası e-cüzdan uygulamalarını farklı satış kanallarında kabul etmektedirler. E-Cüzdanların bir diğer özelliği de, dijital olarak saklanması mümkün olan tüm ödeme yöntemlerini kaydederek, gerekli durumlarda kullanılmasına imkan tanımasıdır. Bu sayede kullanıcı, e-cüzdanında kredi kartlarını, seyahat millerini ya da hediye kartlarını saklayarak, gerekli durumlarda tek hesap üzerinden erişebilmektedir. Bu özellikleri nedeniyle, kullanıcı deneyimine de büyük katkı sağlamaktadır.

Sorrells (2019, 3 Haziran)'e göre, internetin gelişimi, ardından 1994'te Amazon, 1995'te eBay ve kısa bir süre sonra Travelocity ve Expedia gibi çevrimiçi seyahat markalarının doğması, dijital ödeme yöntemlerine olan ihtiyacı teşvik etmiştir. Bunlardan birincisi olan ve 1999'da başlatılan PayPal, bugün dünyanın dört bir yanındaki tüketicilere, ürün ve hizmetler için çevrimiçi ödeme yapmasına

imkan vermektedir. World Payments Report (2019)'a göre, e-cüzdan işlemlerindeki büyüme, bir önceki yıla göre %12'ye ve toplam gayrı nakdi işlem hacmi de 539 milyar dolara ulaşarak son yirmi yılın en yüksek büyüme oranına ulaşmıştır. Bölgesel düzeydeki artışlar çok daha çarpıcı olup, Asya'da %32, Orta Avrupa, Orta Doğu ve Afrika'da %19'dur. Bu artışın dünya genelinde 2022'ye kadar %14 oranında bileşik büyüme hızında artması ve gelişmekte olan pazarlarda ise %23,5 oranında artarak 1.045 milyar dolara ulaşması beklenmektedir.

Worldpay Global Paymets Report (2019)'a göre, 2022 yılına kadar tüm küresel e-ticaret ödemelerinin %47'sinin e-cüzdanlarla gerçekleşeceği ve bu alanda %17 paya sahip kredi kartlarının yaklaşık üç katı bir büyüklüğe ulaşacağı tahmin edilmektedir. Önümüzdeki birkaç yıldaki büyümenin, büyük bir kısmının Çin ve Kuzey Amerika'da olması beklenmektedir.

Bailey (2019)'e göre, günümüzde yolcular, havayollarının veya havayolu bileti satışı yapan aracıların tüm kanallarda kendi ihtiyaçlarına yönelik ödeme sistemlerini sunmalarını beklemektedir. Tercih edilen ödeme yönteminin müşteriler nezdindeki önemi büyük olup, uygun ödeme yöntemi sunulamamasından kaynaklanan satış kayıplarının %15-20 arasında olduğu tahmin edilmektedir. Bu durumun farkında olan havayolları tüm satış kanallarında (satış ofisleri, mobil uygulama ve internet siteleri, çağrı merkezi ve acenteler) en uygun ödeme yöntemini, en doğru pazarda sunmaya çalışmaktadır. Örneğin, Soutwest Airlines bu amaçla, yolcuların ihtiyaç duyduklarını hızlı bir şekilde satın almalarını kolaylaştırmak için Apple Pay ile anlaşmıştır.

3.2.3. Banka Transferi

Güvenlik veya farklı nedenlerle kartlı ödeme yöntemlerini kullanmak istemeyen müşterilerin en çok başvurduğu alternatiflerden biri banka transferleridir. Son yıllarda yaşanan (Open Banking uygulamaları gibi) gelişmeler sayesinde, kullanıcı dostu hale de gelmiş olan bu yöntem, Avrupa kıtası başta olmak üzere, pek çok pazarda havayolları tarafından kabul edilmektedir. Worldpay Global Payment Report (2020)'a göre, açık bankacılık ve AB'nin İkinci Ödeme Hizmetleri Direktifi (PSD2) gibi düzenleyici girişimler, daha fazla ödeme yeniliğinin kapılarını aralamaya yardımcı olmakta ve müşterilerin hesaplarından üçüncü taraflara ödeme yapmalarını kolaylaştırmaktadır. Ayrıca bu yöntemle, hesaptan hesaba ödemeler, ödeme kabul maliyetini azaltarak işletmelere ek maliyet tasarrufu avantajları da sağlamaktadır. Banka transfer işlemlerinin tüm ödeme sistemleri içindeki payı 2019 yılında %9 olup, 2023'te ise %9,3 olması beklenmektedir. Örneğin Kuzey Amerika'da %5,9'dan %6,3'e, Latin Amerika'da %10,9'dan %8,9'a ve EMEA Bölgesinde ise, %16,3'ten %20,4'e çıkması beklenmektedir. Özetle, tüketiciler, daha basit ve güvenlikle desteklenen ödeme seçeneklerini talep etmektedirler. Havayolları, ödeme sistemleri konusunda değişen bu tüketici davranışlarını dikkate alarak, kendi sistemlerini bu tür banka transfer sistemleri ile uyumlu hale getirmelidirler. Çünkü banka havalelerinin, büyük ölçüde PSD2 girişiminin, inovasyon ve rekabeti teşvik etmesi, tüketiciye sunmuş olduğu kullanım kolaylığı gibi faktörler nedeniyle, önümüzdeki beş yıl içinde e-ticaret harcamalarından daha fazla pay alması beklenmektedir.

Ülkemizde de internet bankacılığı oldukça yaygın bir kullanım alanı bulmakla beraber, internet üzerinden artan bankacılık işlemleri beraberinde ciddi bir güvenlik sorunu da doğurmaktadır. Çünkü yapılan bu işlemler sanal ortamlarda üçüncü kişiler tarafından takip edilip ele geçirilebilmektedir. Bu riski yönetebilmek için, bankalar tarafından siber güvenlik alanında çok önemli mesafeler alınmış olmasına rağmen sürekli büyüyen işlem hacimleri nedeniyle maalesef internet bankacılığı riskleri istenilen ölçüde azaltılamamıştır (Yeşilyurt, 2015; Ünlü, 2018).

3.2.4. Diğer Alternatif Ödeme Sistemleri

Mayadiya (2020)'ya göre, teknolojinin ilerlemesi ile hem lokal hem global pazarlarda, kullanıcılara farklı ödeme alternatifleri de sunulmaya başlanmıştır. Bunlar arasında bir mobil ödeme yöntemi olan M-PESA gibi Afrika pazarına özel olanlar olduğu gibi, Uplift ve Klarna gibi, daha geniş pazarlarda, gelir düzeyi ortalama ve altı olan tüketicilerin, ödemelerini erteleyerek ve taksitli olarak yapabilmesine imkan tanıyan yeni ödeme sistemleri de ortaya çıkmıştır. Çoğunlukla güvenlik açısından bir kullanıcı hesabına bağlanmak suretiyle çalışan uygulamalar olduğundan, teoride klasik kredi kartı işlemlerinden daha güvenli oldukları kabul edilmektedir. Bu ödeme yöntemlerinin, sundukları hizmet ve faydanın yanı sıra, mobil kanallardaki kullanım kolaylıkları nedeniyle ilerleyen dönemlerde daha fazla tercih edilerek, pazar paylarını artırmaları da beklenmektedir.

Bu yöntemler aslında seyahat harcamalarına farklı alternatifler sunarak, seyahat etme imkanı olmayan insanlara seyahat imkanı sunmaktadırlar. Sorrells (2019, 3 Haziran)'e göre, 2017 yılında kurulan Uplift, müşterilerine seyahat için taksit ödemeleri sunan bir şirkettir. Kayak, United Vacations, American Airlines ve Universal Orlando Resort, UATP dahil olmak üzere birçok markayla yaptığı ortaklıklarla, müşterilerine anında rezervasyon yapmalarını sağlarken, harcamalarını erteleyerek her ay sabit taksitlerle ödemelerine imkan vermektedir. Sistem müşterilerin harcamalarını riske göre fiyatlamakta ve %4,35 ile %35,99 arasında değişen faiz oranları uygulamaktadır.

3.2.5. Mil, Hediye Kartları (Gift Cards) & Seyahat Çekleri (Voucher)

Sık uçan yolcu programları havayolu sektöründe önemli bir yere sahiptir. John (2019)'a göre, dünyada yaklaşık 220 tane Sık Uçuş Programı (FFP) olduğu bilinmekte ve bu sayı büyümeye devam etmektedir. Sistemin ilk çıkışı, United Airlines'ın 1950'lerde müşterilerini takip etmesine dayanmakta olup, ilk sık uçan yolcu programı ise 1972'de ABD merkezli United için 'Western Direct Marketing' adlı bir şirket tarafından oluşturulmuştur. Ancak, yolcuları 'ödüllendirmek' için mil takibini kullanan ilk sık uçan yolcu programı 1979 yılında Texas International Airlines tarafından başlatılmıştır.

Havayollarının genellikle kendi altyapıları üzerinden sundukları bu yöntemler, yolcuların doğrudan havayolundan aldıkları hizmetlerin ödemesinin yanı sıra, diğer yöntemler ile birleştirerek kullanabilecekleri birer yan ödeme yöntemi olarak da görülebilir. Seyahat milleri, genellikle bir kullanıcı hesabına (account number) bağlı olmakla birlikte, havayollarının çeşitli finansal kuruluşlarla

anlaşarak kredi kartına bağlı olacak şekilde (Co-branded Cards) sundukları uygulamalar da mevcuttur. Sistem, yolcunun havayollarının sık uçan yolcu programına (Frequent Flyer Program) üyeliği ile başlamakta ve yapılan uçuşlar veya kartın kullanıldığı anlaşmalı firmalardan kazanılan seyahat millerinin, belirli bir hesap numarasında birikmesi ile ileride yapılacak olan harcamalarda kullanılmasına dayanmaktadır. Artuğer (2011)'e göre Türkiye'de ilk defa uygulanan mil programı THY'nin Miles programı olup, bunu saha sonra, Atlasjet'in Jetmil'i, Pegasus'un Pegasus Kart'ı izlemiştir. Bunun yanında bankaların çıkarmış olduğu kartlarda elde edilen puanlarla uçak bileti alma imkanı ortaya çıkmıştır. Bunlara örnek olarak, İş Bankası'nın Maximiles, Akbank'ın Wings, Denizbank'ın Miles More ve Garanti Bankasının Miles&Smiles kartı verilebilir.

Hediye kartları, bireysel veya kurumsal olarak doğrudan havayolları internet siteleri ya da havayollarının anlaşmalı olduğu dağıtım kanallarından temin edilebilecek, genellikle tek kullanımlık, içerisinde belirli tutarda bakiye yüklü ödeme yöntemleridir. Üzerinde kullanıcıya ilişkin bir bilgi bulunmayan bu kartların güvenlik açısından tek koruyucu tarafı, kartın üzerinde yer alan bir PIN numarasının satın alındıktan sonra görülebilmesidir.

Seyahat çekleri, çoğunlukla müşteri memnuniyeti amacıyla yolculara sunulan ve bir sonraki seyahatlerinde bilet ya da ek hizmetler (business sınıf upgrade, özel yolcu salonu (business lounge) erişimi, otel ya da yemek harcaması vb.) için kullanabileceği bir ödeme yöntemidir. Örneğin THY, pandemi dolayısı ile uçamayan ya da uçmak istemeyen yolcularına seyahat çeki imkanı sunarak ileride bu seyahat çeki ile uçma imkanı getirmiştir. (Air Türk Haber,2020). Seyahat çekinde amaç bir satıştan ziyade, uçuş aksaklığı gibi müşteri memnuniyetini etkileyen durumların karşısında bir tazminat bedeli olarak yolculara sunulmaktadır.

Bu ödeme yöntemlerinin kullanılmasında diğer yöntemlere göre belirli kısıtlar bulunmaktadır. Bu nedenle kullanımdan önce iyi bir pazar ve satış kanalı araştırması yapılmalıdır. Aksi takdirde istenilen sonucu almak mümkün olmayabilir. Örneğin bu yöntemlerin kabulünde mobil kanallar kullanılacaksa, ödeme sayfalarının oldukça kullanışlı ve mümkün olduğu kadar tek işlemle ödeme imkanı sunması önemlidir. Bir diğer önemli konu da, satış sonrası süreçlerin, tüm kanalları içerecek şekilde değerlendirilmesi ve organize edilmesidir. Accelya (2019)'ya göre önemli olan bu ödeme yöntemlerinin hangisinin kullanılacağından (Multi-Channel, Omni-Channel) ziyade, müşterinin ödeme sürecinde yaşayacağı deneyimin standart hale getirilmesidir. Bu standardizasyonun sağlanması sürecin sağlıklı yürümesi açısından önemli bir katkı sağlayacaktır.

