Bankacılık Hileleri: Sınıflandırılması, Saptanması ve Önlenmesi

***Canol KANDEMİR*[1]**
***Şenol KANDEMİR*[2]**

Öz

Bankaların ulusal ve küresel ekonomideki artan güç ve yetkisi hilekarlar tarafından kötüye kullanılmış ve dolayısıyla söz konusu kuruluşlar hile girişimlerinin önde gelen hedeflerinden biri durumuna gelmiştir. Bankacılık hilelerinin neden olduğu maliyetlerin etkili hile saptama ve önleme politikaları ve uygulamaları yardımıyla azaltılmasının sosyal ve ekonomik refaha olumlu yansıyacağı, bireylerin ve kurumların yaşamları ve sürekliliklerine önemli katkı sağlayacağı düşünülmektedir. Son tahlilde, bankacılık hileleri ile mücadele etmek için hem insan, hem de makine gücünü en önemli savaşçılar olarak bütünleştiren makro bir politikanın belirlenmesi, insan ve teknoloji bileşenlerinin eğitim ve yenileşme yoluyla hile riskine karşı sürekli uyarılması, geleneksel ya da çağdaş hiçbir strateji ve yöntemi dışlamadan sürekli ve hareketli hedefler konumundaki hilelere ve hilekarlara karşı nokta savunması yapmak yerine alan savunması yapılması, potansiyel hile alanının çok hatlı ve katmanlı olarak düzenlenmesi ve böylelikle hileler ile belirli hatlarda verilecek tek tek yerel savaşların değil, alanın tümünde (hile ortamı) tüm hilelere karşı verilecek topyekûn savaşın kazanılmaya çalışılması önerilmektedir.

Anahtar Kelimeler: *Hile Türleri, Hile ile Mücadele Stratejileri ve Yöntemleri, Elektronik Hileler, Kredi Hileleri, Çek Hileleri (JEL Sınıflandırması:M41, M42, G21)*

Banking Frauds: Classification, Detection and Prevention

Abstract

The rising power and influence of banks within the national and global economy has been abused by fraudsters and made them one of the leading targets of fraud attacks. It is considered that reducing the losses due to banking frauds with the support of effective fraud detection and prevention policies and applications will favorably affect social and economic wealth and make a significant contribution to the life and sustainability of individuals and corporations. In the final analysis, for the purpose of fighting banking frauds it has been suggested to form a macro policy integrating both man and machine power as the most essential combatants, continuously alert people and technologies to the risk of fraud by way of education and innovation, make a zone defence instead of a point defence against frauds and fraudsters as permanent and moving targets without excluding any strategy and method whether they be traditional or contemporary, organize the potential fraud environment in a multi-layered and faceted manner and thus try to win the total war against all frauds waged in the whole battlefield (fraud environment), not the local wars waged in each frontline against individual frauds.

Keywords: *Types of Frauds, Strategies and Methods for Combatting Frauds, Electronic Frauds, Loan Frauds, Cheque Frauds (JEL Classification:M41, M42, G21)*

[1] Yrd. Doç. Dr, T.C. Çağ Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası Finans ve Bankacılık Bölümü,
ckandemir@cag.edu.tr
ORCID ID: 0000-0003-2373-0885

[2] Yrd. Doç. Dr, T.C. Çağ Üniversitesi, Hukuk Fakültesi,
senolkandemir@cag.edu.tr
ORCID ID: 0000-0002-7621-4457

Giriş

Bankalar toplum, işletmeler, tüketiciler ve devlet için önemli ve çok özel kurumlar konumundadır, çünkü para yaratma, kredi verme, yatırımları değerlendirme, uluslararası ticareti kolaylaştırma ve vergi ödeme gibi yaşamsal ekonomik işlevleri yerine getirmektedir. (Benston, 2004:15-7 ve 21-2) Bankalar faaliyette bulunurken diğer tüm işletmelerde olduğu gibi aslında bir imtiyaz hakkını kullandıkları için güven kurumu olmaları giderek önem kazanmaktadır, çünkü bankalar fon arz edenler ve kullananlar arasında etkili biçimde konumlandığından borç verenler (mevduat sahipleri) adına borç alanları gözetim altında tutmakla yetkilendirilmiştir. Bankaların toplumun güvenini kazanmaları için söz konusu sorumlulukları doğruluk ve hileden uzak biçimde yerine getirmeleri gerekmektedir. Bankaların aracılık rollerini başarılı bir şekilde yapamamaları ise, bugüne kadar tanık olunan bazı finansal krizlerde yaşanan temel bir sorun olmuştur. Bu nedenle, toplum bankalardan daha çok hesap vermesini, işini doğru yapmasını, saydam olmasını ve etkin aracılık hizmeti vermesini beklemektedir. Bankaların bu rollerini yerine getirmelerini engelleyen gerçek risk ve tehditlerden biri de hileler olmaktadır. Gerçekte, hile küresel bir olgudur ve belli bir sektöre ya da ülkeye de özgü değildir. Bununla birlikte bankalar parayla faaliyette bulunan kuruluşlar olduğu için kararlı hilekarların hedefi olması beklenmeyen bir durum sayılmamaktadır. (Idolor, 2010:63-5)

Banka ve özellikle büyük banka iflâslarının en önemli nedenlerinden biri, iktisat tarihinde de birçok kez görüldüğü gibi, bankacılık hileleri olmuştur. (Benston, 2004:24-5) Nitekim finansal sektörün usülsüzlük ve görevi kötüye kullanma niteliğindeki birçok yıkıcı ve daraltıcı faaliyeti emeklilik fonları için eksi getirilere, kaynakların yanlış dağıtımına ve skandallara yol açmıştır. Yinelenen skandallar ve piyasa yetersizlikleri sadece bireysel finansal hizmetlerde değil, tedarik zincirinin her aşamasında (*yatırım bankacılığı ve kurumsal fon yönetimindeki çıkar çatışmaları, libor manipülasyonu gibi*) yaşanmaktadır. Kurumsal piyasalardaki başarısızlıklar sıradan bireysel müşterilere bulaşmakta, bireysel müşterilere yanlış finansal ürünlerin satılması ise dönüp banka bilançolarını etkilemektedir. (Wehinger, 2013:79-80) Nitekim bankalar, tasarruf sahiplerini dolandırmanın ve vergi yükümlüleri üzerine maliyetler yüklemenin etkili araçları olarak kullanılabilmiştir. Özellikle kamu mülkiyetinde ya da denetiminde olan bankalar, hükümetin himaye ettiği kamu ya da özel işletmeleri sübvansiyonlu kredilerle destekleyebilmiştir. Dürüst olmayan ve fırsatçı bankacılar siyasî destek, kişisel himaye ve rüşvet karşılığında kamudan etkisiz denetim ve gözetim görmüştür. Bu tür bir davranış biçimi bankalara özgü değildir, ancak tasarruf sahiplerinin devletin açık ya da kapalı tasarruf sigortası güvencesi vermesi ile zarardan korunacağına inandığı koşullarda bankacıların tasarruf sahiplerinin paraları üzerindeki kontrolü ile daha da kolaylaşmaktadır. (Benston, 2004:21-3)

Bankaların toplum, devlet ve ekonomiler için giderek artan önemi göz önünde bulundurulduğunda, bu sektörün faydalarını arttırıp maliyetlerini azaltmaya katkıda bulunacak düzenleme ve çalışmaların yapılması gerekliliği ortaya çıkmaktadır. Bu bağlamda, bankacılık hileleri sektörün etkinliğini bozan, faydalarını belirli ellerde toplayan ve fakat maliyetlerini tüm topluma yükleyen bir sorun alanı oluşturmaktadır. Dolayısıyla, sözü edilen hilelerin sayı ve maliyet olarak azaltılması için öncelikle bankalara yönelik yarattığı tehditlerin açık ve belirgin biçimde ortaya konması ve bu amaçla sistematik olarak sınıflandırılması zorunluluğu bulunmaktadır. Kendilerine yönelen yakın ve uzak tehditleri gören ve bilen bankalar doğru strateji ve taktikler belirleyerek doğru yığınak ve konumlandırma yapabilmekte ve hilelere karşı topyekûn savaşı kazanma olasılığını arttırabilmektedir. Doğru bir sınıflandırma sonrasında kullanılacak savunma kuvvet ve araçlarının belirlenmesi için ilgili muhasebe, bankacılık ve ödeme teknolojileri yazınına başvurularak geleneksel ve çağdaş hile saptama ve önleme stratejileri ve yöntemleri açıklığa kavuşturulmuş, son aşamada da anılan strateji ve yöntemlerden etkili, bütünleşik, çok katmanlı bir makro hile yönetim politikası oluşturulması amaçlanmıştır.

1. Bankacılık Hilelerinin Genel Özellikleri

Hilelerin önemli bir bölümü (%66,4) halka açık olan ve olmayan özel şirketlerde yapılmaktadır. Bankacılık ve finansal hizmetler sektörü, kamu kuruluşları ve imalat sanayileri ile birlikte hile olaylarının en çok görüldüğü sektörler arasında gelmektedir. Yalnızca bankacılık ve hizmet sektöründe hile olaylarının %17,8'i gibi göreli küçük bir bölümü saptanmış, ancak söz konusu sektör ima-

lat ve sağlık sektörleriyle birlikte hilenin yol açtığı (*medyan*) kayıplar açısından orta düzeyde zarar gören sektörler arasında yer almıştır. Bankacılık ve finansal hizmetler sektörü, hileler içinde finansal raporlama (*financial reporting fraud*) ve varlıkların kötüye kullanılması (*asset misappropriation*) hilelerinden çok yolsuzluk (*corruption*) olaylarının en sık meydana geldiği sektörler arasında geçmektedir. Nitekim bu sektörde Tablo 1'de de görüldüğü üzere, hile olaylarının ağırlıklı bir bölümü yolsuzluk olayları ve nakit ile ilgili hilelerden kaynaklanmıştır. (ACFE, 2014:4, 24-30) Ülkeler özeline inildiğinde, 2013 yılında İngiltere'de Eylül sonu itibariyle %34 artışla 201.035 hile kayıtlara geçirilmiştir; genel suçlar %15, şiddet içeren suçlar %22 azalırken hile olayları %25 artış göstermiştir. (CFS, 2014:3) ABA'nın (*American Bankers Association*) mevduat hesabı hilesi araştırmasına göre, ABD'de 2012 yılında bankaların %96'sı banka kartları ile yapılan hilelerden, %63'ü çek hilelerinden dolayı zarara uğramıştır. Toplam mevduat hilesi kayıplarının %54'ü banka kartı hilelerinden, %37'si çek hilelerinden ve %9'u diğer hilelerden (*mobil bankacılık, telefon bankacılığı, elektronik bankacılık*) kaynaklanmıştır. (Mazur, 2014:11) Finansal kuruluşlardaki yanlışlıklar diğer sektörlerdeki yanlışlıklardan farklılaşmaktadır. Nitekim likidite hesapları açısından yanlışlık oranları bankacılıkta diğer sektörlerden önemli oranda yüksek bulunmuştur. Aynı şekilde, banka, tasarruf ve kredi kuruluşları net kârı olduğundan %68 daha yüksek göstererek finansal tablolarda en çok yanlışlık yapan kuruluşlar arasında gelmektedir. (Boumediene, 2014:422, 425) 36 banka ve 14 kredi kuruluşunu içeren bir araştırmada da, kredi kuruluşlarının net kârı yüksek gösterme hilelerini en çok yapan kuruluşlar arasında olduğu bulunmuştur. (Green ve Reinstein, 2004:92)

Tablo 1. Bankacılık Hilelerinin Görülme Sıklığı (%)

Nakdi Hileler	37,7
Yolsuzluk	37,3
Ayni Hileler	13,1
Finansal Raporlama Hileleri	10,2
Harcama Hileleri	6,6
Çek Hileleri	5,7
Fatura Hileleri	5,7
Ücret/Bordro Hileleri	5,3

Öte yandan, banka hilelerini dış (k*art ve atm hileleri gibi*) ve iç (*banka çalışanlarının işbirliği ile yapılan*) olarak ikiye ayıran başka bir çalışmaya göre, bankacılıkta en çok yapılan hileler sırasıyla kredi kartı hileleri (%51), ATM hileleri (%45), finansal tablo hileleri (%34), varlıkların kötüye kullanılması hileleri (%28), rüşvet (%13) ve hırsızlık (%7) olmuştur. En çok hile yapılan banka birimleri ise Tablo 2'de verilmiştir. (Nabhan ve Hindi, 2009:17 ve 33) Banka hileleri hem banka çalışanı olan, hem de olmayanlar tarafından yapılabilmektedir. Hile yapan banka çalışanları muhasebeci, şefler, yönetici asistanları ve hizmetliler gibi asıl bankacılık faaliyetleriyle uğraşmaktadır. Bazen banka çalışanları ve hilekarlar arasında işbirliği söz konusu olmaktadır. (Balogun vd, 2013:255) Banka çalışanlarının hilekarlar ile işbirliği gerçek bir tehdit oluşturmaktadır, çünkü personel banka sistemlerine ve müşterilerin kişisel bilgi ve kayıtlarına doğrudan erişim yetkisine sahip bulunmaktadır. (Usman ve Shah, 2013:4) Bu tür hilelerde hilekar genellikle bankanın içinde olmaktadır ve işlenen suçlar bireylerin değil, örgütlü ağların bir faaliyeti biçimindedir. (Buchanan, 2010:58)

Tablo 2. Bankacılık Hilesi Yapılan Birimler (%)

Bireysel Bankacılık	52,0
Yatırım	37,3
Kurumsal Bankacılık	26,0
Operasyon	22,0
Ticari Finansman	15,0
Risk Yönetimi	5,0
Finans	4,0
Diğer	7,0