Yukarıda da ifade edildiği üzere, bu ürünlerin gelir artırıcı etkisinden yararlanabilmek için internet ve mobil gibi direkt satış kanallarında, insanların işlemden vazgeçmeleri olarak tanımlayabileceğimiz "sepet terk oranı" (cart abandonment)'nın minimize edilmesi gerekir. Smith (2014)'e göre, müşterilere tercih edilen uygun ödeme yönteminin sunulmaması durumunda sepet terk oranı %25 gibi çok yüksek bir orana kadar çıkabilmektedir. Bu nedenle, son derece düşük kar marjları ile çalışan havayolu sektöründe, hem gelir kayıplarını azaltmak hem de doğru ödeme yönteminin minimum

maliyet ile en uygun pazarlarda sunulması büyük bir önem arz etmektedir. Aksi takdirde istenilen fayda-maliyet oranını yakalamak mümkün olmayabilir

Yolculara sunulacak olan ödeme yöntemlerinin seçilmesi sonrası, her bir ödeme yönteminin sahtecilik açısından risk değerlendirmesinin yapılması, değerlendirme sonrası kritik performans göstergeleri (KPI) ile süreç analizlerinin netleştirilerek sorumluluk alanları belirlenmelidir. Elizabeth (2018)'e göre, bu KPI'lar; sipariş onay oranları, sipariş düşüş oranları, ters ibraz oranları, manuel inceleme oranları, otomatik düşüş oranları, yanlış düşüş oranları, analiz başına maliyet şeklinde olabilir. Bu KPI'lar havayolunun kendi belirleyeceği periyotlarda analiz edilmeli ve hem sektör hem de rakip havayolları ile karşılaştırılarak gerekli aksiyonlar alınmalıdır. Bu sayede hem sahte işlemler engellenebilir hem de olası gelir kayıplarının önüne geçilebilir.

4. Havayolu Sektöründe Ödeme Sistemleri Dolandırıcılığı

Birçok sektörde olduğu gibi havayolu sektöründe de kullanılan ödeme sistemlerinin sayısı ve hacmi ile bağlantılı olarak dolandırıcılıklar artmış ve artmaya devam etmektedir. Ayrıca gelişen teknolojiler ve mobil uygulamalar insanlara istedikleri yerden rezervasyon yapma imkanı getirmiş olmakla birlikte, dolandırıcılık riskine daha fazla maruz kalmayı da beraberinde getirmiştir. Elizabeth (2018)'e göre, 2021 yılına gelindiğinde uçak biletlerini doğrudan alan ya da rezerve eden yolcuların oranı tüm çevrimiçi biletlerin yarısından fazlasını oluşturacaktır. Bu durum havayolu şirketlerinin kârdan daha büyük bir pay elde etmeleri anlamına gelmekle birlikte dolandırıcılık risklerinin de artması anlamına gelmektedir.

Havayolu sektörü, dolandırıcılar için hem çekici hem de savunmasız bir sektördür. Bu çekicilik ve savunmasızlığın nedenlerini; yüksek değerli ürünler, global erişim ve dijital anonimlik, hızlı tüketim, düşük koruma engelleri, düşük kar marjları ve tedarikçilerin sayı ve çeşitliliği olarak belirtebiliriz.

Enett (2018) Fraud In Travel Payments Report'a göre, seyahat sektöründeki dolandırıcılığın maliyeti 21 milyar dolar olup, 2020 yılında bu tutarın 25 milyar doları aşması beklenmektedir. Yapılan bir araştırmada, araştırmaya katılanların %57'si ödeme işlemlerinde dolandırıcılıkla ilgili endişe taşıdıklarını, en yüksek dolandırıcılık riskini %60 ile tedarikçilere yapılan ödemeler, %35'i web üzerinden, %9'u da yabancı kredi kartları ile alınan ödemeler olarak belirtmişlerdir. Dolandırıcılığın doğrudan maliyetleri olduğu gibi dolaylı maliyetleri de vardır ve bu maliyetler tespit edilebilir. Raporda, seyahat aracıları için dolandırıcılıktan kaynaklanan doğrudan kaybın yaklaşık 6 milyar dolar olduğu ve bu tutarın 2.5 milyar dolarlık kısmının OTA (Online Travel Agency)'lardan kaynaklandığı tahmin edilmektedir. Sektörde, dolaylı maliyetlerin doğrudan maliyetlerin 2.5 katı olduğu kabul edilmektedir. Buna göre, dolandırıcılıkla ilgili dolaylı maliyetlerin, 15 milyar dolar olduğu ve bu tutarın 6,3 milyar dolarının da OTA'lardan kaynaklandığı tahmin edilmekte ve OTA'lar için dolandırıcılık kayıplarının 2020 yılında 11 milyar dolar olacağı tahmin edilmektedir. Dolayısı ile havayolu şirketlerinin dağıtım kanalları açısından bu tercihi (OTA) kullanmak istemeleri durumunda, OTA kaynaklı dolandırıcılıkların doğrudan ve dolaylı maliyetlerini dikkate almaları önemlidir.

Birçok firmaya dolandırıcılık ve suistimal konusunda destek veren Sift (2019)'e göre, havayolu sektöründe, 90'lı yıllarda ödeme yöntemlerinin çeşitlenmeye başlamasıyla birlikte bu yolla yapılan dolandırıcılık ve sahte işlemlerde artmaya başlamıştır. Bu artan dolandırıcılık ve sahte işlemler yeni önleme ve denetleme sistemlerini zorunlu hale getirmiştir. Emarketer (2017)'e göre, 2018 yılında 676 milyar dolar olan dijital seyahat harcamalarının, 2021 yılında 855 milyar dolar seviyesine ulaşması beklenmektedir. Görüleceği üzere dijital kanallarda ortaya çıkan bu hızlı büyüme, bu alandaki dolandırıcılık ve sahtecilik işlemleri için potansiyel bir riskli alan oluşturmaktadır. IATA (2019)'nın, 2019 yılı tahminlerine göre, havayolu sektöründe net kar marjının ortalama %3,1 olduğu göz önünde bulundurulduğunda, dolandırıcılık nedeniyle ortaya çıkacak gelir kayıplarının önemi daha iyi anlaşılır**.** Bu nedenle Sift (2019), ödeme yöntemlerindeki dolandırıcılıkların ciddi olarak incelenmesi ve önlenmesi için gerekli adımların atılması gereğine işaret etmekte ve yapılan çalışmalarda, seyahat firmalarının %40'ının bu dolandırıcılıkları yönetilmesi gereken en önemli problem olarak gördüklerini belirtmektedir.

Sorrells'e (2019, 10 Haziran) göre, seyahat sektörü, giyim, yiyecek ve oyun gibi diğer e-ticaret kategorilerine kıyasla, ödeme sahtekarlığı potansiyelini artırabilen ve tespit etmeyi zorlaştıran bazı özelliklere sahiptir. Bunlardan biri işlem değerinin yüksek olmasıdır. Örneğin yapılan çalışmalarda, hileli bir rezervasyonun ortalama fiyatının 283 $ ile 588 $ arasında olduğu tahmin edilmektedir. Bir diğeri ise son dakika rezervasyonları olup bu kısıtlı zaman nedeniyle kontrollerin anında yapılamamasıdır. Örneğin mobil otel rezervasyonlarının %72'sinin kalış tarihinden sadece bir gün önce yapıldığı tahmin edilmektedir.

CAPA (2011)'ya göre, havayolu sektöründe toplam gelirin %1 – 1,5'luk kısmı dolandırıcılık riski altında olup bu oran, Orta Doğu ve Latin Amerika gibi bazı pazarlarda gelirin %3 – 4'üne kadar çıkabilmektedir. Bu riskleri yönetebilmek için kurulan otomatik dolandırıcılık önleme sistemleri nedeniyle rezervasyonların %8 ile %25'ini kaybedilmekte ve bu sistemler nedeniyle büyük bir gelir kaybı yaşanmaktadır. Nihayet bu duruma, Aralık 2010'da San Francisco'da düzenlenen Havayolu Seyahat Ödemeleri Zirvesi'nde yapılan sunumlarda da dikkat çekilmiştir. CAPA'ya göre, %1 – 1,5'luk sahtekarlık sorunu olan bir sektör için bu otomatik reddetme sistemi inanılmaz derecede boşa giden bir uygulamadır. Çünkü %1-1,5'luk bir risk karşılığında reddedilen rezervasyon oranı çok daha fazladır.

Gerek seyahat sektörü ve gerekse spesifik olarak havayolu sektöründe oluşan yolsuzluk ve dolandırıcılıklar yukarıdaki rakamlardan da görüleceği üzere çok ciddi boyutlardadır. Aşağıda bu dolandırıcılık yöntemlerinden uygulamada en fazla karşılaşılanlara örneklerle yer verilecektir.

4.1. Kredi Kartı Dolandırıcılığı

Havayollarının sunduğu hizmetlerin satın alınması sırasında kullanılan kartlı ödeme yöntemleri, bu dolandırıcılık tipinin başında gelmektedir. Bu dolandırıcılık yöntemi şu şekilde işlemektedir. Tamamlanan işlemler sonucunda, kart sahibi bankasına itirazda bulunarak, işlemi kendisinin gerçekleştirmediğini bildirmekte ve tutarın tekrar hesabına iadesini (chargeback) talep etmektedir. Bu

yöntem, gerçek kart sahibinin bilgilerinin ele geçirilmesi ile yapılan işlemler olarak da tanımlanabilir. Bu bilgiler, kart hamilinin kartının ele geçirilmesinden, POS ya da ATM cihazlarından kopyalanmasına, oltalama (phishing) yönteminden, sahte online siteler yolu ile kart bilgisinin dijital ortamda temin edilmesine kadar farklı yollar ile gerçekleştirilebilmektedir. Chargeback (2020) tarafından yayınlanan Industry Dispute Ratio Raporuna göre kredi kartı dolandırıcılıklarının risk ve hacim olarak sıralaması düşükten yükseğe doğru şu şekildedir. Card Present işlemler, sonrasında kart sahibinin fiziksel olarak satışın yapıldığı yerde bulunmadığı Card not Present online işlemler ve çağrı merkezi işlemleridir. Yüz yüze işlemlerde riskin düşük olmasının nedeni, karta ait bir şifrenin (CHIP & PIN) girilmesi zorunluluğu, kimlik ve imza kontrollerinin yapılabilir olmasıdır. Yüz yüze işlemlerdeki kadar olmamakla birlikte, online kanallardaki kredi kartı dolandırıcılık riskleri de, şifre yönetimi (3D Secure), biyometrik kontroller (parmak izi, yüz tarama.vb) ya da adres teyit sistemi (AVS – Adress Verification System) gibi uygulamalar ile azaltılabilmektedir. Ancak, çağrı merkezlerinde bu yöntemlerin tam anlamı ile kullanılabilmesi mümkün olmadığından, kredi kartı dolandırıcılığı daha fazla olabilmektedir.

Nilson Report (2019)'a göre, dünya genelindeki dolandırıcılık kayıpları, 2018 yılında 27,85 milyar dolara ulaşmıştır. Bu tutarın gelecek beş yıl içinde 35,67 milyar dolara ve 10 yıl içinde ise 40,63 milyar dolara ulaşması beklenmektedir. Küresel anlamda toplam kredi kartı hacmi 40.5 trilyon dolara ulaşmış olup bu tutarın %21.54'ü ve kredi kartı dolandırıcılıklarının da %33,99'u ABD'nde gerçekleşmektedir.

UK Finance (2019) Fraud The Facts Report'a göre, İngiltere'de kredi ve banka kartları ile yapılan dolandırıcılıklar, 2017'de 565,4 milyon pounddan yüzde 19 artış ile 2018'de, 671,4 milyon pounda ulaşmıştır. Her 100 poundluk harcama için dolandırıcılık miktarı 2017 yılında 7 pence iken 2018'de 8,4 pence olarak gerçekleşmiştir. Bütün bunlara rağmen bankalar ve kart şirketleri tarafından alınan önlemlerle 1,12 milyar pound tutarında dolandırıcılık önlenmiştir.

Visa (2014)'ya göre, kredi kartı ile yapılan tüm işlemlerdeki genel dolandırıcılık oranı %0,045 iken havayolu sektöründe dolandırıcılık riskini iyi yöneten şirketler için bu oran sektör ortalamasından %0,006 puan daha düşüktür. Buna rağmen, özellikle güvensiz e-ticaret kanallarında bu oranlar birçok havayolu şirketi için hala çok yüksek gerçekleşmektedir. Öyle ki, Avrupalı bayrak taşıyıcı iki havayolunda bu risk, 60 baz puanı aşarak, Visa genel ortalamasının yaklaşık 13 katına ulaşmıştır. Buna karşılık, Card Present işlemlerde sahtekarlık oranı genel ortalamadan 4 baz puan daha düşüktür. Bunun nedeni, Visa Avrupa işlemlerinin, Chip – Pin ile korunmasıdır. Bu nedenle, sahtekarlık risklerinden korunmak için, kartlı işlemlerde Chip-Pın uygulamalarının yaygınlaştırılması gerekmektedir. Visa Raporu'nda, genel kredi kartı dolandırıcılığı ile havayolu sektöründe kredi kartı ile yapılan dolandırıcılıklar karşılaştırılmış ve havayolu sektöründe kredi kartı dolandırıcılık oranının çok daha yüksek olduğu tespit edilmiştir. Örneğin, ABD'de kredi kartı ile yapılan tüm işlemlerde dolandırıcılık oranı %1,26 iken havayollarında kredi kartı ile yapılan işlemlerde bu oran %19,3'tür. Aynı şekilde bu oranlar İngiltere'de %0,12 ye karşılık %16, Fransa'da, %0,48'e karşılık %15,4, Kanada'da,%1,9'a karşılık %5,5 ve Almanya'da %0,29'a karşılık %5,1'dir.

Feinstein (2019)'e göre, Afrika'daki (18 ülke) havayollarında yapılan dijital ödeme sayısının, 2017-2018 arasında %56'dan fazla arttığı, Afrika içi ve dışındaki uçuşlar için hileli ödeme girişimlerinin çoğunun Kuzey Amerika ve Doğu Avrupa'dan geldiği tespit edilmiştir. 2009-2018 yılları arasında havayolu dijital ödemeleri arasındaki hileli girişimlerin ilk 10 ülkesi küresel nitelikte olup başta ABD, ardından Kanada, Güney Afrika ve Doğu Avrupa ülkeleri gelmektedir. Havayollarının dolandırıcılık risk ekiplerinin, bu ülkelerden yapılacak olan online ve çağrı merkezi kanalları üzerindeki bilet satın almalarında daha dikkatli olmaları ve ek önlemler almaları uygun olacaktır.

4.2. Ters İbraz Sahteciliği (Friendly Fraud – Chargeback Fraud)

Clearsale (2018)'e göre, bu işlemler kart sahibi tarafından yapılmakla beraber, işlemin hatırlanamaması, hizmetten memnun kalınmaması, talep ettiği iadenin gerçekleştirilememesi veya kart hamilinin kötü niyetli olarak hareket etmesi nedeniyle, işleme kendi kredi kartı bankası üzerinden itiraz etmesi (chargeback) nedeniyle meydana gelmektedir. Ters ibraza neden olan dolandırıcılık dışı bir diğer konuda, kart hamilinin, ödemesini yaptığı hizmeti alamaması (Service not provided) ya da iadesinin yapılamamasıdır (Credit not Received). Hizmetin alınamadığı iddiaları gerçek olabileceği gibi dolandırıcılık amaçlı da olabilir. Bu nedenle, bu tür itirazlar (service not as described) için detaylı bir inceleme yapılması önemlidir. Örnek olarak, business sınıfı için bilet alan bir yolcu, koltuğunun bozuk olduğunu iddia ederek bilet parasının iadesini talep edebilmektedir. Ödeme yapılmadan önce, gerçekten yolcunun oturmuş olduğu koltukla ilgili teknik birimlere böyle bir arıza kaydının açılıp açılmadığı, ya da uçuş ekipleri tarafından koltukla ilgili bir arıza tespit edilip edilmediği doğrulanmalıdır. Özellikle, tüketici hakları ile ilgili sert düzenlemeler olan ülkelerde, örneğin ABD'nde bu tür yöntemler daha fazla kullanılabilmektedir.

Havayollarında herhangi bir uçuşun gerçekleşmemesi durumunda, yolcuya bilet bedelinin ne şekilde verileceği bütün detayları ile belirlenmiştir. Dolayısı ile havayolları da bilet iade işlemlerinde bu kurallara göre hareket etmekte ve bilet iadesi yapmaktadırlar. Bu ücret iade kurallarına göre, bilet bedeli üzerinden belli kesintiler yapılmaktadır. İşte bu nedenle, kart sahipleri, kesintiye uğraması muhtemel tutar dahil ücretin tamamını alabilmek için, bilet iadesini havayolu üzerinden değil, bankası üzerinden tüm ödemeye itiraz ederek geri almak istemektedir. Böylece kart sahibi, havayolunun ücret kurallarına takılmadan, ödemiş olduğu tüm bedeli iade olarak alabilmektedir. Bu durum her ne kadar henüz alınmamış bir hizmetin (uçuşu tamamlanmamış bir biletin) iadesi gibi görülse de, havayollarında her bir uçuştaki her bir koltuğun o uçuşa özel olması, yani stoklanamayan bir şey olması nedeniyle, bu seferde boş kalan bir koltuğun bir sonraki sefer için bir gelir katkısı olmamaktadır. Cebeci (2017)'nin aktardığına göre, ABD'li havayollarının bilet iade işlemlerinden elde ettiği gelir yıllık 2,3 milyar dolar gibi önemli bir rakamdır. Genellikle uçuşa 12 saat kalana kadar yapılan iade ve iptal işlemlerinde, THY, Pegasus, Onur Air, Atlas Jet, Sun Expres gibi havayolları ortalama bilet bedelinin %30'u oranında bir kesinti yapmaktadır. Görüleceği üzere bu tutarlar havayolları açısından önemli bir gelir kaynağı olarak değerlendirilmelidir. Bu nedenle bilet iade ve iptaline ilişkin

itirazların uygun bir şekilde incelenmesi ve sektör ortalamasının üzerindeki chargeback ve bilet iade durumlarında dolandırıcılık ve risk ekiplerinin konuyu detaylı olarak değerlendirmeleri önemlidir.

Lustosa (2020)'ya göre, chargeback (ters ibraz), satıcılar için e-ticaret sahtekarlığı kayıplarının arkasındaki en büyük faktörlerden biri olmaya devam etmektedir. Örneğin 2018'de, işletmelerin yarıdan fazlasının hileli chargebackler nedeniyle 11 ila 50 baz puan arasında gelir kaybettiği ve %22'sinin ise 50 baz puandan fazla kayıp verdiği tespit edilmiştir. Bu durum işletmeleri ya e-ticaret kanalının dışına çıkarmakta ya da daha yüksek maliyetlere katlanmalarına neden olmaktadır. Çünkü kredi kartı ihraççıları, chargeback oranları, düzenli olarak aylık işlemlerinin %1'ini aşan bir işletme ile çalışmak istememekte ve hesabı iptal etme yoluna gitmektedir. Bir e-ticaret işletmesi için bunun anlamı çok ciddi anlamda satış kaybı demektir. Bu durumda işletmeler kendilerini sahtekârlığa karşı korumak için aşırı güvenlik kaygıları ile her şüpheli işlemi reddetmekte bu da satışların düşmesine neden olmaktadır. Bu tür sahte işlemlerden kaynaklanan kayıpların 2021 yılına kadar 443 milyar dolara ulaşacağı tahmin edilmektedir.

Havayolları ters ibraz dolandırıcılığına karşı kendi ekipleri ile mücadele edebileceği gibi bu hizmetleri dış kaynak kullanımı yoluyla da alabilir. Elizabeth (2018)'e göre, Avianca'nın ClearSale ile bu alanda kurmuş olduğu işbirliği sektör açısından iyi bir uygulama örneğidir. Avianca, ClearSale ile ortaklık yapana kadar yüksek ters ibraz oranları ile mücadele etmiş ancak istediği sonuçlara ulaşamamıştır. Bu işbirliği sonunda, ClearSale, her havaalanı bağlantısıyla ilişkili olası riski hesaplayan ve modelin altında yatan verileri sürekli olarak izleyen ve güncelleyen özel bir istatistiksel model oluşturmuştur. Model, ClearSale'in siparişlerin %95'ini otomatik olarak onaylaması esasına göre kurgulanmış ve yapılan çalışmalar sonucunda Avianca'nın ters ibraz oranları yarıya indirilmiş ve onay oranları %98'e kadar korunabilmiştir. Avianca örneğinden de görüleceği üzere doğru bir dış kaynak kullanımı havayollarına dolandırıcılıkla ilgili ciddi bir etkinlik ve tasarruf sağlayabilir. Bizim önerimiz belli ölçeğin altında ve iyi bir dolandırıcılık ekibini bünyesinde istihdam etmekte zorlanan havayolları için dış kaynak kullanılmasının daha efektif ve verimli olacağı yönündedir.

4.3. Kullanıcı Hesabı (Account Takeover) Dolandırıcılığı

Baracuda (2020)'ya göre, bu dolandırıcılık tipi, ödeme sistemlerinde kayıtlı kullanıcı bilgilerinin ele geçirilmesi (mil, e-cüzdan, kredi kartı, banka kartı, banka hesabı, kimlik bilgisi ve diğer dijital hesaplara ilişkin bilgiler) sonucu gerçekleştirilmektedir. Dolandırıcılar, bu hesapları ele geçirmek için, genellikle zararlı yazılımlar (Malware, Trojan Horse) ve sahte e-mail (phising) yöntemlerini kullanmaktadırlar. Phising için kullanıcıya, gerçek bir havayolundan ya da havayolu programından üyelik bilgileri güncellemesi, hediye kazandığına dair içerikler gönderilmekte ve kullanıcının gerçek bilgilerini girmesi istenmektedir. Bu sayede dolandırıcılar, gerçek kullanıcının bilgilerine erişerek, havayolunun satış kanallarından bu hesap aracılığıyla işlem gerçekleştirebilmektedirler. Dolandırıcıların kullandığı bir diğer yöntemde, çeşitli internet sitelerinden toplu olarak temin edilen kullanıcı bilgilerinin, kullanıcı hesapları üzerinde denenerek hesabın ele geçirilmeye çalışmasıdır. Söz konusu yöntemleri kullanarak elde edilen hesap bilgileri üzerinden havayolu hizmetleri satın alınabildiği gibi,

hesaba ilişkin bilgiler güncellenerek hesaptaki krediler (mil, voucher, ödül puan ve biletler) farklı kişilere de satılabilmektedir. Smith'e (2014) göre, dolandırıcılar, FFP hesaplarını (genellikle kötü amaçlı bilgisayar yazılımı kullanarak) ele geçirmenin bir banka hesabını ele geçirmekten daha kolay olduğunu keşfettikleri için, şüpheli olmayan müşterilerin hesaplarını giderek daha fazla ele geçirmeye başlamışlardır.

Elliott (2019)'a göre, tatil ve seyahat imkanları geliştikçe, insanlar havayolu, otel veya araba kiralama şirketleri ile daha fazla veri paylaşmakta ve bu da verilerin ele geçirilme riskini artırmaktadır. 13 sektöre yönelik olarak yapılan bir çalışmada havayolu sektörü %61 ile bu alandaki en riskli sektör olarak görünmektedir. Havayollarına yönelik sahtekarlık saldırıları, bir önceki yıla göre, 2016 yılında %16, 2017'de %37 ve 2018'de %29 olmuştur. Hesap devralma dolandırıcılığını sadece geleneksel bir dolandırıcılık olarak değerlendirmemek gerekir. Çünkü dolandırıcılar, bu bilgileri çok daha geniş bir alanda kartın sahibiymiş gibi davranarak hesaba eklenmiş tüm kişisel bilgiler grubuna tam erişim sağlayabilmektedirler. Yani, bu bilgilerle herhangi bir şey satın alabilir, para çekebilir, çalınan bilgileri diğer platformlarda kullanabilir veya diğer bağlı hesaplara erişebilirler. İşte bu yönüyle hesap ele geçirme işlemleri, yalnızca ödeme noktasında yapılan bir sahtekarlıktan çok daha büyük sonuçları olan bir dolandırıcılık yöntemidir.

4.4. Program veya Prosedür Suistimali (Sahte Acenteler, Mil, Voucher vb.)

Bu başlık altında, havayolları tarafından yolcularına sunulan sık uçuş programları (FFP), ödül biletler, aksaklıklar ya da memnuniyetsizlik karşılığı verilen seyahat çekleri (voucher) veya hediye çekleri (Gift Card) üzerinden gerçekleştirilen dolandırıcılıklara yer verilecektir. Havayollarının müşteri sadakat programları için sunmakta olduğu satın alınan ve uçulan biletler karşılığı kazanılan ödül krediler, mil programı hesaplarında yolcu adına bir sonraki satın almalarında kullanılmak üzere saklanmaktadır. IATA (2019) 2019 yılı itibariyle sektörde yaklaşık, 23.8 trilyon kullanılmamış mil olduğunu ve bunun parasal karşılığının da 238 milyar dolar olduğunu tahmin etmektedir. Bu kadar büyük tutarların yer aldığı ve genellikle kredi ya da banka kartı bilgilerini ele geçirmekten daha kolay olduğu için mil dolandırıcılığı, dolandırıcılar açısından önemli bir potansiyel olarak görülmektedir. Smith (2014)'e göre, sadakat dolandırıcılığı, Amerikan Havayolları'nın yaklaşık 30 yıl önce çıkarmış olduğu AAdvantage programı ile başlamış ve bugüne kadar gelmiştir. O zamanki dolandırıcılıklar, kazanılan millerin Duty Free'lerde harcanması sırasında, FFP kart bilgilerini kaydeden çalışanlar ile takas edilen millerle çok indirimli bilet satan seyahat acenteleri tarafından yapılmaktaydı. Smith'in, FFP'si olan yaklaşık 50 kurum ile yapmış olduğu çalışmada, katılımcıların %72'sinin FFP dolandırıcılığı yaşadığı, %18'inin böyle bir şey yaşamadığı ve %10'unun da yaşamamış olduklarını düşündükleri tespit edilmiştir. Katılımcılar ayrıca, dolandırıcılık sorununun hızla büyüdüğünü belirtmişler ve bunun sebebi olarak ta, Müşteri Sadakat Programları Standardı, IFRIC 13'teki değişikliği göstermişlerdir. 2009 yılında, IFRIC 13'te yapılan değişiklikle verilen millerin ancak itfa edilmesi halinde gelir yazılacağı kuralı getirilmiştir. Bu değişiklik nedeniyle mil veren firmalar müşterilerin puanlarını / millerini bir an önce "nakit" veya "nakit benzeri" ürünlere dönüştürmelerine imkan tanımak için,

havayolları dışında da kullanımına izin vermek zorunda kalmışlardır. Bu durumda mil dolandırıcılıklarını tetiklemiştir.