Bankacılık hilelerinde zaman içinde ciddi bir değişim yaşanmıştır. Bu çerçevede, (1979-87) ve (1988-96) dönemleri hesaplar temelinde karşılaştırıldığında, görülme sıklığı açısından ticari alacaklarla ilgili hilelerin %9,68'den %0,00'a, kredilerle ilgili hilelerin %38,71'den %21,21'e, gelir ve giderler ile ilgili hilelerin %38,71'den %15,15'e gerilediği; öte yandan nakit ile ilgili hilelerin %9,68'den %12,12'ye, menkul kıymetlerle ilgili hilelerin %41,94'den %54,56'ya ve kredi karşılıkları ile ilgili hilelerin %41,94'den %48,48'e yükseldiği, hile büyüklüğünün gelir ve giderler dışında düştüğü belirlenmiştir. Banka hilelerinin özellikleri, bankalar ve kredi kuruluşlarıyla ilgili yeni yasal düzenlemeler ve genel olarak finansal tablo

hilelerini ortaya çıkarmak için yapılan yeni standartlar dolayısıyla değişime uğramış, sonuç olarak artan kamu gözetimi hile stratejilerini farklılaştırmış ve en sonunda fiktif bilgiler yaratmaktan çok gerçek bilgilerin ele geçirilmesine yöneltmiştir. Banka hilelerinin yapılma sıklığında bir değişiklik yaşanmamış, ancak hile yöntemi ve büyüklüğü bakımından önemli bir değişim yaşanmıştır. Önceleri hilekarlar fiktif bilgi uydurarak ya da gerçek bilgiyi saklayarak hile yaparken sonraları daha edilgen biçimde bilgi saklayarak hile yapmaya başlamıştır. Bu durum artan kamu ve düzenleyici kuruluş ilgisi, ilgili standartların sektöre özel yol göstericiliği ve diğer sektörel açıklama kurallarından kaynaklanmış görünmektedir. Hile özellikleri ve türlerindeki değişiklikler, geçmişteki saptama çabalarına bir tepki olarak değerlendirilmiştir. Mesleği bankacılık olan hilekarlar geçmişteki yanlışlar ve başarısızlıklardan öğrenmekte, kendi özel tekniklerini geliştirmekte ve değişen kural ve düzenlemelere uyum göstermektedir. (Green ve Reinstein, 2001:87, 97 ve 104-5) Suçlular güvenlik önlemlerinin çevresinden dolanabilme konusunda esnek olduklarından bankalar, kredi kartı çıkaranlar ve satıcılar yeni koşullara uyum sağlamaya zorlanmaktadır. (Buchanan, 2010:58) Hilekarların mevcut koşullar ve ortama bağlı olarak yöntemlerini ve hedeflerini uyarlama esnekliği, hilelerin yeni sektörlere sürekli bir göç hareketi içinde bulunmasından da anlaşılmaktadır. Nitekim 2009'a göre daha az banka hesabı (%15) ve plastik kart (%37) hilesi yapılmış, ancak bu azalış telekomünikasyon araçlarındaki (%30) ve posta yoluyla siparişlerdeki (%34) artışlar ile dengelenmiştir. (Ash, 2011:17) Geçen 10 yılda banka soygunu ve çek hileleri de azalış eğilimindedir, ancak siber suçlar artıştadır. Finansal işlemler nakitten çeklere ve elektronik transferlere kaydıkça, suçlular da aynı şekilde yer değiştirmiştir. Yalnızca soyguncular açısından paranın biriktirildiği bir yer olduğu için değil, genç ve akıllı hırsızlar için daha büyük miktarlarda parayı eskisinden daha kolay ve hızlı biçimde elde edebildiği bir yer olduğu için de bankalar hedef alınmaktadır. Nitekim 2000'lerin sonlarına doğru elektronik bankacılıkla ilgilenen suçlular ticari hesapları ele geçirmeye yönelmeye başlamış, bunun için kullanılan oltalama (*phishing*), zararlı yazılımlar (*malwares*) ve diğer teknikler sürekli evrim geçirmiştir. (Scania ve Ludwig, 2013:3)

2. Bankacılık Hilelerinin Temel Nedenleri ve Sonuçları

Bankacılık en sıkı düzenlenen sektörlerden biri olmasına karşın sermaye sağlamak ve kaynaklara aracılık etmekteki rolü bakımından hilekarlar için en uygun çekim merkezi ve hedefi olarak kalmayı sürdürmüştür. (Rahman ve Anwar, 2014:97-8) Finansal hizmetler sektöründeki kuruluşlar iki temel nedenle hilelerin hedefi olmaktadır. İlk olarak, söz konusu kuruluşlar tarafından yönetilen finansal varlık havuzunun büyüklüğüne bağlı olarak bunlar önemli büyüklükte finansal ödüllerin var olduğu bir ortam oluşturmaktadır. İkincisi, kuruluşların içindekiler (*insiders*) ve özellikle üst yönetim, finansal varlık havuzları üzerindeki yasal kontrol yetkilerini hile yapmak ve bunun ortaya çıkarılmasından korunmak için kullanabilmekte, başka bir anlatımla kontrol yetki ve görevlerinin kendilerine sunduğu fırsatlarından yararlanabilmektedir. Nitekim büyük finansal hileler, bu tür üst düzeyde örgütsel yetkilere sahip olanlarca gerçekleştirilmektedir. (Drew ve Drew, 2010:54-5)

Bankacılık hilelerinin temel nedenleri arasında yetersiz iş eğitimi, mevcut personel üzerinde aşırı iş yükü, rekabet, kamunun düzenlemelerine düşük uyum düzeyi, yetersiz iç kontrol sistemleri, görevli personelin yolsuzluğa eğilimli olması ve uygunsuz istihdam politikaları sayılmaktadır. Hilenin yapılmasının ana nedeni, kontrol ve gözetim ile görevli personel tarafından yerleşik sistem ve kurallara uyulmasında yaşanan gevşeklik ya da ihmâl olarak değerlendirilmektedir. Kayıtsızlık ve bilgi açığı ise, kurallara uymamanın iki temel nedeni durumundadır. Bu bağlamda, ekonomik liberalleşme ve finansal sektörlerde yapılan reformlarla birlikte yeni özel bankalar rekabet yaratacak biçimde bankacılık piyasasına girmiş, mevcut nitelikli müşteriyi çekmek için rekabet etme zorunluluğu ise gelenekselleşmiş ve sınanmış sistem ve kuralların gevşetilmesine neden olmuştur. Yoğun rekabet, görevli banka çalışanlarını gevşetilmiş sistem ve kurallar ile çalışmaya zorlamıştır. Sistemin gevşetilmesine ve kuralların esnetilmesini fark eden etik dışı banka içi ve dışı hilekarlar bu durumu kötüye kullanabilmektedir. (Kanna ve Arora, 2009:1-3, 8-9) Banka çalışanlarının işyerinde eşitsizlik ve iş güvencesizliği algılamaları ile yasal yollarla ulaşılabilecek fırsatların eksikliği ya da yokluğu

onların hileye yönelik eğilimlerini arttırabilmekte ve suç davranışına itebilmektedir. Hilekarların savurgan ve gösterişli yaşam biçimlerine özenmeleri de hileli davranışı uyarabilmektedir. (Balogun vd, 2013:255) Bu durum hilenin meydana gelmesinde teknolojinin ötesinde başka faktörler olduğunu düşündürmektedir. (Usman ve Shah, 2013:4)

Başka bir çalışmada bankacılık hilelerinin birincil ve ikincil nedenleri 7 kategoride incelenmiştir. (Idolor, 2010:62, 68-9, 74-5) Bu çerçevede, açgözlülük (*greed, bireylerin kendi geliri ya da yakın ve uzak ihtiyaçlarının üstünde kazanmak ve bolluk, savurganlık ve ihtişam içinde bir yaşam sürmek amacıyla hızla zenginleşmek için duyduğu içsel ve hastalıklı güdü*) bankacılık sektöründeki birçok hilenin en önemli nedeni olarak görünmektedir. İkinci olarak, yetersiz (*niteliksiz ve deneyimsiz*) insan gücü (*personel*) bankaya iş planlaması ve görevlerin dağıtımında sorunlar çıkarmakta ve bu durum bankanın günlük işlemlerinde hilekarlar tarafından kötüye kullanılabilmektedir. Üçüncü olarak, yetersiz iç kontroller banka çalışanı, müşterisi ya da müşterisi olmayanlar tarafından kötüye kullanılabilecek bir zayıflık oluşturmaktadır. Dördüncü olarak, banka çalışanlarının bankacılık faaliyetlerinin hem teorik, hem de teknik yönleri konusunda yeterli biçimde eğitilmemesi ya da sürekli eğitimden geçirilmemesi bankaların genel olarak performansını düşürmekte ve bu da hilekarlar tarafından kolaylıkla kötüye kullanılabilecek bir ortam yaratmaktadır. Beşinci olarak, hesapların ve defterlerin düzenli biçimde tutulmaması ve dönemsel hesap mutabakatlarının yapılmaması özellikle banka çalışanları tarafından kötüye kullanılabilmektedir. Altıncı olarak, anababalardan çocuklara kalıtım yoluyla geçen özellikler hile risk faktörleri arasında sayılmaktadır. Son olarak, banka personelinin payına düşen ücret ve benzeri ödemelerin yetersiz düzeyde olması, hileli bir şekilde el konulan malların paraya çevrilmesinin kolaylığı, konulan kurallara uyulmamasının cezasız ve yaptırımsız kalması, banka varlıklarını ve çıkarlarını korumakla görevli olan ilişkili kurumların gizlice anlaşması, olumsuz çalışma koşulları, çalışanların yoksulluk ve sadakatsizliği gibi diğer nedenler belirtilmektedir.

Banka hileleri bankaların kurumsal büyümesini tehlikeye atmakta, fon sahiplerinin mevduatlarını kaçırmakta, bankaların sermaye tabanını eritmekte, sonuçta gelir, müşteri ve itibar kaybı oluşmaktadır. Banka hilelerinin en önemli sonucu ise, müşterilerin güveninin kaybolmasıdır. (Idolor, 2010:69) Buchanan da (2010:59), hilenin neden olduğu kayıpların bankanın itibarını ve markasını olumsuz etkilediğini belirlemiştir. Görüldüğü gibi, hilenin yol açtığı kayıplar sadece finansal nitelikte olmayıp itibar ve güven kaybı nedeniyle düşen satışlar da bu kapsamda değerlendirilmektedir. (Excell, 2012:8) Dar anlamda, hileler dolayısıyla bankalar yalnızca sermaye ve itibar kaybetmemekte, iflâs riskine de daha açık duruma gelmektedir. Geniş anlamda ise, hileler salt kaybedilen yatırımcılar ve kaynaklar nedeniyle ülkenin ekonomik durumunu tehdit etmemekte, aynı zamanda ekonomik istikrarsızlık yoluyla siyasal istikrar ve barışı tehlikeye atmaktadır. (Rahman ve Anwar, 2014:98) Öte yandan, bankacılık hilelerinin önemli finansal sonuçları olmaktadır. Nitekim kredi müşterisi şirketlerin düzenleyici kuruluşlardan hile dolayısıyla aldıkları cezalar banka ve şirketler arasındaki sözleşme ilişkilerini etkilemekte, kredi riski ve banka kredilerinin bilgi riski bu çerçevede artmakta ve bankaların kredi politikasını değiştirmektedir. Banka, şirketlerin gelecekteki nakit akımları ve gelir istikrarı konusunda şüpheye düşmekte ve bu nedenle şirketlere ödünç vereceği kredi miktarını azaltarak faiz oranlarını yükseltmektedir. Aynı şekilde, hile yapmayan şirketler ile karşılaştırıldığında, hile yapan şirketlerin kredileri daha az yenilenmektedir. Sonuç olarak, hile olayları şirketlerin borç finansmanı elde etme yeterliliğini azaltmakta, hile yapan şirketlere düzenleyici kuruluşlardan aldığı cezalara ek olarak ikinci bir ceza (*daha az kredi ve daha yüksek faiz oranı*) verilmiş olmaktadır. (Yunsen vd, 2011:163-4)

Hilelerin bankalara ve topluma önemli maliyetler yüklediği anlaşılmaktadır. Örneğin ABA'nın mevduat hesabı hilesi araştırmasına göre, ABD'de yalnızca banka hesaplarına karşı yapılan hilelerin sektöre toplam maliyeti 2012'de 1,744 milyar sterlin olarak gerçekleşmiştir. (Mazur, 2014:11) PwC (*PricewaterhouseCoopers*)'nin 40 ülkede 2007 yılında yaptığı çalışmaya göre de, şirketlerin %43'ünün ekonomik suçlardan dolayı son iki yılda 4,2 milyar dolar zarara uğradığı ve iç kontrol eksikliklerinden dolayı da 5,7 milyar dolar hilenin ortaya çıkarılmaması maliyeti olduğu belirlenmiştir. (Nabhan vd, 2009:15) Elektronik ticaret hacminin sürekli artmasına bağlı olarak internet tacirlerinin ve kart çıkaran bankaların uğradığı kayıpların 2005'de 5-15 milyar dolar arasında olduğu

ve toplam içinde %0,8-0,9 pay oluşturduğu tahmin edilmiştir. (Quah ve Sriganesh, 2008:1721) İngiliz ekonomisinin tüm hilelerden dolayı uğradığı kayıp ve maliyetler 73 milyar sterlin olup yükseliş eğilimi içindedir. Finans ve sigorta kuruluşları 3,5 milyar sterlinlik bir maliyet ile karşı karşıya bulunmaktadır. (CFS, 2012:3) Öte yandan, (1979-96) döneminde menkul kıymet yatırımları ile ilgili hilelerin 10'u iflâs, 2'si birleşme, 7'si yönetim değişikliğine yol açmış, 13'ü ise herhangi bir değişikliğe neden olmamıştır. Krediler ile ilgili hilelerin 6'sı iflâs, 2'si birleşme, 4'ü yönetim değişikliğine yol açmış, 8'i ise herhangi bir değişikliğe neden olmamıştır. Kredi karşılıkları ile ilgili hilelerin 9'u iflâs, 3'ü birleşme, 4'ü yönetim değişikliğine yol açmış, 12'si ise herhangi bir değişikliğe neden olmamıştır. (Green ve Reinstein, 2004:97) Bununla birlikte, hilenin maliyetini tam olarak ölçmek çok zordur, çünkü bankalar çoğu zaman müşterilerinin güvenini kazanmak ve bunu sürdürmek amacıyla banka ile ilişkili hilelerin üstünü örtme eğilimi göstermekte ve dolayısıyla tüm hileler ortaya çıkarılamamakta ya da raporlanmamaktadır. (Idolor, 2010:74)

3. Bankacılık Hilelerinin Türleri

Bankacılık hilesi, genel olarak bir bankadan nakit para ya da diğer varlıkları hileli olarak elde etmek amacıyla bilinçli olarak yanlış bildirim (*misrepresentation*) yapılmasıdır, ki bu çoğu zaman teknik uzmanlık gerektirmektedir. (Usman ve Shah, 2013:4) Hile yapmak için değişmeyen hedefler konumundaki bankacılık sektöründe hızlı zenginleşmenin yolu paraya ulaşmaktan geçtiğinden hem hile sayısı artmakta, hem de giderek karmaşık duruma gelmektedir. (Balogun vd, 2013:254) Burada hile riskinden (*borçlunun kimliği saptanamadığı için kredinin geri ödemesinin sağlanamaması ya da borçlunun geri ödemeye zorlanamaması*) çok, kredi riski (*kimliği bilinen bir borçlunun borcunu ödeyememesi ya da ödeyemeyecek olması*) söz konusu olmaktadır. (Hartman-Vendels vd, 2009:347) Bu bölümde, bankacılık sektöründe sıklıkla gözlenen hileler türlerine göre açıklanmaktadır.

3.1. Kredi Hileleri (Loan Frauds)

Krediler, bankacılık sektörünün en önemli varlıklarından ve fakat banka güvenliği ve sağlamlığı için en büyük risk kaynaklarından birisidir, çünkü bankalar için en büyük risk müşterinin temerrüde düşmesi olmaktadır. Kredi portföyünden kaynaklanan sorunlar olası kredi riski dolayısıyla tarihsel olarak banka zararlarının en önemli nedenleri arasında gelmektedir. Sorunlu krediler (*non-performing loans*) kredi verirken bankaların sağlıklı bir karar verme mekanizmasına sahip olmamasından dolayı artmakta, banka iflâslarına, fon sahiplerinin bankalara yaptıkları yatırımların kaybolmasına ve halkın krediye ulaşamamasına neden olmaktadır. (Ajah ve Inyiama, 2011:1-2) Krediler aracılığıyla bankalar ekonomide belirli insanları ya da alt kümeleri desteklemek için etkili araçlar olabilmektedir, çünkü doğrudan sübvansiyonların tersine olumlu kredi koşulları aracılığıyla servetin dolaylı bir biçimde yeniden dağıtımı sağlanabilmektedir. (Benston, 2004:26-7)

Kredi hilelerinin sık rastlanan nedenleri arasında, etkili iç denetim personelinin yokluğu ya da eksikliği, üst-orta kademe yöneticilerin sık sık değişmesi (*hızlı devir*), önemli denetim ve finans görevlerine niteliksiz personel atanması, müşterilerin istenen bilgi ve finansal tabloları sağlamakta gönülsüz olması ile fiktif ya da çelişkili veriler sunması bulunmaktadır. Kredi ve avans hilelerinin özel nedenleri arasında ise şubelerin onaylanmış krediler, satın alma belgeleri, izin verilen fazla çekimler gibi konularda kontrol otoritelerine bilgi vermemeleri, müşteri menkul kıymet portföyünün, stok ve varlıklarının düzenli aralıklarla ve banka yönergelerinde öngörüldüğü şekilde raporlanmaması, kredi ile alınan varlık miktarı ve kalitesinin fiziksel kontrolünün yapılmaması ve doğrulanmaması, ipotekli malların şubeler tarafından gecikmeli olarak ve yüzeysel biçimde fiziksel kontrollerinin yapılması (*ipotek edilen varlığın sunduğu teminatın kontrolünde bankanın kendi belirlediği kurallara tam olarak uyulmaması ve sonuçta teminat belgelerinin önemli ölçüde eksik olması*), ipotekli varlıkların stoklandığı yerlerde belirgin biçimde tanımlanmasının sağlanmaması, ipotekli varlıkların uygun risklere karşı yeterli ölçüde sigortalanmaması, kredi alan müşterinin sadece kredi veren banka ile ilişkili olmasının güvence altına alınmaması, kredi müşterisinin ve özellikle bireysel müşterilerin kişiliği ve özgeçmişini doğrulamak amacıyla sürecin başlangıcında ciddi bir girişimde bulunulmaması, çekilen kredilerin nerede kullanıldığının doğrulanmaması, çekim hakkının kullanılmasında önceden belirlenen marjların sürdürülmemesi ya da değiştirilmesi, başka bankalardan devralınan müşterilerin ayrıntı-

lı biçimde izlenmemesi, müşteri ve vade temelinde mevcut kredilerle ilgili düzenli raporlar ve tablolar alınmaması belirtilmektedir. Sonuçta krediler ve avanslar, kamu ve düzenleyicilerce önceden belirlenmiş güvenlik amaçlı kural ve önlemlere uyumun istenen düzeyde olmadığı (*yöneticilerde %89, çalışanlarda %70 uyum*) bankacılık işlemleri arasında değerlendirilmiştir. (Khanna ve Arora, 2009:3 ve 10)

Krediler tarihsel olarak bankaların en büyük gelir kaynağı ve en büyük varlık grubu olmasına karşılık 1987'de iflâs eden bankaların %79'unda, kredi birimi çalışanları krediyi güvence altına alma ve onaylama sürecinde izlenecek genel kural ve usülleri yeterli ve ihtiyatlı biçimde uygulamamış, bu bankaların %41'i kredi için yeterli belgelendirmeyi (*güncel nakit akım tabloları, iş planları, yapı denetimleri ve değerlemeleri ve ticaret yasalarının gerektirdiği dosyalar gibi*) yapmamıştır. (Green ve Reinstein, 2004:90) Kredi başvuru ve kullandırma sürecinde (*origination process*) toplanan bilgilerin doğruluğu üzerinde hem kamu, hem de özel kuruluşlar kaygı taşımaktadır, çünkü büyüklüğü ne olursa olsun, kredi müşterilerinin sunduğu az sayıda yanıltıcı malî tablo ile sistematik olarak karşılaşmayan ve yeterli deneyim kazanamayan kredi kuruluşları hilelerin farkına varamayabilmektedir. (Chandler, 2014:82)

ABD'nin tersine özkaynak finansmanından (*equity financing*) çok kredi finansmanına (*debt financing*) ağırlık veren Çin ve Japonya gibi ülkelerde, banka kredileri ekonomik sistem için daha önemli bir kaynak olmaktadır. Çin ile ilgili yapılan gözlemler kamunun ağırlıklı ya da etkili olduğu ülkelerde büyük ölçüde geçerli olmakta, öte yandan sermaye piyasalarının önemli olduğu ülkelerde de göreli daha düşük ağırlıkta olsa da bankalardan daha yüksek tutarda ve hızlı kredi alabilmek amacıyla sıklıkla kredi hilelerine başvurulduğu değerlendirilmektedir. (Higgins, 2012:1174-5,1179, 1182) Nitekim özel ve piyasa odaklı batılı bankacılık sistemlerinden farklı olarak mülkiyet ve ticari girişimlerin finansmanında kamunun ağırlıklı bir konuma sahip bulunduğu, sosyal ve ekonomik eşitliğin kâr güdüsüne göre öncelikli olduğu, kaynak dağıtımında bankaların daha etkili olduğu Çin'de, sosyal ve ekonomik istikrar yaşamsal önemde görülerek kamu politikalarının makro hedefi durumuna gelmiş, bankacılık sisteminde yönetici ya da yönetim kurulu üyesi olan kamu bürokratları da kâr peşinde koşmak yerine söz konusu makroekonomik politika hedefini izlemeye öncelik vermiştir. Kurumsal kültürdeki gelişmelere karşın Çin şirketlerinde kamusal ve özel ticari işlevler arasındaki sınırlar belirgin olmadığı için kamu görevlileri banka sahibi, yöneticisi ya da yönetim kurulu üyesi olarak davranabilmekte, banka faaliyetlerine kamunun politika ve amaçları doğrultusunda müdahale edebilmektedir. Nitekim birçok kamu bankası belirli sayıda ve ayrıcalıklı müşteriye kredi vermeyi sürdürmekte ve daha sonra verimsiz raporlamadan kaçınmak amacıyla aynı müşterilere yeni krediler verilmesini onaylamaktadır. Bu müşterilerin çoğu kamu girişimleri olup geri kalan müşteriler hile yapan bireyler ve özel işletmelerden oluşmaktadır. Bu tür krediler sorunlu ve verimsiz kredi hacminin artmasına neden olmuştur. Ticari ilkelere bağlı kalmada eksiklik ve kurtarılma düşüncesi yanlış kredi tercihleri (*adverse credit selection*) ve çıkar çatışmalarının yaşanmasına açık kapı bırakmıştır. Ayrıca büyük bankaların iflâs etmesine izin vermeme gibi örtülü bir kamu politikası geçerli bulunmaktadır. Son olarak, kredi vermede banka müdürlerinin bölünmemiş yetkiye (*undivided authority*) dayalı olarak tek imza ile kredi verebilmesi, banka müdürlerinin yetkilerini sınırlandıracak kural ve mekanizmaların (*müşterinin kredi alma ve faaliyette bulunma amaçlarına göre yeterliliğini değerlendiren kredi onay komiteleri gibi*) olmaması, banka hesap sahipleri için el ürünü imza yerine damga/mühür kullanımına da izin verilmesi, şube düzeyinde verilen banka kredi onaylarının kontrol edilmesi ile ilgili bir sürecin olmaması nedeniyle banka içinden sahte onaylar verilmesi, bankaların kredi alınması ve kullanılması ile ilgili düzmece ticari senetleri ve yasadışı mevduatları ipotek ya da teminat olarak kabul etmesi de kredi hilelerinin yaygınlaşmasına yol açan sistemik açıklar olarak saptanmaktadır. Çin kültürünün iç kontrol sistemlerini engelleyen yönleri de bulunmaktadır. İş dünyasında kişisel ilişkiler inşa etmek taraflar arasında güven ve bağlılık yaratmakta, ancak bu kültürel özellik yolsuzluk ve hile için uygun bir ortam da oluşturabilmekte, ilişkilerin ve yolsuzluğun iç içe geçtiği gözlenmektedir. Bu ilişkiler tek başına yolsuzluk eyleminin bir kaynağı değilse de, yolsuzluğu kolaylaştıran önemli bir etmendir. Güçlü ve yetkili insanlarla özel ilişkiler, resmî kurallar ve gayrîresmî normlara uyulmaksızın güç alışverişine ve kazanç paylaşımına dönüşebilmektedir. Bununla birlikte, Çin'deki hileler kişisel suçların ötesinde yüksek düzeyli kamu bürokratları ve özel

kesim işadamları arasındaki ilişkileri ve ağları ilgilendiren kurumlaşmış, örgütlü suçlar niteliği kazanmıştır. Boumediene (2014:421) de bu bulguları doğrulamakta ve Tunus'da bankacılık sektöründe maruz kalınan hile riskinin, büyük ölçüde projeler için verilen büyük kredilerde sağlam teminatlar alınmaması ve olması gerekenden daha düşük faiz oranları ile kredi verilmesinden kaynaklandığını saptamaktadır.