Mil dolandırıcılıklarında kullanılan yöntemlerden biri, kullanıcılara yollanan sahte bir elektronik posta ile şifresini güncellemesi gerektiği bilgisi verilmekte ve kullanıcının bu sahte yönlendirme üzerinden gerçek kullanıcı bilgilerini iletmesi neticesinde, mil hesapları ele geçirilebilmektedir. Bir diğer yöntem ise, kötü niyetli acentelerin, yolculara sattığı biletler karşılığında bir mil hesabı oluşturarak ya da hali hazırda mil kazanması gereken yolcunun bilgilerini kendi mil hesabına aktararak, haksız mil elde etmesi ve bu biletleri yeniden ücretli olarak başka yolculara satmasıdır. Örneğin, bir seyahat acentesi yolcularına düşük ücretli biletlerin seyahat mili kazandırmadığını söyleyerek, yolcularının satın aldığı biletlere istinaden oluşan milleri kendi hesabına aktarmak suretiyle, 3.7 milyon mil elde etmiş ve bu dolandırıcılık ortaya çıkartılana kadar kendisi ve ailesi için 100 bin dolarlık mili harcamış olduğu tespit edilmiştir. Benzer bir örnek, Delta Havayollarının Skybonus programı için meydana gelmiş olup, acente sahibi benzer bir yöntem ile haksız olarak toplam 1.75 milyon dolarlık (42 milyon mil) bonus kazanmış ve harcamıştır. (Slotnick, 2019; Helsel, 2019)

Mil haricinde, havayollarında kullanım alanları ve hacmi artan seyahat çekleri ve hediye kartlarında da sahtecilik işlemleri gözlemlenmektedir. Havayollarının dijital kanallarında, satış ofislerinde veya anlaşmalı firmalar üzerinden satışa sunulan hediye çekleri, çalıntı kredi kartları ile satın alınabilmektedir. Bunun yanı sıra, tıpkı kredi kartlarında olduğu gibi, hediye çekleri de dijital bilgiler içerdiğinden, kopyalanabilmekte, şifreleri alınabilmekte veya çoğaltılabilmektedir. Son olarak, havayollarının veri güvenlik sistemine erişim veya seyahat çeki bilgilerinin mail ortamında paylaşılması sonucunda, bu veriler dışarıya aktarılmakta ve dolandırıcıların eline geçebilmektedir.

Aksoy ve Sever (2012)'e göre, dolandırıcılık amaçlı kullanılan yöntemlerden biri de, ikiz ya da sahte web siteleridir. Bu yöntemde piyasada bilinirliği ve güveni yüksek olan firmaların sahte web siteleri yapılmakta ve müşteriler bu sitelere girerek farkında olmadan dolandırılmaktadırlar. Panda Labs'ın 2010 raporuna göre; her hafta 57 bin sahte web sitesinin oluşturulduğu ve bu sahte sitelerin %63,72'sinin bankalara, %26,81'inin ise online alışveriş yapılan tanınmış işletmelere ait olduğu belirtilmektedir. Uygun fiyatla uçak bileti almak isteyen yolcularda, bu sahte acentelerin kurbanı olabilmektedir. Bunlar genellikle çalıntı kartlarla aldıkları biletleri ucuza satmakta ve bu işlemler tespit edildiğinde de havayolları sahte işlem ile gerçekleştirilen bilet satışını iptal etmektedir. Bu durumda, finansal kayıp sadece havayolu için değil, esas amacı uygun ücretli havayolu ulaşım hizmeti almak isteyen tüketiciyi de etkilemektedir. Elliot (2018)'a göre, American Airlines'la benzer alan adına sahip 17 sahte site bulunmakta ve bunların 12 tanesi kötü amaçlı faaliyet kapsamında kara listede bulunmaktadır. Bunun yanında, United Airlines, Delta Airlines, Southwest Airlines, Alaska Airlines ile hem otel hem havayolu rezervasyonu yapılabilen Expedia ve Trip Advisor gibi firmalar taklit edilerek açılmış birçok sahte site bulunmakta ve müşteriler bu sahte siteler yolu ile dolandırılabilmektedirler.

Havayolu sektöründe acente dolandırıcılıklarının en yaygın olduğu alan, Adale (2018)'ye göre, çevrimiçi seyahat acenteleri (OTA)'dir. 2017 yılına göre 2018'de toplam çevrimiçi dolandırıcılık %13

artmasına rağmen bu oran seyahat sektöründe %37 olarak gerçekleşmiştir. Seyahat markaları ve çevrimiçi seyahat acenteleri (OTA) ile yapılan büyük miktarda işlem nedeniyle bu alan seyahat sahtekarlığı yapmak isteyenler için önemli bir alan olarak görülmektedir. Bu nedenle havayolları bu alanı riskli alan olarak belirlemeli ve uygun denetim teknikleri ile bu dolandırıcılıkların önüne geçmelidir

Silk (2020)'e göre, dolandırıcılar dikkatini kredi kartı sahtekarlığından sadakat programları sahtekarlığına doğru kaydırmaya başlamıştır. Bu dolandırıcılığın boyutları tam olarak bilinmemekle beraber, 2017 yılı için bu tutar yaklaşık 1 milyar dolar ve dünya çapındaki havayolu milleri kullanımının %1'i olarak tahmin edilmektedir. Yapılan çalışmalarda, sadakat programı dolandırıcılığının son 15 ila 18 ay içinde hızlandığı ve özellikle havayollarına yöneldiği görülmektedir. E-ticaret sahtekarlığı önleme şirketi Forter'e göre, 2020 yılında, havayolu, konaklama ve perakende sektörleri de dahil olmak üzere dünya çapında sadakat üyeliklerinin sayısının 5,5 milyara ulaşması beklenmekte ve bu üyeliklerin %45'inin aktif olmadığı tahmin edilmektedir. Bu da onları saldırılara karşı özellikle savunmasız hale getirmektedir. Örneğin, 2018 yılında yapılan saldırılarda Birtish Airways'in 500.000 müşterisine ait veriler ele geçirilmiş ve Marriott saldırısında da, 383 milyon kayıt ele geçirilmiştir. Elliott (2019)'a göre, sık uçan yolcu ve sadakat programı müşterileri dolandırıcılıklar karşısında savunmasız durumdadır ve bu alan hızla büyüyen bir dolandırıcılık alanıdır. Bu alandaki dolandırıcılıklarda, 2018'in ikinci çeyreği ile 2019'un ikinci çeyreği arasında %89 oranında artış olmuştur.

5. Havayolu Sektöründe Ödeme Sistemi Dolandırıcılıklarının Önlenmesine Yönelik Öneriler

Sektör uzmanlarına göre, havayolları her üç dakikada bir ödeme dolandırıcılığının kurbanı olmaktadır. Bu nedenle dolandırıcılık havayollarının ele alması gereken ciddi bir sorundur. Amadeus (2014)'a göre, dolandırıcılıkla ilgili alınacak tedbirlerde çok kısıtlayıcı kurallar konulması durumunda, satışların azalması riski ortaya çıkabilirken, tersine, çok gevşek kurallar konulması da ters ibraz nedeniyle maliyetleri artırabilir. Belirlenecek sistem ve kural setinin bu ikisi arasında dengeyi sağlayacak şekilde kurgulanması gerekir. ACI Worldwide (2017)'a göre, havayolu sektöründe yaygın bir dolandırıcılık olmasına rağmen çok az sayıda dolandırıcılık aracı kullanılmakta ve manuel inceleme süreçlerine, adres doğrulama sistemlerine (AVS), kart doğrulama numarasına (CVN) ve 3D Secure gibi önleme tedbirlerine büyük ölçüde güvenilmektedir. Sektördeki veri büyüklükleri ve işlem hacimleri dikkate alındığında, manuel süreçler oldukça verimsiz, doğruluğu zayıf ve dolandırıcılık ekiplerini tüketen bir süreçtir. Bu nedenle sektörde bazı şirketlerde dolandırıcılık oranları hedef seviyenin on katına kadar ulaşabilmektedir. Sonuç olarak, manuel ve verimsiz süreçler bir yandan dolandırıcılık zararlarını artırırken diğer taraftan iyi müşterileri de azaltarak gelir kaybına neden olmaktadır.

Gerek havayolu ve gerekse diğer sektörlerde ödeme sistemleri yoluyla yapılan işlemlerde en önemli unsur kuşkusuz ki güven unsurudur. Bu güveni sağlamak üzere, Ödeme Kartları Endüstrisi Veri Güvenliği Standardı (PCI DSS) oluşturulmuştur. Yeşilyurt (2015)'a göre, bu standardın amacı,

ödeme kartlarının güvenliğinin sağlanması ve alınabilecek güvenlik tedbirlerinin global çapta yayılmasının teşvik edilmesidir. Standart, banka ve kredi kartlarının kullanımı esnasındaki güvenlik tedbirlerinin yanı sıra, e-ticaret sektöründeki tüm aktörlere de uygulanabilecek niteliktedir. Standart temel olarak;

- Güvenli ağ sistemlerinin oluşturulması ve bakımını,
- Kart sahibinin verilerinin korunmasını,
- Güvenlik zafiyeti yönetimi ve takibini,
- Güçlü erişim kontrol önlemlerinin uygulanmasını,
- Ağların düzenli olarak takibi ve testlerini,
- Bilgi güvenliği ilkelerinin korunmasını hedeflemektedir.

Aksoy ve Sever (2012)' de, ödeme sistemleri açısından güven konusuna vurgu yapmakta ve sistem güvencesini, tedarikçinin online alım satım sisteminin güvenliği ve güvenilirliği olarak tarif etmektedirler. Online alışverişlerde, kredi kartı kullanıcısına cep telefonu mesajı gönderilmesi, vatandaşlık numarası ile kredi kartı sahibinin bilgilerinin örtüştürülmesi, güvenlik kodlarının istenmesi gibi uygulamaların tüketicideki güvenlik ve güvenilirlik duygularını artırdığını belirtmektedirler. Zengin ve Güngördü (2013)'de, tüketicilerin mobil cüzdan kullanmalarındaki en büyük faktörün algılanan güvenlik ve güven duygusu olduğunu belirtmektedirler.

Pek çok farklı neden ve yöntem ile havayolu sektöründe ödeme sistemlerinde dolandırıcılık gerçekleştirilmekte ve bu hacim her geçen yıl artış göstermektedir. Dolandırıcıların kullandıkları yöntemler karmaşık ve üst düzey bir hal almaya başladıkça, sektör içerisinde yer alan paydaşlar da bu yöntemlere nasıl karşılık vermeleri gerektiği konusundaki çalışmalarını artırmaktadırlar. Enett (2018) tarafından Edgar, Dunn Company'e yaptırılan Fraud In Travel Payments Report'ta özetle, dolandırıcılıkla tek başına mücadelenin mümkün olmadığı, sektör genelinde işbirliğinin zorunlu hale geldiği belirtilmektedir.

Visa (2014) tarafından yapılan çalışmada havayollarındaki dolandırıcılıkların,%14'ü güvenli e-ticaret, %32'si posta/telefon siparişi (MOTO) ve %54'ü güvenli olmayan e-ticaret platformlarında yapılmaktadır. Görüleceği üzere en fazla dolandırıcılık riski güvenli olmayan e-ticaret alanında ortaya çıkmaktadır. Buna karşılık, güvenli e-ticaret (VbV, Verifying by Visa) işlemlerinde dolandırıcılık riski düştüğü gibi uğranılan zararın tazmini de mümkün olabilmektedir. Visa, kredi kartı dolandırıcılıklarında, yöneticilerin doğrudan kar ve zarar etkisini temsil ettikleri için genellikle ters ibrazlara (chargebacks) odaklandıklarını belirtmektedir. Visa bunu gerekli görmekle beraber yeterli olmadığını, bunun yanında TC40 (Visa kredi kartı işlemlerindeki her türlü dolandırıcılık işlemlerine ait rapor) raporlarının da alınması ve takip edilmesinin dolandırıcılık risk ve zararlarını engellemek için önemli olduğunu belirtmektedir.