3.2. Hesap Hileleri (Account Frauds)

Bilgiye dayalı ekonomilerde, bir kredi kartı ya da kredi almak amacıyla yanlış bir kimlik (*sahte ya da çalınmış kimlik*) kullanılması anlamına gelen hesap hilesi ya da kimlik hırsızlığı (*identity fraud*) ciddi bir sorun durumuna gelmiştir. Burada kredi riski değil, hile riski (*bir bankanın kredi alan müşterisinin kimliğini belirleyemediği için kredinin geri ödenmesini sağlayamaması*) söz konusu olmaktadır. Özellikle internetin kişisel olmayan ve sınırsız doğası, işlemin hızı ile birlikte müşterinin tanınması ve doğrulanmasında kaçınılmaz biçimde zorluk yaratmakta ve hileli temsiliyete neden olmaktadır. Yüz yüze müşterilerden istenen belgelerin aynısının yüz yüze olmayan müşterilerden (*non face-to-face*) istenmesi mümkün olsa da, bu belgelerde adı geçen müşterileri yüz yüze müşterilerle eşleştirmede çok büyük güçlük bulunmaktadır. Mevcut hesaplar üstünde yapılan hilelerde, hırsız mevcut bir hesabı ya da kredi ilişkisini (*örneğin kredi kartı hesabını*) ele geçirmektedir. Yeni hesap hilesinde ise, hırsız başkalarının kişisel bilgilerini kullanarak mağdur adına yeni hesaplar açmakta ya da yeni kredi ilişkileri oluşturmaktadır. Hırsızların yeni hesaplar açarak elde ettikleri mal ve hizmetlerin medyan değeri 1.500 $ olarak bildirilmişken, bu değer mevcut hesaplar ile yapılan kimlik hırsızlığı yoluyla kötüye kullanmalarda 500 $'dan az saptanmıştır. Başka bir deyişle, yeni hesap hileleri mevcut hesap hilelerinden çok daha maliyetli olmaktadır. Almanya'da hesap hileleri 1999'da 13 milyar €'dan 35 milyar €'ya çıkmıştır. Hesap hilelerinin sonuçlarına bakıldığında, sayısal olarak bir artış, ortaya çıkarma (*clear-up rate*) oranlarında bir azalma ve dolayısıyla bu tür hilelere bağlı parasal kayıpların istikrarlı bir yükseliş içinde olduğu belirlenmiştir. (Hartman-Vendels vd, 2009:347-8, 357) İngiltere'de ise 2013'de saptanan 220.000'den fazla hilenin %60'ı kimlik ile ilgili suçlardan kaynaklanmıştır. (Gold, 2014:17) Bu ülkede 2011'de kimlik hileleri yol açtığı maliyetler (1.2 milyar £) ve olumsuz etkilenen yetişkin nüfus açısından (%9,4) elektronik bankacılık hilelerinin de önüne geçip daha ivedi bir sorun konumuna yükselmiştir. (CFS, 2012:3) Kimlik hırsızlığı, 2009 Küresel Telekomünikasyon Hile Araştırması'na göre, en sık yapılan hiledir ve toplam hilelerin (72-80 milyar $) %29'unu oluşturmaktadır. Telekomünikasyon operatörleri kimlik hilesi maliyetlerini, tahsil edilemeyen alacak olarak kaydetmekte, dolayısıyla gerçek hile maliyetleri yüksek fiyatlar ve vergiler aracılığıyla toplumun üzerine yıkılmaktadır. (Ghosh, 2010:9 ve 13)

Bankacılıkta zimmet (*defalcation*) de hesap hilelerinin bir alt kümesi olarak genellikle müşterilerin emanet ettiği paraların (*mevduatların*) banka çalışanı ya da müşteri tarafından belgeler tahrif edilerek zimmete geçirilmesi biçiminde yapılan çok yaygın bir banka hilesidir. Banka çalışanı ve müşterinin zimmet için işbirliği yapması durumunda hile daha örtülü biçimde yapılmakta ve ortaya çıkarılması zorlaşmaktadır. Müşteri hizmetleri görevlisinin müşteri hesabına yapılan ödemeleri zimmete geçirmesi ve şüpheli müşterilere faturalandırılan ödemelerden bir miktar paranın zimmete geçirilmesi, bu hilenin diğer biçimlerini oluşturmaktadır. Aynı şekilde, müşterinin önceden onayı olmaksızın onun hesabından büyük tutarda para çekmek amacıyla müşteri imzasının taklit edilerek kullanılması da hesap hilesi niteliğindedir. Bir tür kalpazanlık (*forgery*) olan bu tür sahtecilikler banka çalışanları tarafından ya da banka çalışanları ile banka dışından kişilerin işbirliği ile yapılabilmektedir. Burada müşterinin örnek imzalarının (*specimen signature*) sahtesi üretilmektedir. Hesap hilelerinin başka bir biçimi fatura manipülasyonu (*manipulation of vouchers*) ile yapılmaktadır. Burada bir hesabın kayıtları başka bir hesabın kayıtlarının yerine geçirilmekte, böylece banka müşterilerinin mevduatları fiktif bir hesaba aktarılmaktadır. Bu tür hileler denge ve kontrollerin (*görevlerin düzgün ayrılmaması, faturaların ve banka kayıtlarının günlük ve ayrıntılı olarak incelenmemesi gibi*) yetersiz olması durumunda artış göstermektedir. (Idolor, 2010:66-7) Sık yapılan hesap hilelerinden birisi de, avans ödemesidir. (*advance fee*) Bu hile bilinmeyen bir kişi ya da kuruluştan gelen bir mektup ya da e-posta ile başlamakta, bu mektup ya da e-postada bir iş planı ya da teklifi bulunmaktadır. Posta ya da mektubu alandan iş teklifinin açıklanması için belirli bir hesaba büyük bir miktar para yatırılmasını istenmekte, para yatırıldıktan sonra

bilinmeyen kişi ya da kuruluş ortadan kaybolmaktadır. (Balogun, 2013:254)

2000'lerin sonlarına doğru elektronik bankacılıkla ilgilenen suçlular ticari işletme hesaplarını hedef almaya başlamıştır. İşletmelerin ele geçirilmesi ile ilgili tipik senaryo (*phishing*), oltaya takılan bir yemin (*e-postanın*) bir alıcıya gönderilerek alıcının sahte bir web sitesine ya da virüslü (*zararlı*) bir eklentiye yönlendirilmesi ve sonuç olarak sahte siteye veri girişi yapması ya da hedef işletmeye virüslü yazılımın kurulması biçiminde gerçekleşmektedir. Her iki yoldan da hırsızlar hedef işletmenin sanal hesap giriş bilgilerini kullanarak yetkisiz fon transferleri gerçekleştirebilmektedir. Zararlı yazılım (*malware*) ve diğer teknikler sürekli evrim geçirmekte ve oltalamadan ortadaki adam saldırılarına (*man-in-the- middle attacks, bir banka müşterisinin oturumunu basmak ve gerçek zamanlı olarak güvenlik kodlarını ele geçirmek*), kişisel ya da ticari mobil aygıtlara zararlı yazılım yerleştirmekten sahte ve zararlı uygulama ya da metin iletileri kullanarak şirket sistemlerine erişim sağlamaya (*smishing*), sosyal medya sahtekarlıklarından, doğrulama için kullanılan telefon hatlarına sızılmasına, sahte gerçek zamanlı banka chat oturumlarından banka ya da çalışanlarına doğrudan korsan saldırılarına kadar uzanmaktadır. (Scania ve Ludwig, 2013:3)

3.3. Plastik Kart Hileleri ve Kartsız Hileler (Plastic Card Frauds, Card-Not-Present Frauds)

Plastik kart hileleri, yasal bir hesabın sahip olduğu olanakların izinsiz ve yetkisiz biçimde kullanılması eylemidir. Ödeme trafiğinin artması, çağdaş teknolojinin ilerlemesi ve hile taktiklerinin gelişmesi ile birlikte plastik kart hileleri de artış göstermekte, dünya ölçeğinde kart çıkaran şirketler, tacirler ve müşterilere büyük zararlar vermektedir. Plastik kartlar, sistem kullanıcılarına geniş bir hizmet yelpazesi sunarak çağdaş ödeme sistemlerinin ayrılmaz bir parçası olmayı başarmasına karşılık nakit ile ilgili hilelere benzeyen ve temel olarak çalınma ve sahtecilikten ileri gelen hilelerden olumsuz etkilenmektedir. (Krivko, 2010:6070) Ödeme kartları (*payment/debit and credit card frauds*), en değerli ve yaygın sistemlerden birisidir. Bunlar elektronik transferler ve banka çeklerinin ek önlemlerle korunmasından dolayı nakit gerektirmeyen ödeme araçlarından en çok kullanılanı olmuştur. Ödeme kartı hileleri, kart bilgilerinin çalınması, değiştirilmesi ve doğrudan bir kazanç sağlamak amacıyla yeniden kullanılması yoluyla gerçekleştirilmekte ve iki aşamalı bir suç oluşturmaktadır; önce kart bilgileri ele geçirilmekte, sonra da karttan harcama gerçekleştirilmektedir. Bu tür hileler genellikle iki kategoride değerlendirilmektedir: Kartsız ve fiziksel hileler. Kartsız hilelerde veriler, ödeme kartlarının açıklarından, oltalamadan ya da kötü amaçlı yazılımlardan, fiziksel hilelerde ise veriler kaybolan ya da çalınan kartlardan, kopyalamadan, ATM işlemlerinden ya da kart bilgilerinin çalınmasından elde edilmektedir. (Souvignet vd, 2014:143-4) Elektronik web alışverişlerinin yakın bir gelecekte perakende harcamaların %30-50'si arasında olması beklenmekte, bu durum ise beraberinde kartla ilgili (*kartlı ve kartsız*) hilelerin artışını getirmektedir. İngiltere'de tüketicilerin her bir sterlinlik harcamasının %17'si elektronik alışverişler yoluyla yapılmaktadır. Elektronik ticaretteki patlama kart ile yapılan hileler yanında temassız hileler (*card-not-present fraud*) için daha büyük fırsatlar sunmaktadır. Buna karşılık, internet perakendeciliğindeki büyüme yeterli güvenlik önlemleri eşliğinde yaşanmamakta, güvenlik yaklaşımındaki gevşeklik ise bu tür hilelerin sayısı ve maliyetlerinde ciddi artışlara neden olmaktadır. Kartsız hilelerdeki artışın diğer kanallarda yapılan hilelerin kat kat üstünde olması özellikle önemli bir noktadır. Nitekim tüketicilerin elektronik olarak daha çok para harcama eğiliminde olması titiz bir doğrulama eksikliği ile birleşince kartsız hilelerin mevcut koşullarda artmayı sürdürmesi beklenmektedir. (Brunswick, 2009:12-3) Kart hileleri son dönemde ciddi bir değişime uğramış, hilekarların kartları klonlamak ve kart bilgilerini toplamak amacıyla ATM'lerde çok küçük kameralardan yararlanarak PIN numaralarını kaydettikleri (*skimming*) zamanlar geride kalmıştır. (Gold, 2014:12)

Kredi kartı ile yapılan hilelerde, sahibinin bilgisi olmadan çeşitli yollardan elde ettikleri kart ya da kart bilgileri yasadışı biçimce kullanılmaktadır. Bu yollar arasında yeni çıkarılan kartları içeren postaların alıkonulması, sıyırıcılar (*skimmer*) kullanılarak kart bilgilerinin kopyalanması ve çoğaltılması, gizli müşteri bilgilerinin klonlanmış (*gerçek gibi görünen*) web siteleri ve güvenilir bir insan maskesi aracılığıyla oltalanması ya da bu bilgilerin kredi kartı şirketlerindeki etik davranmayan çalışanlardan alınması belirtilmektedir. Hilekarlar BIN (*Bank Identification Number*) kul-

lanarak da kredi kartı yapabilmektedir. Kredi kartı hileleri en az kart sahiplerini etkilemektedir, çünkü yapılan işlemlerle ilgili sorumlulukları sınırlıdır; mevcut yasalar, tüketiciyi koruma politikaları ve sigorta uygulamaları kart sahiplerinin çıkarlarını çoğu ülkede korumaktadır. Bu hilelerden en çok etkilenenler ise, internet tacirleridir ve bunların elinde çoğu durumda kart sahiplerinin bilgilerinin kötüye kullanılması ile ilgili hiçbir kanıt (*sayısal imza gibi*) bulunmamaktadır. Tacirler, kredi kartı geri ödemesi, malların gönderilmesi, kart komisyonları ve kendi idari giderlerini üstlenmek durumunda kalmaktadır. Aynı tacirin yaygın biçimde hileli işlemlere karışması müşterileri kendisinden kaçırmakta, kart çıkaran bankaların hizmetlerini geri çekmelerine ve itibar kaybına yol açmaktadır. Öte yandan, kart çıkaran bankalar hile olaylarının araştırılması ile ilgili idari giderleri üstlenmek ve hile ile mücadele etmek için gerekli yazılım ve donanım altyapısını kurmak zorunda kalmaktadır. Bu bankalar ayrıca işlemlerin gecikmesi ile ilgili maliyetlere de katlanmaktadır. Araştırmalara göre, hileli işlem tarihi ile kredi kartı geri ödemesi bildirim tarihi arasında geçen ortalama sürenin 72 gün gibi uzun bir zaman olduğu olması hilekarlara daha büyük zararlar yaratmaları için yeterli zamanı kazandırmıştır. (Quah ve Srinagesh, 2008:1721-2) Avrupa'da ödeme kartları ile ilgili hilelerin 1,5 milyar €'ya ulaştığı saptanmıştır; bu hile örgütlü suç oluşumları için de kârlı bir faaliyet alanı olarak görülmüştür. (Souvignet vd, 2014:144) İngiltere'nin hile önleme kurumuna göre ise 2013'de genel olarak hileler 2012'deki düzeyinin %11 altında gerçekleşmesine karşılık, ödeme kartları ile ilgili hileler 2012'ye göre %24 artış göstermiş ve 2013'deki doğrulanmış hilelerin %30'unu oluşturmuştur. (Gold, 2014:17)

3.4. Çek Hileleri (Cheque Frauds)

Çek hileleri, yanlış ve yanıltıcı belgeler yardımıyla yapılan harcama hileleri arasında değerlendirilmektedir. Genellikle hile yapan kişiler çeki düzenleyen ya da düzenlettiren çalışanlar arasından çıkmaktadır. (Singleton vd, 2006:117) Genellikle boş çekler ele geçirip çeki imzalamaya yetkili olanların imzasının taklit edilmesi, düzenlenmiş geçerli bir çekin ele geçirilmesi ve lehdar adının değiştirilmesi, ciro ile devredilecek kişi adının değiştirilmesi ve her iki durumda da hile yapan kişilerin adının yazılması, çek imzalamaya yetkili olanların yetki sınırları içinde kendilerine ya da suç ortaklarına çek yazması ve usüle uygun ve geçerli çeklerle birlikte düzmece çeklerin imzaya gönderilmesi ile yapılmıştır. (Biegalman ve Bartov, 2006:172-3) Çek hileleri genellikle uygun fırsat/ortam koşullarından yararlanılarak yapılmaktadır. Sözgelimi banka ödeme emirleri, mevduat alındıları, çek defterleri gibi güvenlik altında bulundurulması gereken değerli belge ve formların gözetim sorumluluğu onayları alınmadan vezne ve sayım görevlilerine verilebilmektedir. Bu bağlamda, çek defterlerinin her zaman sadece hesap sahibine verilmesi ve teslim edilmesi güvence altına alınmayabilmekte, büyük tutarlı çek defterleri verilen müşterilerin kimi zaman yazılı talebi dahi aranmayabilmekte, örnek imza sirkülerleri gün sonu kilitli kasada saklanmayabilmekte, hareketsiz hesapların imzaları hareketli (*canlı*) hesapların imzalarından her zaman ayrı tutulmayabilmektedir. (Khanna ve Arora, 2009:9)

Çek hileleri de azalma eğiliminde olmakla birlikte finansal kuruluşlar için bir tehdit kaynağı olmaya devam etmektedir. Bu hileler önceleri karşılıksız çek yazma (*bad cheque writing*) biçiminde iken zaman içinde değişime uğramış ve farklı ülkeleri, kanalları ve kimlik hırsızlığını da içeren hilelere dönüşmüştür. ABA 2009 araştırmasına göre, 2008'de mevduat hesabı ile ilgili hilelerin %26'sı ve toplam zararın %30'u çek hileleri ve sahteciliklerine bağlanmıştır. Bankacılık sektöründe çekle ilgili hilelerin neden olduğu zararlar 1,027 milyar doları bulmuştur. Söz konusu kayıpların %38'ini kapanan hesaplar ve mevduat hilelerini içeren hileler, %30'unu sahte çek hileleri (*counterfeit cheques*) ve %22'sini sahte ciro hileleri oluşturmaktadır. Ödeme biçimleri değiştikçe, hile eğilimleri de değişmektedir, ancak çekler bu sürecin daha uzun süre bir parçası olmayı sürdürecek gibi görünmektedir. Bankacılık sektöründe çek hileleri genel olarak iki kategoriye ayrılmaktadır. Bunlardan birincisi mevduat hilesi (*deposit fraud*) olarak adlandırılmaktadır. Burada ATM'lere konulan çeklere el konulmaktadır; çekli işlemin yapılması ile çeki yazanın bankasında tahsil edilmesi arasında geçen süre (*float*) hilekara zaman kazandırmaktadır. Diğer çek hilesi ise, sorumluluk yükleyen hile (*on-us fraud*) olarak adlandırılmakta ve aynı finansal kuruluşa yazılan çeklerle (*sahte çekler, sahte imzalı çekler gibi*) yapılmaktadır. (Sarra, 2011:289-90) Veznedarın kendi adına sahte bir çek düzenleyerek sahte ödemeler yaptırması da (*fake payments*) da bu kapsamdadır. Bunlar, diğer banka çalışanları ya

da müşterilerin işbirliği ile ya da onlar olmadan da yapılabilmektedir. Bu tür hilelerin başka bir biçiminde, üçüncü kişiler başkalarının kılığına (*kimliğine*) girerek (*impersonation*) yeni çek defterleri almak istemektedir. Bunlar, olayın farkında olmayan müşterilerin örnek imzaları ya da pasaport fotoğraflarını çıkarma becerisi ve yetkisi olan banka çalışanları ile gizli işbirliği yapılması durumunda daha yüksek maliyetlere yol açmaktadır. Çekler gibi ödeme emirleri de kalpazanlığın hedefi olabilmektedir. (Idolor, 2010:66-8)

3.5. Akreditif Hileleri (Letter of Credit Frauds)

Akreditif işleminde, satıcının akreditif koşullarına tam olarak uyması durumunda bankalar satıcıya borcu ödeyeceklerini onaylamaktadır. Bankalar kendilerine tam olarak kanıtlanması zor sahte belgeler teslim edilse de, gelenekler ve standart uygulamalara uygun olmayan işlemler söz konusu olsa da bu durum değişmemekte, belgeler yüzeysel olarak incelenmekte, akreditif şekil koşullarına uygun olduğu sürece malların ya da taşıması gereken özelliklerin gerçekten olup olmadığına bakılmaksızın satıcıya ödeme yükümlülükleri yerine getirilebilmektedir. Bu tür hilelerde genel olarak, akreditif koşullarına uygun düzenlenmiş sahte belgeler satıcı tarafından bankaya verilmektedir. Satıcının (*ihracatçının*) ülkesindeki muhabir banka (*confirming bank*) belgeleri ithalatçının (*alıcının*) bankasına göndermekte ve satıcıya ödeme yapmaktadır. Alıcı kargonun yüklendiğini ve hedef ülkeye (*varış ülkesine*) doğru yol almakta olduğuna inanmaktadır. Birçok durumda gemi varış limanına ulaştığında, alıcı kargonun sözleşmede öngörülen ürünler olmadığını ya da hiç yükleme yapılmadığını anlamaktadır, ancak sözleşme gereği ödemesini yapmış durumdadır. Alıcı, satıcının akreditif işlemlerinde yaptığı hileden olumsuz etkilenmiştir, çünkü kullanılan kredilerin bankaya geri ödenmesi yükümlülüğü hâlâ üzerinde bulunmaktadır, ancak yanlış (*hileli*) ürün almış ya da hiçbir ürün almamıştır. Akreditif işlemlerindeki hileler genel olarak satıcı, alıcı ya da finansal aracılar tarafından yapılabilmektedir. Bunlar arasında en yaygın olan satıcılar tarafından yapılmış olanlardır ve alıcılar üzerince yıkıcı etkiler bırakmaktadır. Malezya'da ticari bankalar ile 2010-2011 yıllarında yapılan bir araştırmaya göre, akreditif hilelerinin %70'i belgesel hile (*documentary fraud*), %25'i konteyner hilesi (*container fraud*) ve %1'i de sigorta hilesidir. (*insurance fraud*) Bu hilelerin işlem temelinde görünümü ise, Tablo 3'de gösterilmiştir. Finansal ve ekonomik kriz dönemlerinde belgesel hileler artış göstermekte, hilekarlar hiç olmayan kargolar için bankalardan finansman sağlamak amacıyla akreditif işlemlerini kötüye kullanabilmektedir. Bankaların riskleri özellikle ödemeler serbest bırakıldıktan sonra artış göstermektedir. Kargo sigorta hilesinin en temel yöntemi, malların gerektiğinden fazla tutarda sigortalanması olmaktadır; satıcı malları gerçek değerinden daha yüksek değerde sigortalatmakta, hayalî bir kayıp ya da bozulma yaratmakta, sigorta şirketinden gerçek değerinden daha yüksek bir tazminat talep etmekte ve böylelikle sigorta gelirlerinden de kâr sağlayabilmektedir. Konteyner hileleri ise, satıcının alıcıya hileli ürünler göndermesi durumunda görülmektedir. (Chehashim ve Mahdzan, 2014:224-6, 228-30, 233)

Tablo 3. Akreditif Hilelerinin Görülme Sıklığı (%)

Sahte Konşimento	45,0
Sahte Sevkiyat/Teslimat Emri	30,0
Alıcı/Satıcının Gizli Anlaşması	30,0
Üçüncü Taraf Katılımıyla	20,0
Kara Para Aklama Amaçlı	20,0
Banka Çalışanları ile Anlaşmalı	10,0

3.6. Bilgisayar Hileleri (Computer Frauds)

Bu tür hileler, bankaları etkilediği algılaması en yüksek olan hile türünü oluşturmaktadır ve banka bilgisayarlarının veri toplama, girilen verileri işleme ve hatta veri çıkışı ve yayımı aşamalarında hileli biçimde manipülasyonuna dayanmaktadır. Uygunsuz veri giriş sistemleri, virüsler, yazılımlara müdahaleler, işlemlerin manipülasyonu ve siber (*sanal*) hırsızlıklar nedeniyle bilgisayar hileleri ortaya çıkabilmektedir. ATM (*otomatik para çekme makinaları*) ve gerçek zamanlı internet bankacılığı ve ticaretin yoğun biçimde kullanıldığı bu çağda, siber hırsızlık ve suçlardan kaynaklanan bilgisayar hileleri korkutucu bir boyut kazanmıştır. (Idolor, 2010:68) Teknoloji hem fırsatlar, hem de yeni tehditler anlamına gelmektedir. Kablosuz iletişim, küresel bilgisayar ağları ve diğer teknolojik olanaklar bilgisayar hilekarlarının hile yaparken işlerini kolaylaştırmakta, örneğin mikro bellekler aracılığıyla bir işletmenin bütün bilgilerini alıp kapıdan çıkıp gitmesini olanak vermekte ya da dünyanın başka bir noktasından sistemlere erişim

sağlamasına yardımcı olmaktadır. Dolayısıyla, internet, intranet ve diğer sistemler bilgisayar hilekarları için uygun araçlara dönüşmüştür. Bilgisayar hilekarları bir bilgisayar hilesi yapmadan önce hedeflerin hem içinde, hem de dışında bir ya da birkaç kaynaktan yararlanarak sosyal mühendislik (iletişim becerileri), hırsızlık, korsanlık ya da bunların bir karması ile bilgi toplamaktadır. (Kovacich, 2009:10, 14)

3.7. Kara Para Aklama (Money Laundering)

Bu tür hileler, suç faaliyetlerinden elde edilen paraların bankada suçlular adına saklanması, yabancı bankalara transferi ya da yasal ekonomiye yatırım yapılması yoluyla yasallaştırılması yoluyla yapılmaktadır. Siyasetçiler ve işbirlikçi banka çalışanlarının da karışabildiği bu olaylar tehlikeli boyutlara ulaşmıştır. (Idolor, 2010:67) Bu denkleme muhasebecileri de eklemek gerekmektedir, çünkü kara para aklama operasyonlarında reel ve sanal ekonomi arasındaki bağlantı muhasebe kullanılarak saklanabilmektedir. Ekonomik ve finansal suç dünyasının ortak varlıklarının bankalar ve aracılardan oluşan ağda dolaştırılmasının yönetimi bu tür bir kullanıma örnek olarak verilmektedir. Muhasebe bilgileri, yasal para ile aklanmış para arasındaki tutarsızlıkları önleyecek ve kamunun gözlediği yaşam biçimini açıklayabilecek biçimde düzenlenebilmektedir. (Compin, 2008:591-9)

3.8. Ponzi Hileleri (Ponzi Schemes)

Bankacılık sektöründeki en yaygın hilelerden biri de, gerçek ve yasal bir faaliyete ya da yatırım stratejisine dayanmayan bir tür mevduat toplama ve dağıtma hilesi olan Ponzi yönteminin kullanılmasıdır. Ponzi yöntemini başlatan bileşen, bilmeyerek para yatıran yatırımcılardır; sayıları giderek artan yatırımcıların desteği genellikle yüksek ve istikrarlı kazançlar vaad edilerek kullanılmaktır. Yatırımını ya da salt bunun getirisini geri almak isteyenlerin ödemeleri bu sisteme yeni katılan yatırımcıların katkılarından yapılmaktadır. Yöntem gerçek ve yasal bir faaliyete, işe ya da yatırım stratejisine dayanmadığı için eninde sonunda ortaya çıkmaktadır, çünkü yatırımcıların likidite talepleri mutlaka Ponzi kurucusunun yeni yatırımları fonlama yeteneğinin üzerine çıkmaktadır. (Drew ve Drew, 2010:53) Türkiye'de 2000'lerin başında 25 bankanın Tasarruf Mevduatı Sigorta Fonu (TMSF)'na devri ile sonuçlanan süreçte, riskleri dağıtması ve yüksek riskten kaçınması gereken banka yönetimleri gözetim, düzenleme ve denetim kurumlarının bilgisi dahilinde piyasalardan çoğunlukla iradî ya da kimi zaman da gayrî iradî olarak yüksek faizle mevduat toplamış ya da borçlanmıştır. Çoğunlukla hakîm ortağın grup şirketlerine kredi veren bankaların topladıkları mevduatların yüksek faiz ve esnek koşullar tuzağıyla sözü edilen bankalara çekilmekte olduğu ve bankaların bu süreçte yasal bir araç (saklama kasası) ve güven kurumu olarak kullanıldığı gözlenmektedir, ki bu mekanizma da Ponzi yöntemine büyük ölçüde uymaktadır. Örneğin bu bankalardan birinde artan zararların yol açtığı öz kaynak açığını kapatabilecek sermaye artırımının yapılamaması ve aktiflerde en büyük plasman alanı olarak görünen grup içi ve dışı kredilerin faiz geliri üretememesi sonucu likidite sorunlarının çok ileri düzeylere çıkması az sayıda mudiden yüksek faizle mevduat toplanması zorunluluğunu yanında getirmiş, bu şekilde toplanan kaynaklar daha yüksek faiz ile kredi olarak kullandırılamayınca ya da daha yüksek getiri sağlayan alanlara yatırılamayınca bankanın varlık ve kaynak bileşimi giderek bozulmuştur. (Kandemir, 2016:250, 254, 282)