ARC (2020)'ye göre, ödeme sistemleri yoluyla yapılan dolandırıcılıkların önlenebilmesi için, kontrol noktalarının mümkün olduğunca otomatik hale getirilmesi, başarılı işlem hacminin korunması veya artırılması ve müşteri memnuniyetinin sağlanması için bir denge mekanizmasının kurulması gerekir. Sahte işlemleri önlemek amacıyla kullanılacak yöntemlerin, hizmetin satın alması sürecinde müşteri deneyimi ve memnuniyetini kötü yönde etkilememesi, mümkünse kontrolleri hiç hissetmemesi en önemli gereksinimlerin başında gelmektedir. Bu hedeflere ulaşabilmek ve ödeme sistemi dolandırıcılıklarının önlenmesine yönelik önerilerimiz aşağıdaki gibidir.

5.1 Tüm Satış Kanallarını Kapsayacak Bir Kontrol Sisteminin Kurulması

Havayolları, biletlerini ve ek hizmetlerini pek çok farklı satış ve dağıtım kanalı üzerinden yolcularına sunmaktadır. Bu kanallar, havayollarının kendi internet siteleri, mobil uygulamalar, çağrı merkezleri, şehir ve havaalanı (CTO/ATO) satış ofisleri, online ve offline acentelerdir. Etkin bir kontrol sistemi için, birbirinden farklı bu kanallar ve kural setleri için tek bir standart ve prosedürlere bağlı bir süreç yönetimi gerekmektedir. Dolandırıcılık işlemleri sadece bir satış kanalı üzerinde yoğunlaşmayıp, hizmetin tüketiciye sunulduğu tüm kanallarda meydana gelebildiği gibi, bir kanaldan alınan biletin, farklı kanallardan değiştirilmesi de mümkündür. Bu nedenle dolandırıcılar, rezervasyon değişikliklerini genellikle dolandırıcılığın fark edilmesini zorlaştıracak şekilde farklı kanallarda yapmaktadırlar. Örneğin, orijinal rezervasyonları çevrimiçi yaptıkları halde, rezervasyon değişikliğini çağrı merkezinden yapmaları yaygın bir uygulamadır. Çünkü çağrı merkezi personeli genellikle dolandırıcılık tespit etmek üzere eğitilmez. Ayrıca, veri derleme ve kanallar arasındaki bilgi paylaşımındaki eksikliklerde bu tür dolandırıcılık faaliyetleri için iyi bir fırsat yaratmaktadır.

ACI Worldwide (2017)'a göre, yabancı ödeme kartlarındaki yüksek dolandırıcılık oranları, seyahat sektörü için ortak bir sorun olmaya devam etmekte ve uluslararası alanda büyümek isteyen satıcılar için, özellikle dolandırıcılık yönetimi zorlukları yaratmaktadır. Bu anlamda bazı seyahat rotaları artık çok bilinen bir hal almış ve önemli birer risk içermektedirler. Bu rotalar, Nijerya, Mısır, Malezya, Endonezya, Rusya, Dominik Cumhuriyeti, Gana, Brezilya ve Güney Afrika gibi yerlerdir.

Feinstein (2019), sahtekarlığı azaltmak ve riski yönetmek için havayollarına beş öneride bulunmaktadır. Bunlar;

- Gerçek zamanlı izleme sistemleri kullanan bir ödeme hizmeti sağlayıcısıyla çalışmak.
- Sahtecilik geçmişi bilinen müşterilerden gelen şüpheli işlemleri otomatik olarak reddetmek için bir 'Negatif Liste' sistemi oluşturmak
- Kart ödemeleri için sağlam bir check-in prosedürü oluşturmak ve şüpheli rezervasyonlar hakkında ek bilgi toplamak.
- Personellerin uçuş rezervasyonları ve check-in prosedürlerini uygularken karşılaştığı hileli herhangi bir faaliyeti tespit etmeleri konusunda eğitmek.

- Gereksiz anlaşmazlıkları ve ters ibrazları önlemek için geri ödeme politikanızın açıkça müşterilerinize iletildiğinden emin olmak.

5.2 Risk Analiz Metodolojisi Geliştirilmesi

Sahte işlemlerin doğru ve hızlı bir şekilde tespit edilmesi, hem gelir kaybının önlenmesi hem de müşteri memnuniyeti açısından önem taşımaktadır. Tercih edilen kural seti nedeniyle yapılan analizin hatalı olması durumunda "sahte işlem" olarak reddedilen bir gerçek işlemin nasıl gelir azaltıcı bir etkisi varsa, benzer şekilde kullanılan kural seti nedeniyle tespit edilemeyen sahte bir işlemin kabul edilmesi de aynı şekilde gelir azaltıcı etkisi olacaktır. Bu nedenle risk analiz metodolojisi açısından optimum bir kural setinin belirlenmesi birinci derecede önemlidir. ACI Worldwide (2017) analistleri, dolandırıcılıkla ilgili iyi bir risk analiz metodolojisi için;

- 3 DS'in ötesine geçilmesini,
- Olumlu müşteri profilinin oluşturulmasını,
- Mevcut tüm verilerin kullanılmasını,
- Şirketinize uygun sahtekarlık stratejilerinin belirlenmesini,
- Yüksek riskli ve yakın tarihli rezervasyonlara öncelik verilmesini,
- İşlem akış görüntülerinin takibini,
- Kapsamlı izleme ve raporlama süreçlerinin kullanımını tavsiye etmektedirler.

Bütün bunları yapabilmek, işlemleri izlemek ve verileri zamanında sorgulamak için iş zekası araçlarını ve analizlerini kullanmak hem dolandırıcılık önleme performansını artıracak hem de sürekli bir iyileştirme sürecini desteklemeye yardımcı olacaktır.

Dolandırıcılıkla mücadele risk yönetim stratejisi için konunun uzmanları iki yönlü bir yaklaşım önermektedirler. Stratejinin birinci ayağında, şüpheli işlemleri inceleyecek iyi bir eğitim ve deneyime sahip dolandırıcılık analistlerine, yani iyi bir insan kaynağına sahip olmak. Diğer ayağında ise bilgisayar algoritmalarını, özel kuralları ve kanıtlanmış istatistiksel teknikleri, mevcut ve geçmiş verileri, sektördeki dolandırıcılık istatistiklerini ve işlem bilgilerini analiz etmek için kullanan bir makine öğrenmesi (Machine Learning)'dir. Ancak yapay zeka ve makine öğrenmesine dayanan sistemler, şüpheli olarak tanımlanan her işlemi reddedeceği için satışları düşürme riskinin dikkate alınması gerekmektedir (Elizabeth, 2018; Lustosa, 2020).

Dawes (2018), havayollarına dolandırıcılıklardan kaynaklanan mali ve operasyonel zarar riskini azaltmak için beş yol önermektedir. Bunlar;

- **İşlem Sahteciliğine karşı;** son dakika rezervasyonlar ve değişikliklerini, özellikle kalkış tarihleri veya ilk rezervasyon yeri ile önemli ölçüde farklı olan yerleri tespit etmek. Ayrıca, kalkış şehri ile ödeme kartı sahibinin adresi, müşteri sadakat geçmişi ve IP adresini eşleştirmek.

- **Hesap Devralmaya karşı;** hesap devralmaları tanımlanmalı, doğru araçlarla şüpheli hesap etkinlikleri otomatik olarak belirlenmeli ve geçerli hesap sahipleriyle gereksiz gerginlik oluşturmadan ek kimlik doğrulama önlemleri alınmalıdır.
- **Sadakat Programı Dolandırıcılığına karşı;** yeni sadakat programı üyelerinin ilk işlem olarak mil satın almaları sınırlandırılmalı veya yasaklanmalı ve ancak seyahat yoluyla mil kazanım zorunluluğu getirilmeli, ayrıca milleri diğer hesaplara – sık veya büyük miktarlarda – aktaran hesaplar belirlenmeli ve izlenmelidir.
- **Ödül Amaçlı Kötüye Kullanıma karşı;** biletleri ortalama müşteriden daha sık iptal ve iade eden kişiler belirlenmeli ve izlenmelidir.
- **Sahte Kart Dolandırıcılığına karşı;** sahte kart dolandırıcılığını yalnızca bir ad ve kart numarasıyla tespit etmek zordur. Bunun için daha fazla veri kaynağı kullanmak, yüz yüze işlemleri teşvik etmek ve e-ticaret kimlik doğrulama önlemlerini artırmak gerekir.

5.3 Kullanıcı Hesapları Yönetimi ve Yolcu Bilgilendirmeleri Sistemi Kurulması

Visa (2018)'ya göre, hizmetin sunulduğu kanallarda, sunulan hizmetin içeriği, değişiklik koşulları, iade süreci ve satış sonrası aşamaları müşteriye, kısa, net ve anlaşılır olarak sunulmalıdır. Bu sayede, özellikle ters ibraz sahteciliği (Friendly Fraud) en düşük seviyeye indirilebilecektir. Yine bu çerçevede, bilet satışı sonrası yolcunun ya da kart / hesap sahibinin, hizmet almakta olduğu finansal kuruluş tarafından sağlanan detaylı işlem dökümünde (ekstresinde) işleme ilişkin açık bilgilerin bulunması faydalı olacaktır.

Mil hesaplarının ele geçirilmesi işlemleri Paul (2018)'e göre, 1990'lara kadar gitmekte ve havayolları için daha iyi bir kimlik doğrulama sistemi geliştirilene kadar da devam edecektir. Örneğin, 2015 yılında Amerika'da, hem American Airlines hem de United Airlines'ta binlerce müşteri hesabı dolandırıcılık yoluyla ele geçirilmiştir. ABD havayolu sektörü, bu problemi çözebilmek ve veri güvenliği ile potansiyel güvenlik açıklarını tespit etmek için siber güvenlik uzmanlarıyla işbirliği içinde çalışmaya devam etmekte ve yolcu bilgilerini korumak için BT sistemlerine ve koruyucu önlemlere yatırım yapmaktadır.

Locke (2018), British Airways'in, müşteri sadakat programı ile ilgili dolandırıcılık riskine karşı, sistemi sürekli olarak kötüye kullanım açısından izlediğini ve bir risk tespit edilmesi halinde derhal uygun önlemlerin alındığını belirtmektedir. Ayrıca, müşterilere sahip oldukları her hesap için benzersiz şifreler kullanmaları ve bu şifreleri sık sık değiştirmeleri önerilmektedir. Etihad, sahtecilikle ilgili sorunları ele almak, şüpheli işlemlerin işlenmesini aktif olarak önlemek için özel bir sahtekarlık önleme ekibi kurmuştur. Emirates Skywards programındaki müşterilerinin hile yoluyla kaybolan veya çalınan millerini kurtarmalarına yardımcı olmakta ve hesaplarının herhangi bir şekilde ele geçirildiğine inanıyorsa üyelerin proaktif olarak şifrelerini sıfırlamalarını istemektedir.

Buna rağmen, Etihad ve Emirates dahil olmak üzere yaklaşık 20 havayolunun ödül programı puanları, değerlerinin altında satılmaktadır. Benzer şekilde, LoyaltyOne'a ait Kanada'nın en büyük sadakat programı olan Air Miles Kanada'nın, mil puanlarının mağazalarda ürün satın almak için kullanıldığı tespit edilmiştir. Hackerlar tarafından ele geçirilen bu miller internet üzerinden değerinin çok altında usulsüz ve yasadışı bir şekilde satılmaktadır. Örneğin, havayolları arasında değeri değişmekle birlikte bir mil değeri 0,01 ile 0,02 dolar arasında olmasına rağmen, 100.000 mil yaklaşık olarak internette 884 dolara satılmaktadır. Hırsızlar kimlik kanıtı gerektiği için çalınan milleri, gerçek uçak bileti veya otel harcamalarında değil, perakendecilerde indirim ve hediye kartları gibi ödüller için kullanmaktadırlar (Locke, 2018, Fuscaldo, 2018, Fraud.org,2019)

Mil dolandırıcılıkları sadece havayollarına saldırılar yoluyla değil bazen havayolu çalışanları tarafından da yapılmaktadır. Haq (2010)' a göre, bir Emirates Havayolları çalışanı, 2,6 milyon Skywards hava milini hileli bir şekilde toplayıp Kenya'ya düşük maliyetli biletler şeklinde yolculara sattığı için suçlu bulunmuştur. Bu olayda, gerçek yolcular Skywards programına bilgileri olmadan kaydedilmiş ve adlarına hesaplar açılmıştır. Ancak, havayolu çalışanı milleri toplamak için kendi e-posta adresini ekleyerek, Dubai'den Londra'ya 57 dönüş uçuşuna eşdeğer mil toplamıştır. Daha sonra bir acente ile anlaşarak, Kenya'ya uçacak yolculara daha ucuz uçuş fırsatı olarak kendi özel hattından iletişim kurmalarını isteyerek satmıştır. The Guardian (2004)'ın haberine göre, Londra'da bir havaalanı çalışanının, yaklaşık 5 milyon mili business class uçuşlarında açtığı sahte hesaplarla kullandığı ve en sonunda check – in personelinin dikkati ile yakalandığı ve 9 ay hapis cezasına çarptırıldığı belirtilmektedir.