3.9. Kanallar Arası (Çapraz) Hileler (Cross Channel Frauds)

Bu tür hileler, deneyimli suçluların yasadışı yöntemlerini uygulayabileceği artan sayıda hizmet kanalından yararlanması ile yapılmaktadır. Bireysel ve kurumsal müşterilerin bankacılık işlemlerini yapmak için birçok kanal olması dolayısıyla bugün her zamankinden daha çok açık söz konusudur, çünkü banka müşterileri 7 gün/24 saat hizmet almak ve bu hizmetlere kolayca erişmek istemektedir. Bu konuda zorluk, söz konusu müşteri hizmetlerini verirken uygun bir güvenlik düzeyini de sağlayacak bir denge kurmaktadır. Suçlular, her zaman ve her yerde sınırsız hizmet sağlama çabası ile müşterilere üst düzey güvenliği sağlama arasındaki kurulması ve sürdürmesi zor dengeyi kötüye kullanabilmektedir. Potansiyel sanal bir hırsızın tüm yapması gereken yasal bir müşterinin kullanıcı adı ve parolasını ele geçirmektir; müşterinin banka hesabına girildikten sonra her türlü işlemin yapılması olasıdır. Bu tür hileler ileri düzeyde karmaşık ya da basit olabilmektedir. Son zamanlarda kullanımı artan bir yönteme göre, hırsızlar banka irtibat noktalarını çeşitli araçlarla hedef almakta, müşteri hizmetleri temsilcisini kendisinden kimlik

bilgilerini alması için soru sormaya ikna etmektedir. İrtibat noktaları bu aşamada farkında olmadan hileye ortam hazırlamış olmaktadır. Suçlular, temel doğrulama sorularına verilebilecek yanıtları öğrendikten sonra bu bilgileri paraya erişim sağlamak amacıyla başka kanallarda kullanmaktadır. Bu tür hileler için önemli nokta, hilekarın finansal kuruluşların kullandığı doğrulama protokollarını başarıyla geçmesi olmaktadır. (Ginovsky, 2013:18-9)

3.10. Yağmalama (Looting) ve Risk Öteleme (Risk Shifting)

Yağmalama ve risk öteleme hipotezi, zor durumda olan bankaların içinin iyice boşaltılmasını açıklayan gerçekçi bir düşüncedir. (Boyd ve Hakenes, 2014:43-5, 57) Buna göre, yağmalama ve risk öteleme, iflâs etmiş olan ya da iflâsa yakın bankaların gösterdikleri bir tepkidir. Bir banka krizde ve özkaynakları tükenmiş ise, beklenen getirileri düşük düzeyde de olsa bilerek ve isteyerek büyük risklere girebilmektedir, çünkü eğer yüksek getiri olasılığı düşük olan bu oyun (*gambling for resurrection*) tutarsa banka yaşamını sürdürebilmekte, tutmazsa iflâs etmiş olmakta, dolayısıyla banka açısından iflâstan daha olumsuz bir sonuç ortaya çıkmamış olmaktadır. Risk öteleme ihtiyacı kendi başına bir amaç değil, yağmalamayı kolaylaştırmak için bir araç olarak görülmekte, dolayısıyla risk öteleme ve yağmalama eşzamanlı gözlenmektedir. Gelişmekte olan ülkelerde yağmalama krizde başvurulan olağan bir strateji olmuştur. Bu tür bir yağmalama, genellikle yapay olarak şişirilmiş kâr perdesi arkasında gerçekleştirilmektedir. Risk öteleme davranışları da, temel olarak banka yöneticilerinin kişisel amaçlı olarak bankayı yağmalamasını kolaylaştırmaktadır. Mevduatları başka noktaya çevirme (*diverted deposits fraud*) hilesi de bu kapsamdadır; burada banka yöneticileri bankanın bir bölümünü bilanço dışı tutmakta, dolayısıyla denetçiler kendi kendine borç verme (*self-lending*) olayının farkına varamamaktadır. Bu tür taktikler açık hırsızlıktan (*outright theft*) biraz daha fazlası olmakta, hissedarlar ve alacaklıların yasalarca zayıf biçimde korunmasından, denetçilerin yolsuzluğa bulaşmasından ve muhasebe standartlarının gevşek olmasından kaynaklanabilmektedir. Daha iyi bir kurumsal ve yasal ortam olması durumunda açık yağmalamanın (*blatant looting*) yapılmasının daha maliyetli olması beklenmektedir. Risk öteleme ve yağmalamada banka sahipliğinin rantı temel olarak bilgili hissedar-yöneticilere (*owner-managers*) gitmektedir, çünkü hissedar-yöneticilerin iç hissedarlar olarak bankayı yağmalayabilme olasılığı dış hissedarlara göre daha yüksek değerlendirilmektedir. Özellikle banka getirilerinin kötü olduğu koşullarda hissedar yöneticiler risk almada göreli olarak daha istekli davranmakta ve bankayı yağmalamaya yönelmektedir. Öte yandan, banka getirileri yüksek olduğunda hem iç, hem de dış hissedarlar bunları paylaşmak istemekte, bu durum ise her iki sınıfın da mevduat sigortası kurumunun aleyhine risk ötelemek istemesine neden olmaktadır.

Özellikle kredilerinin büyük bölümünü bir hakim ortağın denetiminde olan grup şirketlerine ya da benzer durumda olan banka sahibi başka bir hakim ortağın grup şirketlerine karşılıklı olarak kullandırmış olan Türk bankaları ve yöneticilerinin 2000'lerin başında yaptığı ve TMSF (*Tasarruf Mevduatı Sigorta Fonu*)'ye devir ile sonuçlanan işlemler risk öteleme ve yağmalama faaliyeti olarak değerlendirilmiştir. Ancak girişimciler yaptıkları faaliyetlerin sorumluluğunu gerçekten üstlenmedikleri ve ekonomik sistem de her durumda sonuç sorumluluğunu üzerine aldığı zaman, sözü edilen banka sahibi birtakım girişimcilerin neden olduğu iflâs ve zararlarının sosyalleşmesi ile sonuçlanan ve banka kaynaklarını özel tüketim amaçlarıyla kullanmaktan kamudan satın alınan bankaların özelleştirme taksitlerinin banka kaynaklarıyla ödenmesine kadar uzanan bir dizi yüksek riskli, ekonomik amacı olmayan ve sorumsuz işlem ve faaliyetler gerçekleştirilmesi gerçekte öngörülebilir bir gelişme niteliğindedir. (Kandemir, 2016:251, 254-5)

3.11. Elektronik Bankacılık (e-banking) Hileleri

Elektronik bankacılık, bankacılığın bireylere ve şirketlere elektronik araçlarla (*sabit ya da mobil telefon, internet*) verildiği bir hizmet sınıfıdır. Bu kanal bir kez kurulduktan sonra bankacılık hizmetlerini sunmak için en düşük maliyetli kanal olduğundan, bankalar tüm dünyada e-bankacılık hizmetlerine yönelmeyi sürdürmektedir. (Usman ve Shah, 2013:1-2) ABD nüfusunun önemli bir kesimi elektronik bankacılık hizmetlerini kullanmaktadır. (Quah ve Sriganesh, 2008:1721) Yine, İngiltere'de düzenli internet kullanıcılarının önemli bir bölümü aynı zamanda elektronik

bankacılık (*online banking*) kanallarını da kullanmaktadır. Internet alışverişi ve elektronik bankacılıktaki bu büyük artış özellikle oltalama ve kötü amaçlı finansal yazılımlar gibi saldırılar ile daha çok karşılaşılmasını yanında getirmiş, dolayısıyla elektronik bankacılıktaki hile maliyetleri de artış göstermiştir. (Ash, 2011:16) Elektronik bankacılık hileleri özellikle işlemler büyük tutarlarda yapıldığı, işlemler anonim (*ad vermeden*) yapıldığı ya da satış noktasında yapıldığı, talepler satış noktasında doğrulanamadığı ve ödeme talebinde bulunanlar hileli işlemlerin maliyetlerini üstlendikleri zamanlarda yoğunlaşmaktadır. (Usman ve Shah, 2013:4)

3.12. Diğer Çeşitli Hileler

Bu tür hileler genellikle hırsızlık (*theft*), yetkisiz borçlanma (*unofficial borrowing*) ve dövizlerin kötüye kullanılması (*foreign exchange malpractices*) gibi banka varlıklarının kötüye kullanılması ile ilgili bulunmaktadır. (Idolor, 2010:66-7, 73) Hırsızlıkta nakit para, seyahat çekleri ve dövizler yasa dışı olarak biriktirilmekte, bankanın mülkiyetinde olan motorlu taşıtlar, kırtasiye malzemeleri, cihazlar ve elektronik eşyalar alıkonulmaktadır. Yetkisiz borçlanmada, banka çalışanları gayrıresmi olarak kasadan para almaktadır; personel karşılığında vadeli çek benzeri hiçbir değer vermeden, karşılıksız olarak borçlanmış olmaktadır. Bu tür borçlanmalar maaşların ödenmemiş olduğu hafta ya da ay sonlarında yoğunlaşmaktadır. Kimi durumlarda kasadan alınan paralar birkaç saatlik ya da günlük işlerde kullanıldıktan sonra hiçbir iz bırakmadan yerine konmaktadır. Nijerya'da banka çalışanının acil gereksinimi olduğu zaman ve aldığı tutarı daha sonra ödeyeceği ya da ileri tarihli bir çek yazacağı düşünüldüğü için çoğu zaman olağan bir işlem olarak kabul edilmektedir, ancak bu tür işlemler sık sık ve resmi belge olmadan yapıldığı zaman manipülasyona açık olmaktadır, çünkü alınan para banka kasasına konmadan dengeleme yapmak için başkaca hileli işlemler yapmak gerekmektedir. Dövizlerin kötüye kullanılmasında ise, müşteri gereksinim ve talepleri doğrultusunda dövizle ilgili belgelerin sahtesi yapılmakta ya da bankaya tahsis edilen dövizler ön planda hayalet müşteriler kullanılarak kara borsaya yönlendirilmektedir. Olayın farkında olmayan ve iyi niyetli müşterilere resmi kurlardan daha yüksek kurlardan döviz satışı yapılabilmekte ve bu müşteriler bankadan ayrıldıktan sonra dengeleme yapılmaktadır. Bu tür hileler zayıf kontrol, kayıt ve muhasebe sistemleri ile yolsuzluğa bulaşmış üst yönetime sahip olan bankalarda daha verimli bir ortam bulmaktadır. Döviz manipülasyonları da olağan bir ticari işlem olarak kabul edilmekte ve bankaya kara borsadan daha yüksek getiriler sağlamak için banka parasıyla spekülasyon yapılmaktadır, ancak bu durum kara borsanın kurumlaşmasına katkıda bulunmaktadır. Son olarak, durum raporunun (*vaziyet özetinin*) sahtesi yapılarak (*falsification of status reports*) üçüncü taraflar yanıltılabilmektedir.

4. Bankacılık Hilesi Saptama/Önleme Strateji ve Yöntemleri

4.1. Genel Amaçlı Bankacılık Hilesi Saptama/ Önleme Strateji ve Yöntemleri

Bankacılık hilelerini ortaya çıkarmak için hile türünü bakılmaksızın uygulanabilecek birtakım genel stratejiler bulunmaktadır. (Guardian Analytics, 2013:6-7) Bunlardan birincisi, sisteme girişten çıkışa kadar olan tüm işlemleri izlemektir, çünkü hile eylemi belirli bir zaman aralığında gerçekleşmektedir. Oturum açılışından kapanışına kadar olan tüm elektronik ve mobil bankacılık işlemlerinin izinin sürülmesi, işlemin gerçekleşmesinden çok önce hileye ilişkin birtakım erken uyarı göstergeleri (*örneğin geleneksel uygulamalardan sapma gösteren tutar, işlem sırası, harcama ya da yatırım*) ortaya çıkarabilmektedir. İkincisi, işlemin gerçekleşmesini beklememek ve önleyici davranmaktır, çünkü hilenin önlenmesinde çalınan paraların telafi ya da tazmin edilmesinden çok önleyici bir anlayış ile hileyi daha gelişme aşamasında iken erkenden fark edebilmek ve etkisizleştirebilmek (*örneğin, banka çalışanlarına eski ve yeni ortaya çıkan hile risk faktörlerini öğretmek ve iş etiğini önemsemek*) önemlidir. Üçüncüsü, daha önceden gözlenen normal davranıştan sapan tutarsızlıkları (*anomaly detection*), (*örneğin güvenilir müşterilerin işlemleriyle karşılaştırma yaparak*) başka bir deyişle olağan olmayan davranışı saptamaktır. Suçlular bir ya da birkaç noktada yasalara uyan müşterilerin beklenen davranışlarına göre anormal nitelikte iş ve eylemler yapmaktadır. Dördüncüsü, ortalama davranış üzerinde değil, (*önemli tutarda işlem yapan müşterileri kendi kendisi ve birbirleriyle karşılaştırabilecek kontrol sistemleri kurarak*) bireysel müşteri üzerinde odaklanmaktır, çünkü bazı anomali saptama yöntemleri normal

davranışı tanımlamak için genelleştirilmiş ya da anakütle düzeyinde veriler kullanmakta, oysa bir kişi için olağan olan öbürü için olağandışı olabilmektedir. Beşincisi, (*örneğin birden çok kanaldan doğrulama yaptırarak*) çok aşamalı, katmanlı ya da düzeyli güvenlik anlayışına sahip olmaktır, çünkü hilekarlar çoğu güvenlik önleminden kaçmanın yolunu bulmaktadır, ancak tüm güvenlik önlemlerini aşmak aşırı ölçüde güç bir iştir. Çok aşamalı bir güvenlik stratejisine göre (*a layered security strategy*), hilekar bir katmanı geçerse, başka bir katman onu karşılamaktadır. Son olarak, işlemlerin yapıldığı elektronik aygıtların riskli olduğunu varsaymaktır, çünkü müşteriler antivirüs yazılımlarını aygıtlarına kurmak ve güncellemek konusunda özenli davransalar bile bu aygıtların risk altında olduğu düşünülmektedir. Kaldı ki, antivirüs çözümleri virüslerin yalnızca %5'ini yakalayabilmektedir. Bu genel stratejiler yanında hesap sahibinin davranışlarını gözetlemek amacıyla oturumları karşılaştırmak ve müşterileri taramak (*kullanılan aygıtların sıklıkla kullanılanlar ile uyumluluğunu belirlemek, internet servis sağlayıcısı ile internet protokol adresini önceki işlem ile karşılaştırmak*) gibi birtakım özel taktikler de söz konusudur. Genellikle her müşterinin oturumları arasında saat, süre, sıralama ve zamanlama gibi yönlerden benzerlikler bulunmaktadır; eğer daha önce gösterilen davranışla bir uyumsuzluk saptanır ise, önleyici davranarak hesap ayrıntılı olarak incelenebilmektedir. Bunun yanında, hilekarlar bir hesapta açık ya da zayıflık bulduklarında bunu diğer hesaplarda da kullandıkları için bir hile saptandığında benzer hile girişimlerini diğer müşteriler için de taramak gerekebilmektedir. Söz konusu strateji ve taktiklere bankacılık işlemleri için birtakım iyi uygulamaları da eklemek olanaklıdır. Bir kez,açık iletişim kanalları kurmak gerekmektedir. Bu konu özellikle çoklu banka kanalları için önemlidir, çünkü hilekarların kendilerine gerekli olan bilgileri elektronik olarak topladığı ve daha sonra başka kanallarda para transferine yönelik olarak kullanmak istediği bilinmektedir. İkincisi, bankaların olayları yönetme (*case management*) yeteneğine sahip olmasıdır. Saldırıları izlemek, nasıl sonuçlandığını, fiilî zararlarını, önlenen maliyetleri ve diğer ayrıntıları kaydetmek bu yönetim kapsamındadır. Üçüncüsü, hızlı tepki vermek için hazır olmaktır. Hızlı davranma yeteneği, hilenin gerçekleşmesine değin beklemek ve hızlı tepki göstermek yerine hile önleme ve müdahale stratejisi ve yönteminin önceden belirlenmesi ile başlamaktadır. Son olarak, müşteri ilişkileri ve etkileşimlerine önem vermektir; müşteriler önündeki tüm seçenekleri bilmeyi, bankaların etkili biçimde onları gözetmelerini ve varlıklarını korumalarını olumlu değerlendirmektedir.

Bankalar hile riskini azaltmak için 2 önemli strateji daha kullanmaktadır. Öncelikle üst yönetimce desteklenen güçlü bir kurumsal kültür ve önleyici bir hile yönetim programı yardımıyla potansiyel hile caydırılmaya ve daha sonra meydana gelen hileli faaliyetler ortaya çıkarılmaya çalışılmaktadır. Kurumsal kültür, etik eğitimine dayanmaktadır. Bu bağlamda hilelere karşı en kapsayıcı yaklaşım, hile olarak değerlendirilebilecek eylemler ve bunların saptanması ve önlenmesi konusunda çalışanlar katında bir bilinç (*farkındalık*) yaratmak olmaktadır. (Rahman ve Anwar, 2014:97-102) Uluslararası standartlar ile karşılaştırılabilir nitelikte ve etkin uygulamalar ile simgelenen sağlam bir kurumsal yönetim, hilelerin önlenmesinde önemli bir bileşendir. Üst yönetim, bankaların varlıklarını korumayı amaçlayan ve doğası gereği güvene dayalı işlevi dolayısıyla yüksek etik standartlara bağlı kalmayı sürdürmelidir. Ayrıca bankalar ücret ve ikramiye sistemlerini sürekli gözden geçirmelidir, çünkü çalışanlar iyi bir şekilde ücretlendirilir ve hilenin bulunması ve önlenmesinde başarı gösterenler maddi ve maddi olmayan ödüllerle teşvik edilir ise, hile olaylarında azalma görülebilecektir. Aynı biçimde, bankaların iç denetim birimleri yetersiz personelin toplandığı bir bölüm olarak görülmemeli, görevli personel tüm bankacılık işlemleri konusunda yeterince nitelikli, eğitimli ve deneyimli olmalıdır. (Idolor, 2010:77) Ek olarak banka yöneticilerinin gerek banka içinde, gerekse şubeler arasında yapılan hilelerin içsel ve dışsal nedenleri ile bunların önlenmesi yolları üzerinde daha çok çözüm üretmesi, iş ortamında çalışanları hile yapmaya yatkın duruma getiren etkenleri incelemesi, risk derecesi yüksek para ile doğrudan ilgili birimlerde astları uygun biçimde yakın gözetim altında tutması, ödeme araçlarına ve özellikle çeklere ilgi göstermesi ve savurgan yaşam biçimini sürmekte olan insanların işe alınmamasına özen göstermesi etkili olabilmektedir. (Balogun vd, 2013:260)

Banka hileleri ile mücadelede sosyo-kültürel etkenlerin de önemli olduğu belirlenmiştir. Nitekim yaş, cinsiyet, uyrukluk, eğitim ve kıdem arasında anlamlı ilişkiler bulunmuştur. (Nabhan ve Hindi, 2009:34-5) Belirli demografik ve sosyo-ekono-

mik özelliklerin hile riskini arttırdığı belirlenen Almanya'nın tersine, ABD'de söz konusu özelliklerin hile riskini önemli derecede yükselttiği ve hilekarların belirli özelliklere sahip olduğu saptanmamıştır. Ayrıca, bankacılık hilelerinde hilekarın kişisel özelliklerinden başka sosyal ve ekonomik sistemle ilgili etmenlerin daha önemli ve belirleyici olduğu düşüncesi de kabul görmektedir. Nitekim Rudesill ve Rudesill (2001:59), hile profillerinin idari suçlarla (*beyaz yakalı suçlar*) genel nüfus arasında önemli farklılıklar ortaya koymadığını, bununla birlikte hile yapan kişilerin genellikle kontrol sistemlerinin zayıflıklarını öğrenerek bunların nasıl aşılacağını bilen insanlar olduklarını ortaya koymuştur. Wells (1990:82) de aynı sonuca ulaşmıştır; buna göre hile yapan kişilerin demografik görünümü, sıradan ve ortalama yurttaşlardan çok farklı değildir; hilekarlar yaşamın her alanından, bütün toplumsal kesimlerden ve her türlü iktisadi ortamdan gelebilmektedir. Dolayısıyla, çoğu insanın hile yapmayacağı ve yalnızca belirli bir tipolojinin hile yapacağı düşüncesinin uygulamada karşılığı bulunmamaktadır. Son tahlilde, ödül vaadi ne kadar büyük ve ceza tehdidi ne kadar düşükse, toplum ve etik dışı davranış güdüsü o kadar büyük olmaktadır.

Bankacılık sektörü sürekli hileye karşı sistemlere yatırım yapmak ve suçluların bir adım önünde olmak zorundadır (Ash, 2011:16), çünkü teknolojideki hızlı gelişmeler dolayısıyla yapılabilecek en iyi iş, suçlulardan geri kalmamak ve onlara ayak uydurabilmektir. Bankalar ayrıca tüm çalışanlarını güvenlik tehditleri ve bunların belirtilerine tanı koyma konusunda eğitmek durumundadır, çünkü güvenlik sadece güvenlik görevlilerini ilgilendirmemektedir. Bütünleştirilmiş bir güvenlik planı etkinlik ve düşük suç göstergeleri bakımından olumlu sonuçlar vermiştir. Böylesi bir planda güvenliğin tüm bileşenleri fiziksel, lojistik, elektronik güvenlik, personel eğitimi suçun kurum içinde ve dışında ortaya çıkarılmasını içine alan tek bir birimde toplanmaktadır. Ayrıca suçluların bir adım ilerisinde olmak ve hile tekniklerini araştırmak amacıyla kurulan laboratuvarlarda yapılan araştırma–geliştirme yatırımları da herhangi bir güvenlik planının ayrılmaz bir parçası olarak değerlendirilmeye başlanmıştır. Birçok banka daha gelişmiş güvenlik çözümlerine yatırım yapmaktadır, çünkü müşteriler hesap ve fonlarını koruyacağına ilişkin bankalara güvenlerini yitirirler ise, rakip bir bankaya yönelebilmektedir. Bankalar ayrıca iç ve dış tehditlerin elektronik yolunu tekrar izleyerek bir daha olmasının önüne geçmek amacıyla adli bilgi teknolojileri (*forensic IT*) kullanabilmektedir. (Buchanan, 2010:59)

Bu çerçevede, Katarlı bankacılar ile gerçekleştirilen bir çalışmaya göre, banka hilelerinin ortaya çıkarılmasında en sık kullanılan yöntemler Tablo 4'de özetlenmiştir. Alınan önlemlerin %77'si önleyici, %62'si ortaya çıkarıcı ve %57'si düzeltici özelliktedir ve bankalar bunları aynı biçimde kullanmamaktadır. Üst yönetim düzeltici kontrollere önem vermekle birlikte önleyici kontrollere daha çok önem vermesi gerekmektedir. İç kontrol bileşenlerinden en çok kullanılanlar sırasıyla kontrol ortamı (%72), risk değerleme (%67), izleme (%59), kontrol faaliyetleri (%48) ve bilgi ve iletişim (%39)'dir. Hile ortaya çıkarıldıktan sonra ise en çok yapılan işlemler, sırasıyla denetim komitesine raporlama (%65), diğer işlemler (%22), yönetim kuruluna raporlama (%9) ve hemen işten çıkarma (%4) olmaktadır. (Nabhan, 2009:33-4, 36)

Tablo 4. Bankacılık Hilelerini Saptama Yöntemleri (%)

İç Kontroller	66,0
İç Denetim	28,0
Kamunun Bildirimi	19,0
Yönetimin Özel İncelemesi	7,0
Müşterinin Bildirimi	20,0
Çalışanın Özel İncelemesi	7,0
Rastlantı	2,0
Mevcut Hile ile Mücadele Politikası	4,0
Diğer	4,0

Öte yandan, hileden korunma yazılım ya da uygulamaları banka yönetici ve çalışanları tarafından en etkili önlem olarak kabul edilmekte, banka mutabakatları, parolaların korunması, iç kontrol sisteminin gözden geçirilmesi ve geliştirilmesi ile sürekli izleme (*continuous monitoring*), denetim komitesinin rolünün arttırılması, çalışanların özgeçmişlerinin kapsamlı incelenmesi, veri madenciliği stratejileri, süreç kontrolü, kurumsal politikalar, bütünleştirilmiş hile kontrolü, geleneksel teftiş, denetim ve çalışanlara yönelik etkili iletişim teknikleri, ihbar hatları, güvenlik koruma duvarı oluşturulması, üst yönetimin artan dikkati, kasa sayımları, stokların sayımı ve incelemesi

ve sayısal analiz tek başına değerlendirildiğinde en etkili araç ve teknikler arasında sayılmaktadır. Bunlar arasında, büyük tutarlı nakdî işlemlerden kaynaklanan hileler ile mücadelede ise en etkili yöntem banka mutabakatı olarak algılanmaktadır; düzenli olarak banka mutabakatları hazırlayarak nakdin çalınmaması güvence altına alınabilmekte, muhasebe yanlışlıkları ve aktarılmamış banka işlemleri belirlenip düzeltilebilmektedir. En etkisiz yöntem ise sayısal analiz bulunmuştur; bu yöntem bankalarca pek bilinmemekte, hile göstergelerini hile türü ile eşleştirmede denetçilere yardımcı olmamakta, sadece potansiyel bir sorun olduğuna işaret etmekte, dolayısıyla hile türü ve hilekarın kimliğinin belirlenmesi için hile incelemecilerinin ayrı bir çalışma yapması gerekmektedir. (Rahman ve Anwar, 2014:97-102) 2012'de İngiltere'de saptanan hile önleme faaliyetlerinde en sık kullandıkları araçlar arasında elle yapılan geleneksel incelemeler (*manual reviews*), işlemlerin izlenmesi (*transaction monitoring*), geri arama işlemleri (*call back procedures*) ve sıradışı yöntemler (*out-of-pattern detection*) gelmektedir. Tüm bu faaliyetler için bankalarca 13 milyar dolar harcama yapılmıştır. (Mazur, 2014:11) Son dönemde hile önleme maliyetlerindeki düşüş, bir dizi bankacılık uygulamasına (*ülke içi ve dışı daha yaygın chip ve pin kullanılması, mastercard ve visanın güvenlik kodlarının daha çok kullanılması, hile önleme araçlarının bankalar ve satıcılar tarafından daha çok kullanılması*) bağlanmaktadır. (Ash, 2011:16) Elektronik bankacılık hilelerinin azalmasının olası nedenleri arasında müşterilerin güncel virüs programlarıyla kendi kişisel bilgisayarlarını korumaları, bankaların gelişmiş hile saptama yöntemleri kullanmaları ve müşterilerine internet bankacılığına girmeleri için ek yazılımlar ve elle kullanılabilen aygıtlar vermeleri bulunmaktadır. (CFS, 2012:3) Hile sayısının azalması olumlu olmakla birlikte hilekarların dikkatlerini eldeki olanakları ve çözümleri en iyi biçimde kullanmayan hedef kuruluşlara çevirdiği ve yeniden saldırıda bulunmak amacıyla yeni kanal, ürün ve fırsat arayışı içinde olduğu düşünülmektedir. (Gold, 2014:17)