5.4 Yeni Teknolojik Altyapılar Kullanılması

İletişimden eğitime, sağlıktan perakendeye kadar tüm sektörlerde etkisi hissedilen dijital dönüşüm süreçleri, havayolları için de vazgeçilmez öğelerin başında gelmektedir. BBC (2020)'nin haberine göre, dijitalleşmenin, seyahat ve turizm pazarında 2025 yılına dek, 305 milyar dolar ek gelir sağlayacağı öngörülmektedir. Sadece ürün ve hizmetlerin satış ve dağıtımında değil, satış sonrası süreçlerin yürütülmesinin yanı sıra, sahte işlemlerin tespiti, analizi ve sonuçlandırılmasında kullanılan yöntemler de, teknolojideki değişimlere paralel olarak değişmekte ve gelişmektedir. Sift (2019)'e göre, klasik kural seti kullanılan yaklaşımlardaki, kısıtlı veri ile çalışılması, manuel ve işlem tamamlandıktan sonraki kontroller gibi sorunlar yerini yapay zeka ya da makine öğrenmesi temelli mekanizmalara bırakmaktadır. Makine öğrenmesi sistemi, sadece sahte işlemleri tespit edip durdurmak ile kalmaz, ayrıca gerçek işlemleri de analiz ederek, anlık olarak kullanıcı deneyiminde olumlu bir etki de yaratır. Benzer şekilde yapay zeka içeren algoritmalar da, anlık olarak değerlendirmelerde bulunarak, en optimum seçeneğin belirlenmesine yardımcı olmaktadır. Şekerli (2019)'ye göre işletmeler, dolandırıcılık girişimlerinin tespitinde, güvenliğin artırılmasında, ses ve görüntü tanıma ile daha etkin insan-makine ara yüzlerinin oluşturulması gibi alanlarda da yapay zeka uygulamalarını kullanabilmektedirler.

Proaktif olarak dolandırıcılıkla mücadelede teknolojiyi kullanan sektörlerden biride bankacılık sektörüdür. Bankacılık sektörü, hem doğrudan hem de dolaylı olarak ödeme sistemlerinin önemli bir aktörü ve paydaşıdır. UK Finance (2019) Fraud The Facts Report'a göre, bankalar, potansiyel sahtekarlığı tanımlamak ve önlemek için, küresel dijital kimlik aracı olarak tanımlanan bir sistemi kullanmaktadırlar. Sistem, birçok ülkedeki milyarlarca gerçek zamanlı işlemi analiz ederek cihaz, coğrafi konum, davranışsal ve tehdit istihbarat girdisi de dahil tüm ek verileri analiz etmekte ve bunu tarihsel verilerle birleştirerek müşterisinin davranışının bir resmini oluşturmakta ve böylece olağandışı ve potansiyel olarak hileli faaliyetleri tanımlamakta ve işlem gerçekleştiği anda tespit edebilmektedir. Bunun yanında, izleme teknolojisi, bağlantılı hesap ağlarını ortaya çıkarmak için kullanılmakta ve veri anormallikleri analiz edilerek dolandırıcılıklar önlenmeye çalışılmaktadır. The Mule Insights Tactical Solutions yazılımıyla para birden fazla hesap arasında bölünmüş veya farklı kurumlar arasında seyahat etmiş olsa bile, hesaplar arasındaki şüpheli ödemeler izlenebilmektedir. Bunun yanında, İngiltere'de, tüm ödeme sağlayıcılar için yüksek tutarlı ve yüksek riskli işlemler için çok faktörlü kimlik doğrulaması kullanmasını gerektiren yeni kurallar setinin yürürlüğe girmesi beklenmektedir. Bu kuralların, bir müşteri çevrimiçi olarak belirli işlemleri gerçekleştirdiğinde, kısa mesaj veya biyometri yoluyla gönderilen bir defalık şifre gibi ikinci bir güvenlik düzeyi gerektireceği yönünde olması beklenmektedir. Bunun yanında, telefon bankacılığı sahtekarlığıyla mücadele etmek için bazı bankalar, her telefonun sahip olduğu farklı ses tonunu ve bulundukları ortamı tanımasını sağlayan teknoloji kullanmaktadırlar. Ayrıca, 'davranışsal biyometri' ile kişilerin oturum açtıklarında cihazlarına yazma ve kaydırma yöntemleri veya cihazlarını kavrama açısından nasıl tuttuklarını izleyen bir yazılım yardımı ile de dolandırıcılıklar önlenmeye çalışılmaktadır.

Praetsch (2019)'e göre, havayolları dolandırıcılık riskine karşı hala, 80'lerin 90'ların uygulamaları olan, adres doğrulama hizmetleri (AVS) ve kart doğrulama numaraları (CVN) ile iş yapmaya devam etmektedir. Çok basit bir şekilde açık web ve karanlık webde yapılacak kısa bir araştırma bile bu yöntemlerin ne kadar yetersiz olduğunu göstermeye yeter. Havayolları artık bu riskleri yönetmek için, biyometrik veriler, davranışsal veriler ve cihaz kimliği verileri kullanmak zorundadır. Bu teknolojilerle, bir kişinin sesini, parmak izini veya göz taramasını doğrulayarak kim olduğu ve söylediği kişi olup olmadığı tespit edilebilmektedir. Diğer taraftan, bir müşterinin web sayfanızla ve / veya cihazlarıyla nasıl etkileşime girdiğiyle kimlik doğrulaması yapılabilmektedir. Ayrıca, cihaz kimliği verileri ile kişisel olarak tanımlanabilir bilginin (PII) kullanımı da yaygın hale gelmektedir.

Herhangi bir alanda teknolojiden yararlanma konusu gündeme geldiğinde genel olarak, manuel ve rutin olarak yapılan işlemlerin makine veya sistemler tarafından yapılması anlaşılmaktadır. Ancak havayolu sektöründe amaç sadece manuel işlemlerin otomatize edilmesi değil, daha akıllı otomasyon sistemlerine geçerek, iyi bir dolandırıcılık analistinin verebileceği kararları alabilecek yapay zeka sistemlerine geçilmesidir. Bu tür teknolojileri büyük bankalar, Apple ve Microsoft gibi şirketler kullanmaktadır. Bu nedenle havayolu şirketleri de dolandırıcılık risklerini yönetebilmek için bu teknolojileri dikkate almak zorundadır.

5.5 Koordinasyon, Eğitim ve İşbirliği

Ödeme yöntemleri dolandırıcılıkları, sektörde tek bir paydaşı etkileyen bir sorun olmayıp, havayollarından acentelere, kart kuruluşlarından aracı firmalara kadar pek çok noktada finansal kayıplara ve verimsiz iş süreçlerine neden olmaktadır. Sorunun çözümlenebilmesi için de, tedarik zincirinde yer alan tüm tarafların etkin bir işbirliği içinde olması gerekmektedir. Ayrıca, satış ve rezervasyon operasyonunda çalışan personeller, başta olmak üzere, tüm ekiplerin sahte işlemleri tespit ve analiz edebilecek seviyede eğitime tabi tutulması önemlidir. Çalışanların yanı sıra, yolcuların da bu işlemlere yönelik bilgilendirilmesi, sahte işlemler daha başlamadan önlenebilmesi açısından etkili bir yaklaşım olarak değerlendirilebilir. Yolcuların, bilet alacakları acenteyi, IATA internet sitesi üzerinden, IATA üyesi olup olmadığını sorgulamaları da sahte acentelerin tespiti açısından önemlidir. Sift (2019)'e göre, yolcuların özellikle olması gerekenden çok uygun fiyatlı havayolu biletlerine bir önyargı ile yaklaşması, mümkünse farklı kanallardan (havayolu internet sitesi, diğer acente veya meta arama motorları (metasearch engine)) üzerinden talep edilen uçuşa ilişkin ortalama ücretlerin kontrol edilmesi gerekmektedir. İşbirlikleri çerçevesinde, uluslararası kuruluşların (IATA, ICAO, Europol vb) sunduğu veri paylaşımı, program ve prosedür çalışmalarına dahil olunması da etkili bir sahte işlem yönetimi koordinasyonu sağlayacak, güncel gelişmeler takip edilerek, gereken önlemler kısa sürede tüm havayolu sektörü içerisinde alınabilecektir (Europol, 2018, IATA (2016). Levens (2017)'e göre, havayolu dolandırıcılık analistlerinin, toplantılar ve çevrimiçi forumlar aracılığıyla bilgi alışverişinde bulunabilmeleri de önemli bir boşluğu doldurabilir. Bu amaçla kurulan açık platformlardan biri FraudChasers'dır. Bu platform aracılığıyla, dolandırıcılık analistleri sohbet edebilmekte, bilgi paylaşmakta ve gelecek toplantılar hakkında bilgi gönderebilmekte ve iyi uygulama örneklerini paylaşabilmektedirler. Bu işbirliğinin bir sonraki adımı ise veri paylaşmaktır. Ancak veri paylaşmadaki temel sorun, işletmelerin paylaştığı bu şüpheli sahtekarlık verilerinin sahipliğinin korunmasıdır. Bunun yanında, ödeme hizmeti sağlayıcıları, yazılım tedarikçileri, bankalar, sektör birlikleri, tüzel kişiler, ulusal polis kuvvetleri ve uluslararası kolluk kuvvetleri ve yargı alanlarında da işbirliği gereklidir

Bu alanda kullanılan yöntemlerden biride e-posta verileri üzerinden yapılan analizlerle dolandırıcılıkların önlenmesidir. Praetsch (2017)'göre, Emailage, kullanmış olduğu ağ istihbarat teknolojisi ile birçok endüstriden şirketlerin sahtekarlık bildirmesine izin vermekte ve böylece ortak ağda biriken işlem geçmişi sayesinde giderek daha doğru risk puanlaması yapılmasına imkan veren veriler sağlamaktadır. Süreç şöyle işlemektedir: herhangi bir dolandırıcılık ile karşılaşan işletmeler e-posta ile bu durumu bildirmekte ve bu e-postalar düzenli olarak onaylandıkça, kalıplar değiştikçe sahtekarlık modelleri güncellenmekte ve risk puanlamaları da buna göre değişmektedir. Böylece, işletmeler kendi durumlarını hem sektör genelinde hem de emsalleri ile mukayese edebilmektedirler. Bütün bu ağın arkasında çalışan ve sahtekarlıktan önce ortaya çıkacak kalıpları tanıyabilen makine öğrenmesi algoritmaları vardır

İngiltere'de, UK Finance (2019), kart dolandırıcılığını önlemek üzere, kendi istihbarat ağındaki güvenliği ihlal edilmiş kart ayrıntılarını hızlı ve güvenli bir şekilde belirlemekte ve bu bilgileri hükümet ve kolluk kuvvetleriyle paylaşmaktadır. Ayrıca, kart sahtekarlığı ile ilgili organize suç gruplarını

hedefleyen özel bir polis birimi olan Özel Kart ve Ödeme Suç Birimi (Dedicated Card and Payment Crime Unit)'ne de sponsor olmaktadır.

Günümüzde dolandırıcılığın almış olduğu şekil ve hacim dikkate alındığında, tek başına mücadele ile başarı elde etme şansının olmadığı açıktır. Nitekim Visa (2014)'ya göre, havayolu sektöründe sahtekarlık oranının yüksekliğine neden olan faktörlerden biri diğer paydaşlarla yetersiz işbirliği, diğeri de yetkililerle yani kolluk kuvvetleri ile sınırlı işbirliğidir.

6. Sonuç

Özetle, ödeme sistemlerinin gelişmesi ve yaygınlaşması beraberinde, bu yolla yapılan dolandırıcılık risklerini artırmakta ve risklerle mücadele etmek her geçen gün daha zor ve karmaşık bir hal almaktadır. Havayollarının bu riskleri önlemesi, denetlemesi ve yönetebilmesi için;

- Veri uyumluluğu ve bilginin güvenliğini sağlamak için BT altyapılarına daha fazla yatırım yapmaları,
- Kullanılan sistemlerin, güvenlik açıklarını tespit etmek ve müşteri bilgilerini korumak için siber güvenlik uzmanlarıyla işbirliği içinde çalışmaları,
- Çağrı merkezi üzerinden satış yapan havayolları için konuşma tanıma sistemlerini kullanmaları,
- Kapsamlı bir raporlama sistemi kurmaları,
- Dolandırıcılık riskine karşı daha güvenli olan sanal kartlar (VCC) ve sanal hesap numaraları (VAN) kullanmaları,
- Çevrimiçi saldırılar konusunda hem çalışanlara hem de müşterilere yönelik bilgilendirme ve farkındalık eğitimlerini desteklemeleri,
- Dolandırıcılık riskine karşı tüm paydaşlarla işbirliği içinde olmaları,
- Uçuş işlemlerinde hileli işlemlerin yoğunlaştığı bölge ve ülkeler için ek güvenlik önlemleri almaları,
- İyi eğitimli ve tecrübeli bir dolandırıcılık ekibi kurmaları,
- İyi ve etkin çalışan bir iç kontrol sistemi ve iç denetim birimi kurmaları,
- Dolandırıcılık konusunda sektörel deneyimi iyi olan firmalardan dış kaynak kullanmaları önerilmektedir.

Bu önemlerden hangilerinin uygulanması gerektiği tamamen, her bir işletmenin kendi içinde yapacağı ihtiyaç analizine göre belirlenmelidir. Çünkü ihtiyacın doğru belirlenmemesi halinde işletmeler, ya eksik ya da gereğinden fazla yatırım veya maliyete katlanmak zorunda kalabilirler.

KAYNAKÇA

Accelya (2019, 6 Ağustos). A new alternative form of payment every day – what airlines need to do. August 6, 2019, https://w3.accelya.com/blog/a-new-afop-every-day adresinden alındı (10.01.2020).

ACFE (2020). Report to the nations 2020: global study on occupational fraud and Abuse. https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf adresinden alındı (11.06.2020).

ACI Worldwide. Managing fraud on travel bookings. https://www.aciworldwide.com/-/media/files/collateral/trends/managing-fraud-on-travel-bookings-tl-us-1114-5581.pdf adresinden alındı(10.06.2020).

ACTA and the Canadian Travel Fraud Prevention Group (2016). http://www.acta.ca/news-releases/fraud1124. adresinden alındı (04.06.2020).

Adale, Fraud prevention within the online travel industry. https://fraud.net/n/fraud-prevention-within-the-online-travel-industry/ adresinden alındı (06.06.2020).

Airturk Haber (2020). https://www.airturkhaber.com/haberler/thyden-seyahat-ceki-secenegi/ adresinden alındı (18.07.2020)

Aksoy R. & Sever H. (2012). Elektronik pazarlarda güven problemi ve kriminal faaliyetler. *Electronic Journal of Vocational Colleges.* (2) 1, 154-164.

Alponat, T. (2006). *Kartlı ödeme sistemlerinin skonomiye etkisi ve Türkiye'de kartlı ödeme sistemleri*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi, İstanbul.

Amadeus (2014). Fraud management for airlines. https://amadeus.com/documents/en/travel-industry/sales-sheet/amadeus-fraud-management-for-airlines.pdf adresinden alındı (05.06.2020).

ARC (2020). Fraud prevention best Practices. https://www2.arccorp.com/support-training/fraud-prevention/best-practices/ adresinden alındı (17.01.2020).

Artuğer, S. (2011). *Sık uçan yolcu programlarının müşteri bağlılığı üzerine etkisi.* (Yayınlanmamış Doktora Tezi). Adnan Menderes Üniversitesi, Aydın.

Bailey, J. (2019, 30 Eylül). The future of paying for airline tickets – an interview with cellpoint digital, 30 September 2019. https://simpleflying.com/airline-tickets-future/ adresinden alındı (20.01.2020).

BBC (2020). How digitalisation is revolutionising the travel industry. http://www.bbc.com/storyworks/travel/the-new-tourism-trend/technology-redefine-tourism-industry adresinden alındı (01.05.2020).

BKM seçilen sektöre göre aylık gelişim, havayolu sektör verileri (2015-2019). https://bkm.com.tr/secilen-sektore-gore-aylik – gelisim/?filter_group=4&List=Listele adresinden alındı (03.06.2020).

Barracuda (2020). *Account takeover*. https://www.barracuda.com/glossary/account-takeover adresinden alındı (05.07.2020).

CAPA (2011, 22 Mart). *Fraud costs airlines USD1.4 billion a year. regional airlines the fraudsters' "carriers of choice"* 22-Mar-2011. https://centreforaviation.com/analysis/reports/fraud-costs-airlines-usd14-billion-a-year-regional-airlines-the-fraudsters-carriers-of-choice-48150 adresinden alındı (05.06.2020).

Cebeci, U. (2017). *Bileti iptal etmenin faturası çok ağır.* https://www.hurriyet.com.tr/seyahat/bileti-iptal-etmenin-faturasi-cok-agir-18378945 adresinden alındı (18.06.2020).

Chargeback.com (2020). Industry dispute ratios. https://chargeback.com/ebooks/dispute-ratios-by-industry/ adresinden alındı (25.04.2020).

Clearsale. (2018). Friendly fraud vs. chargeback fraud: can you tell the difference? https://blog.clear.sale/friendly-fraud-vs-chargeback-fraud-the-difference adresinden alındı (08.06.2020).

Cybersource. (2019). Benchmark study: 2018 global airline online fraud management March 2018, https://www.cybersource.com/content/dam/cybs2019/documents/2018-global-airline-online-fraud-management-report.pdf adresinden alındı (05.06.2020).

Dawes, M. (2018, 31 Ağustos). Tips for reducing the top 5 exploits of airline card fraud. Aug 31st, 2018. https://www.aviationpros.com/airlines/blog/12426940/tips-for-reducing-the-top-5-exploits-of-airline-card-fraud adresinden alındı (05.06.2020).

Diker, A. & Varol A. (2013). E-ticaret ve güvenlik. *1st International Symposium on Digital Forensics and Security (ISDFS'13)* (20-21 May 2013). Elazığ, Turkey. ss.29-33.

Elizabeth, S. (2018). Why airline fraud is unique – and what airlines can do about it. Nov 20, 2018. https://blog.clear.sale/why-airline-fraud-is-unique-and-what-airlines-can-do adresinden alındı (05.06.2020).

Elliott C. (2018). These are the most dangerous travel sites in the world. https://www.forbes.com/sites/christopherelliott/2018/08/31/these-are-the-most-dangerous-travel-sites-in-the-world/?sh=280c80234309 adresinden alındı (05.07.2020).

Elliott, C. (2019). Fraud attacks against travelers are taking off and no one is safe. https://www.forbes.com/sites/christopherelliott/2019/10/25/fraud-attacks-against-travelers-rise/#4fa87d113ab4 adresinden alındı (05.06.2020).

Emarketer (2017, 21 Aralık). How digital has transformed the way people travel. https://www.emarketer.com/content/how-digital-has-transformed-the-way-people-travel adresinden alındı (05.03.2020)

Enett (2018). Fraud-in-travel-payments-2018-report.pdf. https://www.enett.com/media/1907/fraud-in-travel-payments-2018-report.pdf adresinden alındı (05.06.2020).

Europol, (2016, 19 Ekim). Global action against airline fraudsters: 193 detained, https://www.europol.europa.eu/newsroom/news/global-action-against-airline-fraudsters-193-detained adresinden alındı (04.06.2020).

Europol, (2016, 20 Haziran). More than 140 detained in global action against airline fraud. https://www.europol.europa.eu/newsroom/news/more-140-detained-in-global-action-against-airline-fraud adresinden alındı (04.06.2020).

Europol, (2017, 13 Haziran). 153 detaine for ticket fraud following woldwide law enforcement operation. https://www.europol.europa.eu/newsroom/news/153-detained-for-ticket-fraud-following-worldwide-law-enforcement-operation adresinden alındı (04.06.2020).

Europol, (2018). Global airport action days. https://www.europol.europa.eu/activities-services/europol-in-action/operations/global-airport-action-days-gaad adresinden alındı (01.05.2020).

Federal Trade Commission (2014, February). Consumer sentinel network data book, for january-december 2013. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf adresinden alındı (15.06.2020).

Feinstein, E. (2019, 29 Ekim). DPO group provides tips to help africa's airline industry guard against fraudulent online payments. Posted, https://www.africanaerospace.aero/dpo-group-provides-tips-to-help-africa-s-airline-industry-guard-against-fraudulent-online-payments.html adresinden alındı (05.06.2020).

Fraud.org (2019,1 Kasım). Scammers ruining travel plans by stealing victims' frequent flyer miles., https://www.fraud.org/frequent_flyer_alert. adresinden alındı (06.06.2020)

Fuscaldo, D. (2018, 20 Eylül). Hackers have a new target: your frequent flyer miles. https://www.forbes.com/sites/donnafuscaldo/2018/09/20/hackers-have-a-new-target-frequent-flyer-miles/#1c07fee31d7f adresinden alındı (06.06.2020).

Haq, R. (2010, 4 Ekim). Emirates employee in air miles fraud scheme. https://www.arabianindustry.com/aviation/news/2010/oct/4/emirates-employee-in-air-miles-fraud-scheme-3750500/ adresinden alındı (06.06.2020).

Helsel, P. (2019, 14 Eylül). Travel agent scammed Delta out of $1.75M in frequent flyer miles, prosecutors say. https://www.nbcnews.com/news/us-news/travel-agent-scammed-delta-out-1-75m-frequent-flyer-miles-n1054436 adresinden alındı (06.06.2020).

https://bkm.com.tr/internetten-yapilan-kartli-odeme-islemleri/ adresinden alındı (03.06.2020).

https://bkm.com.tr/pos-atm-kart-sayilari/ adresinden alındı (03.06.2020).

https://bkm.com.tr/yabanci-banka-kartlarinin-yurt-ici-kullanimi/ adresinden alındı (03.06.2020).

https://bkm.com.tr/yabanci-kredi-kartlarinin-yurt-ici-kullanimi/ adresinden alındı (03.06.2020).

https://bkm.com.tr/yerli-banka-kartlarinin-yurtici-ve-yurtdisi-kullanimi/ adresinden alındı (03.06.2020).

https://bkm.com.tr/yerli-kredi-kartlarinin-yurt-ici-ve-yurtdisi-kullanimi/ adresinden alındı (03.06.2020).

IATA. (2016). News brief: reducing fraudulent payment transactions. https://www.iata.org/en/pressroom/pr/2016-01-07-01/ adresinden alındı (01.03.2020).

IATA (2016). Industry fraud prevention. https://www.iata.org/en/programs/airline-distribution/industry-fraud-prevention-initiative/#tab-1 adresinden alındı (04.06.2020).

IATA (2016). Industry fraud prevention. https://www.iata.org/en/programs/airline-distribution/industry-fraud-prevention-initiative/#tab-3 adresinden alındı (04.06.2020).

IATA. (2019, 11 Aralık). After challenging year, improvement expected for 2020. https://www.iata.org/en/pressroom/pr/2019-12-11-01/ adresinden alındı (22.06.2020).

IATA (2019). Fraud prevention strengthening the defences. https://www.airlines.iata.org/analysis/fraud-prevention-strengthening-the-defences adresinden alındı (06.03.2019).

IATA Perseuss (2020). https://www.iata.org/en/services/finance/perseuss/ adresinden alındı (04.06.2020).

Interpol. Airline ticket fraud. https://www.interpol.int/Crimes/Financial-crime/Airline-ticket-fraud adresinden alındı (05.06.2020).

Interpol, (2019, 27 Kasım). Airline ticket fraud: worldwide crackdown leads to 79 arrests. https://www.interpol.int/News-and-Events/News/2019/Airline-ticket-fraud-worldwide-crackdown-leads-to-79-arrests adresinden alındı (05.06.2020).

John, P. (2019, 3 Nisan). Miles are money... keeping 'loyalty' fraudsters at bay!. https://desktop.gulf-times.com/story/627763/Miles-are-money-keeping-loyalty-fraudsters-at-bay adresinden alındı (06.06.2020).

Kijek, A. (2017). Fast facts about fraud detection in travel business. https://nethone.com/blog/travel-fraud-infographic/ adresinden alındı (01.03.2020).

Levens, S. (2017, 26 Mart). The battle against credit card fraud: cooperation between airlines and law enforcement is key to success. https://www.asi-mag.com/battle-credit-card-fraud-cooperation-airlines-law-enforcement-key-success-2/ adresinden alındı (05.06.2020).

Locke, S. (2018, 7 Ekim). Hackers are now after your air miles to sell on the dark web. https://www.thenational.ae/business/money/hackers-are-now-after-your-air-miles-to-sell-on-the-dark-web-1.777998 adresinden alındı (06.06.2020).

Lustosa, B. (2020, 27 Nisan). The true cost of e-commerce fraud. https://blog.clear.sale/the-true-cost-of-e-commerce-fraud adresinden alındı (05.06.2020).

Mavadiya, M. (2020, 26 Şubat). Buy now, pay later schemes to double their market share by 2023. Forbes. https://www.forbes.com/sites/madhvimavadiya/2020/02/26/buy-now-pay-later-schemes-to-double-their-market-share-by-2023/amp/ adresinden alındı (01.03.2020).

National Fraud Authority (2013). Annual fraud indicator https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf adresinden alındı (15.06.2020).

Özcan, E. (2016). Ödeme sistemleri. https://fintechistanbul.org/wp-content/uploads/2016/08/072_Fintech_Regulasyonlari_Odeme_Sistemleri_EOzcan_BDDK.pdf adresinden alındı (28.05.2020).

Paul, K. (2018, 22 Eylül). How hackers can drain your frequent flyer miles. https://www.marketwatch.com/story/how-hackers-can-drain-your-frequent-flyer-miles-2018-09-20 adresinden alındı (06.06.2020).

Praetsch, R. (2017). Putting email at the core of digital identity. https://www.about-fraud.com/2017/10/12/emailage-core-digital-identity/ adresinden alındı (05.06.2020).

Praetsch, R. (2019, 30 Ocak). Airlines need better anti-fraud data. https://thepaypers.com/expert-opinion/airlines-need-better-anti-fraud-data—7771555 adresinden alındı (05.06.2020).

PSM Payment System Magazine (2014). Türkiye'nin dijital cüzdan haritası. http://www.psmmag.com/haber/turkiyenin-dijital-cuzdan-haritasi/1100575 adresinden alındı (05.06.2020).

Sift (2019). ebook-the-future-of-travel-fraud-fighting. https://pages.siftscience.com/cs-pw-ebook-future-of-travel-fraud-fighting.html adresinden alındı (27.12.2019).

Silk, R. (2020, 2 Mart). Latest targets of fraudsters are hotel and airline loyalty points. https://www.travelweekly.com/Travel-News/Airline-News/Latest-targets-of-fraudsters-are-hotel-and-airline-loyalty-points adresinden alındı (06.06.2020).

Slotnick, D. (2019, 13 Eylül). A man was charged with fraudulently earning more than 42 million frequent-flyer miles worth $1.75 million. Sep 13, 2019. https://www.businessinsider.com/delta-frequent-flyer-miles-fraud-gennady-podolsky-2019-9 adresinden alındı (13.09.2019).

Smith, C. (2014, 2 Temmuz). Chart: shipping costs are a top reason people abandon their shopping cart. Jul 2, 2014. http://www.businessinsider.com/chart-shipping-costs-are-a-top-reason-people-abandon-their-shopping-cart-2014-7 adresinden alındı (10.01.2020).

Smith, M. (2014). Loyalty fraud trends and developments. Travel Payments Insider. March (1). 3-7. https://cf.uatp.com/files/uploads/PDF/Travel-Payments-Insider-Issue1.pdf adresinden alındı (06.06.2020).

Sorrels, M. (2019, 3 Haziran). Travel payments, part 1: beyond credit cards and cash. June 3, 2019. https://www.phocuswire.com/Payments-month-part-1-alternative-payment-models adresinden alındı (05.06.2020).

Sorrels, M. (2019, 10 Haziran). Travel payments, part 2: balancing friction and risk in fighting fraud. June 10, 2019. https://www.phocuswire.com/Payments-month-part-2-fraud adresinden alındı (05.06.2020).

Şekerli, E. B. (2019). Ticari havayolu taşımacılığı sektöründe makine öğrenmesi uygulamalarının incelenmesi. *Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi.* 22 (2), 405-419.

TCMB (2014). *Ödeme sistemleri Türkiye'de ödeme sistemleri*. Ankara.

The Guardian (2004). Airport worker jailed for air miles fraud. https://www.theguardian.com/business/2004/jun/03/theairlineindustry.uknews adresinden alındı (06.06.2020).

The Nison Report (2018). https://nilsonreport.com/upload/pdf/Payment_Card_Fraud_Losses_Reach_.pdf adresinden alındı (03.06.2020).

The Nilson Report (2019). https://nilsonreport.com/upload/pdf/Payment_Card_Fraud_Losses_Reach_.pdf adresinden alındı (03.06.2020).

TÜİK hanehalkı bilişim teknolojileri kullanım araştırması, 2011-2019. http://www.tuik.gov.tr/PreTablo.do?alt_id=1028 adresinden alındı (03.06.2020).

UK Finance (2019). Faud The Facts 2019. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf adresinden alındı (04.06.2020).

Ünlü, U. (2018). İnternet bankacılığı sisteminde tüketicilerin karşılaşacağı olası saldırılar ve çözüm önerileri. *Bankacılar Dergisi*. 104, 82-96.

Visa (2014). Managing payment card fraud a guide for airlines. http://www.aeropay.eu/wp-content/uploads/2017/07/visa-airline-fraud-guide.pdf adresinden alındı (05.06.2020).

Visa (2018) Loyalty fraud management. https://www.visa.com.co/dam/VCOM/regional/lac/SPA/Default/Documents/PDFs/loyalty-fraud-management-01.pdf adresinden alındı (10.04.2020).

World Payments Report (2019). https://worldpaymentsreport.com/ adresinden alındı (19.06.2020).

Worldpay (2019). Global payments report. http://offers.worldpayglobal.com/rs/850-JOA-856/images/Global%20Payments%20Report_Digital%202018.pdf adresinden alındı (19.06.2020).

Worldpay (2020, January) Global Payment Report. http://offers.worldpayglobal.com/rs/850-JOA-856/images/GPR-2020.pdfmkt_tok=eyJpIjoiWm1SalpEUXhOelEyWkdZeiIsInQiOiJXbXVmdHZ4OFJuNXlyM2cxbWRMUGliZThRU044RnBQbUVZdGJkdDNrdUxkMU1SSGl3NmRGOVFsSXhlRDVuV1dvNXFaSTVra2ZJZFFZWmI4SUN3R0ZkQ3h2M2IrUktLOHcrZGhBaHduN2FidmlPRWpNYlBLMFJmYUFUaXpPQ0ZzYiJ9 adresinden alındı (27.06.2020).

Yalçın, F. (2018). Mobil cüzdan dünyası ve en sık kullanılan uygulamalar. https://fintechistanbul.org/2018/08/31/mobil-cuzdan-dunyasi-ve-en-sik-kullanilan-uygulamalar/ adresinden alındı (01.06.2020).

Yeşilyurt H. (2015). Finansal hizmet sektöründe siber güvenlik riskleri ve çözüm yolları: ödeme sistemleri ve tedarik zinciri bütünlüğü. *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*. 13 (2), 97-120.

Yılmaz, A. (2015). Türkiye'deki dolandırıcılık tipolojileri: dolandırıcılık olaylarının kategorik tasnifi ve yapılış şekilleri. *Hacettepe Üniversitesi Sosyolojik Araştırmalar E-Dergisi*. 12, 1-24. https://www.researchgate.net/publication/301565138_Turkiye'deki_Dolandiricilik_Tipolojileri_Dolandiricilik_Olaylarinin_Kategorik_Tasnifi_ve_Yapilis_Sekilleri_The_Fraud_Typologies_in_Turkey_The_Categorical_Classifications_and_Methods_of_Frauds adresinden alındı (23.12.2019).

Zengin, B. & Güngördü, A. (2013). Elektronik ödeme sistemlerinin olası etkileri üzerine bir inceleme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*. 15 (3), 129-150

SUGGESTIONS ON ASSESSMENT OF EFFECTS OF FRAUDULENT TRANSACTIONS MADE THROUGH PAYMENT SYSTEMS ON AVIATION SECTOR AS WELL AS INSPECTION AND PREVENTION OF SUCH TRANSACTIONS

Zekeriya DEMİR *

The aviation sector is greatly important for the world economy thanks to the employment and the economic magnitude and value-added it provides. According to the IATA data, the sector provided employment for over 10 million people directly and 65.5 million people indirectly, produced a turnover of 885 billion dollars directly and 2.7 trillion dollars indirectly, and carried 4.6 billion people and 66 million tons of cargoes in 2018. The increase in the varieties of the financial instruments and payment systems the sector uses due to its abovementioned magnitude has brought new fraud risks in its wake. This study handles the frauds committed in the aviation sector through the payment systems that have become more important due to the developing technology and changing consumer behaviors, the effect of these frauds on the sector, and the efforts intended for the inspection and prevention of these frauds.

Fraud is not a fact specific to the present day and certain sectors, but instead changes by time and place. ACFE's Fraud Report of 2020 estimates that fraud and deceit committed by employees amount to 3.6 billion dollars, that the businesses lose almost 5% of their annual revenues to such deceit and fraud, and this costs the world economy almost 4.5 trillion dollars a year. IATA estimates US$ 858 million annual financial loss in the sector caused by fraud. For a sector where the average profitability is about 3%, it is obvious how serious the effect of the fraud-induced losses on the financial statements is.

Fraud is not only ethical but also a legal matter, thus, it is regulated by laws in numerous countries. In Turkey, the fraud crimes are regulated by Turkish Criminal Code Number 5237. According to the last five years' data (2014-2018), a rise is observed in the number of crimes committed through

* Turkish Airlines Inc., Accounting and Financial Control Directorate

Received: 16.07.2020
Accepted: 23.10.2020

payment systems and the relevant cases as well as the number of the conviction verdicts adjudged in Turkey.

Numerous institutions try to prevent fraud in the aviation sector; IATA, in particular, ACTA, Europol, Interpol, and the credit card companies like Visa are some of them. At this point, it is impossible for any one of them to prevent frauds in the sector alone; and it is obvious that a serious inter-institutional cooperation is necessary.

In the aviation sector, offering the customer the right payment system alternatives is not less important than reaching the customer through the right sales channels. When we look at the payment methods accepted by the sales channels in the sector, we see that the global credit cards and bank cards top the list with a very high rate like 99% and are followed by PayPal and the other electronic purses by 58%, which are followed by UATP, bank transfers, country – or region-based credit cards, cash on delivery, payment with mobile phone, electronic cheque, ACH (Accounting Clearing House), automatic payment, gift cards, and Western Union. In addition to them, there are also regional payment alternatives like M-Pesa, Uplift, and Klarna. Besides, the mileage, gift cards, and traveler's cheques distributed to increase the customer loyalty can also be used as payment instruments.

As is the case with numerous sectors, frauds have increased and continue to increase in connection with the increasing number and volume of the payment systems in the aviation sector as well. The aviation sector is both attractive and defenseless for the fraudsters. The reasons of this attractiveness and defenselessness can be listed as high-value products, global access and digital anonymity, fast consumption, weak protection barriers, low profit margins, and the number and diversity of suppliers. In 2018, the cost of fraud in the travel sector was 21 billion dollars, and this amount is anticipated to exceed 25 billion dollars in 2020. In addition to its direct costs, fraud also has indirect costs, which are deemed to be 2.5 times the direct costs. The digital travel expenditures, which amounted to 676 billion dollars in 2018, are expected to reach 855 billion dollars in 2021. As can be seen, this fast growth in the digital channels constitutes a potential risk area for fraudulent and deceitful transactions. Therefore, it is necessary to take serious steps towards investigation and prevention of the payment system frauds. In the aviation sector, 1 – 1.5% of the total revenue is under the fraud risk, and in certain markets like the Middle East and Latin America, this figure can go up to 3 – 4% of the revenue.

In the world, the amount of the credit card frauds reached 27.85 billion dollars in 2018 and is anticipated to reach 35.67 billion dollars in five years and 40.63 billion dollars in 10 years. Visa specifies that the airline companies managing the fraud risk well perform 6 points higher than the sector average, but the rates are high for most of the airline companies, and much higher through insecure e-trade channel. Another important source of corruption in the sector is chargeback fraud; it is estimated that more than half of the businesses lost revenue by 11 to 50 base points in 2018 due to this reason, and 22% of the businesses lost revenue by more than 50 base points. Since people share

more data with airlines, hotels, or car rental companies as their travel habits increase and become diversified, the payment system risk of capturing of the personal data also rises. In terms of capturing of the personal data, the aviation sector is regarded as the riskiest sector in this area by 61%.

It is estimated that there is 23.8 trillion of unused miles in the sector as of the year 2019, the money equivalent of which is estimated to be 238 billion dollars. An area that includes such big amounts and generally known to be easier than capturing the credit and bank card data is regarded as an important potential for fraudsters. Although the dimensions of this type of fraud is not known exactly, it is estimated that this amount is about 1 billion dollars in 2017, and 1% of the airline mile usage across the world is fraudulent.

According to the sector experts, airline companies fall victim to payment fraud every three minutes. Therefore, fraud is a serious problem the airline companies must deal with. However, very restrictive rules in the measures taken against fraud might cause a risk of decline in sales, while keeping the rules very loose might increase the costs due to chargeback. The system and set of rules to be established must be designed to strike the balance between these two possibilities.

The path to follow to prevent payment system frauds in the aviation sector can be as follows:

- Establishment of a General Control System to cover All Sales Channels
- Development of Risk Analysis Methodology
- Establishment of User Accounts Management and Passenger Information System
- Use of New Technological Infrastructures
- Coordination, Training & Cooperation

To sum up, development and spread of the payment systems increase the risks of payment system frauds, and fighting these risks is becoming harder and more complicated with each passing day. In order to be able to prevent, inspect, and manage these risks, it is suggested that the airline companies;

- Invest more in the IT infrastructures to ensure data compliance, conformity, and information security,
- Cooperate with cyber security experts to detect the security gaps of the systems they use and protect the customer information,
- Use talk and voice recognition systems, the airline companies making sales through call center especially,
- Establish a comprehensive reporting system to be able to manage the fraud risk,
- Use virtual credit cards (VCC) and virtual account numbers (VAN) that are more secure against the fraud risk,

- Support information and awareness trainings given to both the employees and the customers in relation to online attacks,
- Cooperate with all stakeholders against the fraud risk,
- Take additional security measures in flight transactions for the regions and countries where the fraudulent transactions concentrate,
- Build a well-trained and experienced anti-fraud team,
- Establish internal control system and internal inspection department that function well and effectively,
- Outsource through the firms that have good sectoral experience about fraud.

The measures to be taken among the abovementioned ones must be selected as per each company's own internal need analysis, because if the need cannot be determined correctly, the companies may have to bear inadequate or excessive investment or cost.