Sanal dünyada yapılan hilelerin etkili biçimde saptanmasında birçok hizmet kanalları ve birçok ürünün davranış biçimlerinin belirlenmesine ve analizine gerçek zamanlı olarak olanak veren bir sistem de iş analizleridir (*business analytics*). Bunlar tahmin modellerince desteklenen saptama, önleme ve soruşturma kurallarının uygulanmasında kullanılabilmektedir. Bu analiz salt suç türlerini doğru biçimde belirlemeye yardımcı olmakla kalmamakta, aynı zamanda ve gerektiğinde her bir işlemin gizlendiği ve çapraz kanalların kullanıldığı suçların ortaya çıkarılmasını da desteklemektedir. İş analizi tarafından desteklenen başarılı bir hile önleme stratejisinde analiz edilecek verinin niteliğini iyileştirmek (*doğru veriye ulaşmak*), kurumların hile ile mücadelelerinde ulaşabilecekleri sonuçlar üzerinde önemli bir etkiye sahiptir. Tüm kurum ölçeğinde finansal suç yönetim sürecini birleştirilmesi ve hileye karşı ekipler oluşturulması durumunda parçalı yaklaşımlar yok edilerek doğru veriye erişim sağlanabilmektedir. (Ajah ve Inyiama, 2011:17)

Bankacılık hilelerinin önemli bir bölümünü oluşturan elektronik hileleri ortaya çıkarmaya yönelik çözümler tepkisel (*reactive*) , önleyici (*proactive*) ya da bunların bir bileşimi olabilmektedir. (Excell, 2012:8-10) Tepkisel çözümler, hile yapıldıktan sonra yapanları belirlemek, hilenin nasıl yapıldığını ortaya koymak ve gelecekte aynı hilenin yapılmasını önlemek amacıyla kullanılmaktadır; bunlar ödemelerin bloklanması ve web sitesine erişimin yasaklanması gibi çözümleri içerebilmektedir, ancak bu yaklaşım kusurludur, çünkü öncelikle hilenin yapılmasını gerektirmektedir. Önleyici çözümler ise, suçu hile yapılmadan önce engellemeye yöneliktir. Bu çözümler hile yapması olası müşterilerin risklerini belirlemeye çalışmakta ve belirlenen risk düzeyine bağlı olarak söz konusu müşterilerin işlemleri sınırlandırılabilmektedir. Bu yaklaşım, şirketlerin elektronik hilelere açıklık derecesini düşürürken, müşterinin sınırlı da olsa işlem yapmasına izin vererek dışlanmamasını yanında getirmektedir. Önleyici stratejiler hesap, işlem ve ağ düzeylerinde müşteri bilgilerinin, işlemin yapıldığı makinaların ve müşterinin kullandığı ödeme yöntemlerinin doğruluğunu sağlamak için birçok kontroller gerçekleştirmektedir. Söz konusu kontroller hileli noktaları belirlemede iyi bir başlangıç noktası oluşturmasına rağmen doğru görünen ve fakat gerçekte hileli davranışları saptamakta etkili olamamaktadır. Nitekim hileli işlemlerin yasal işlemlere gittikçe daha çok benzemesi ve dolayısıyla gerçek ve hileli işlemleri ayırt etmenin giderek zorlaşması e-finans ve ticaret şirketleri için temel bir sorun oluşturmakta ve şirketleri iki uç noktada konumlandırmaktadır: Şirketler ya elektronik hileleri önlemek için hiçbir girişimde bulunmamaktadır, ki bu daha olumsuz

sonuçların ortaya çıkmasına neden olabilmektedir ya da hile belirtisi gösteren tüm şüpheli davranışları reddetmektedir, ki bu da potansiyel olarak iyi niyetli müşterilerin ve yasal işlemlerin de reddedilmesine yol açabilmektedir. Bu aşamada, daha önce gözlenmiş olgu ve özelliklere (*başvuru sahibinin konumu, kredi özgeçmişi ve diğer müşteri işlemlerinden türetilen bilgiler gibi*) dayalı makina öğrenme yöntemleri bulunmaktadır. Sözü edilen yöntemlerin, işlemleri geçmişteki hile örnekleri ile karşılaştırmaya olanak verecek puan kartları (*score card*) bulunmakta, müşteri ya da işlem geçmişteki hileli bir davranışı sergilemiş ise uyarı vermektedir. Anılan sistem güncellenip yeni hile türleri ve yeni gözlemleri içermeye başladıkça, hileli ve hilesiz işlemleri ayıran çizgi yeniden oluşmaktadır. Ancak bu yöntemlerde hileleri bulmak için gereken veriler belirli bir tarihte toplanmakta ve analiz yapılıncaya kadar güncelliğini yitirebilmektedir. Ayrıca bu veriler genellikle kümelerin tipik özelliklerine ilişkin olduğundan saptama ve önleme faaliyetleri için sınırlı ölçüde yararlı olabilmektedir. Sinir ağları gibi statik modeller hileyi hiç kaçırmayan bir korunma mekanizması ile yasal müşterilerin reddedilerek dışlanmaması ikilemini dengelemede zorlanmaktadır. Hile ile mücadelede yeni bir yaklaşımın kilit ögesi, davranışsal analiz yapmak olmaktadır. Bu tür bir analiz Bayesgil çıkarım teorisine dayanmakta ve kendi kendine öğrenen (*self-learning*) bir hile önleme sistemi sağlayarak hileyi zamanında doğru biçimde tahmin edebilmektedir. Bayes temelli davranışsal analiz böylelikle önceki gözlem ve bilinenlerden bir sonraki düşünceyi oluşturarak gerçek zamanlı bir sistem yaratmaktadır.

Bankacılık hilelerini ortaya çıkarma ve önlemede risk faktörlerini belirlemeye özel önem verilmesi gerekmektedir, çünkü risk faktörlerini belirlemek hilelerin ortaya çıkarılmasında ilk adımı oluşturmaktadır. Risk faktörleri hilelerin başarılı bir biçimde ortaya çıkarılmasına ve hilelerin ortaya çıkarılmasında etkili yöntem ve süreçlerin tasarlanmasına yardımcı olmaktadır. (Singleton vd, 2006:125-6) Sözgelimi hile yaptığı için mahkum edilen bankacıların, mahkum edilmeyenlere ya da suçlanmayan bankacılara ve bankacı olmayanlara göre daha gösterişli (*savurgan*) yaşam biçimlerini benimsedikleri bulunmuştur. Böyle bir yaşam biçimine kavuşmak için olanakları olmayan ya da olacağına inanmayan insanlar, bu amacı gerçekleştirmek amacıyla suç eylemlerine karışmaktadır. (Balogun vd, 2013:255, 259) Kazanılan gelirlerle uyumlu olmayan yaşam biçimlerinin önemli bir risk faktörü olduğu banka iflâslarında gözlenmektedir. (Sullivan ve Webb, 2011:64) Hile risk faktörleri hilenin olduğunu kesin olarak göstermemekle birlikte hilenin olabileceği konusunda uyarıcı olmaktadır. Hile üçgeninin her üç bileşeni (*baskı ve güdü, tutum ve rasyonalizasyon, fırsat ve ortam koşulları*) de saptandığı zaman önemli yanlışlık riski yükselmektedir. (Ramos, 2003:31-2) Bununla birlikte hile risk faktörleri belirli kayıt ve koşullar çerçevesinde ihtiyatla değerlendirilmek durumundadır. (Golden vd, 2006:127-8) Uygulamada Türkiye'de denetçiler dünyadaki meslektaşları gibi tutum ve rasyonalizasyon koşulları ile ilgili finansal raporlama risk faktörlerine daha çok önem veriyor görünmekte, aynı şekilde fırsat ve ortam koşulları ile ilgili varlıkların kötüye kullanılması hile risk faktörlerinin daha etkili olduğunu değerlendirmektedir, çünkü fırsat ve ortam ile ilgili koşullar özel olarak iç kontroller ve genel olarak kontrol çevresi ile yakından ilişkili görülmektedir. (Kandemir, 2013:83)

(2002-2008) döneminde 21 OECD ülkesinden 200'den fazla bankayı içeren bir çalışmada risk göstergeleri, sermaye yeterliliği ile ilgili risk göstergeleri (*Toplam Özkaynaklar/Toplam Aktifler ve Toplam Sermaye Oranı*), varlık kalitesine ilişkin risk göstergeleri (*Karşılıklar/Toplam Krediler, Sorunlu Krediler/Toplam Krediler, Kredibilitesi Düşük Kredi ya da Özsermaye, Kredibilitesi Düşük Kredi/Özsermaye*), yönetim kalitesi risk göstergeleri (*Toplam Maliyetler/Toplam Gelirler, GÜG/Toplam Varlıklar, Kâr/İşçi Sayısı, Giderler/Gelirler*), kârlılıkla ilgili risk göstergeleri (*Kâr/Özkaynaklar, Kâr/Toplam Varlıklar, Şüpheli Varlıklar/Toplam Gelirler, z-değeri*), likidite ve kaldıraç ile ilgili risk göstergeleri (*Dönen Varlıklar/Toplam Varlıklar, Toplam Krediler/Mevduatlar, Sabit Varlıklar/Toplam Varlıklar, Eşikaltı Krediler/Özkaynaklar, Dönen Varlıklar/Kısa Vadeli Borçlar, Merkez Bankası'na Borçlar, Diğer Ticari Bankalara Borçlar*), piyasa riski yönetimi risk göstergeleri (*Toplam Faiz Giderleri/Toplam Mevduatlar, Bilanço Dışı Hesaplar/Toplam Varlıklar, Resmî Mevduatlar/Toplam Mevduatlar, Kamu Kesimi Menkul Kıymetleri/Toplam Varlıklar, Hisse Senedi Getirilerinin Değişkenliği*) olarak belirlenmiş ve toplam 25 faktör içinden bankacılık riskindeki değişikliğin büyük bölümünü açıklayan en önemli iki gösterge, sermaye ve varlık riskleri ile likidite

ve piyasa riskleri olarak bulunmuştur. (Klomp ve de Haan, 2012:3198-9)

Banka çalışanlarına ek olarak özellikle yüksek risk taşıyan bankalarda üst ve orta kademe yönetimin kontrol edilmesine özel bir önem verilmesi gereği ortaya çıkmaktadır, çünkü hilekarın şirketteki konumu ile hileden kaynaklanan kayıp ve maliyetlerin büyüklüğü arasında güçlü ve doğru orantılı bir ilişki bulunmaktadır. (Boumediene, 2014:422) Buna göre, şirket sahipleri ve yönetim kurulu üyelerinin yol açtığı kayıplar yöneticilerin yol açtığı kayıpların 3, çalışanların yol açtığı kayıpların 9 katına ulaşmaktadır. Yöneticilerin daha çok yüksek riskli bankalarda (*düşük performans gösteren ya da yüksek büyüme oranlarına sahip bankalarda*) hile yaptıkları belirlenmekte, düşük sermaye oranlarına sahip bankalarda ise yönetim hilelerine daha az rastlanmaktadır.

Banka hilelerinin özellikleri zaman içinde değişim göstermiş ve günümüzde fiktif bilgiler yaratmaktan çok gerçek bilgilerin ele geçirilmesi yoluyla yapılmaya başlanmıştır. Artan hile riski ve hileli finansal raporlama da kamu politikaları ve düzenlemelerini etkilemiştir. Bankalar ve kredi kuruluşlarıyla ilgili düzenlemelerin ve eşzamanlı olarak finansal tablo hilelerini ortaya çıkarmak amacıyla yapılan standartların değiştirilmesi yoluyla artan kamu gözetimi ve denetimi hile stratejilerini değiştirmiştir. Kamunun düzenlediği piyasalarda faaliyet gösteren firmalarda çok bilinen yanlışlıklar daha az yapılmakta, daha az finansal tablo yanlışlık oranına sahip olunmakta ve denetimin ortaya çıkardığı yanlışlık sayısı kamu gözetimi altında olmayan şirketlere göre daha yüksek olmaktadır. Yapılacak yeni düzenlemelerde, değişen banka hilesi stratejileri dikkate alınmak durumundadır. Bu çerçevede esnek varlık değerleme yöntemlerini sınırlandıran ve önemli bilgilerin açıklanmasını genişleten düzenlemeler akla gelmektedir. Bu düzenlemeler geçerli bilgiyi saklayan ve varlıkları fazla değerleyen yönetimlerin daha ağır cezalandırılması ile birlikte düşünülmelidir. Son yapılan yasa ve düzenlemeler yönetimin sorumluluğunu arttırarak, açıklama kapsamı ve niteliğini yükselterek, ceza ve yaptırımları ağırlaştırarak hileleri önlemeyi amaçlamaktadır. Sektöre özel düzenlemeler ise, muhasebe ve denetim standartları aracılığıyla banka ve kredi kuruluşlarındaki finansal raporlamanın güvenilirliğini yükseltmeyi amaçlamaktadır. Kamu ve özel düzenlemelerin etkili bir bileşimi hilelerin ortaya çıkarılması becerisini yükseltebilecektir. Dolayısıyla, halka açık şirketler için yapılan düzenleme, standart ve kuralların tüm bu noktaları da dikkate alarak kamunun güvenini sağlayacak ve sürdürecek yeterlilikte olması beklenmekte, kamu düzenleyici ve diğer yasal kuruluşların hileli finansal raporlamayı caydıracak yapıda olması istenmektedir. (Green ve Reinstein, 2004:87-8, 90, 104-5) Güçlü ve etkili makro ve mikro gözetim, risklerin erkenden saptanması için gerekli olan önemli düzenleme bileşenlerinden birisidir. Politika oluşturucular ve düzenleyicilerin finansal tüketicilerin korunması ile birlikte etkinlik, tam rekabet, sosyal olarak yararlı bilgiler ve kamu güvenini de dikkate alarak piyasaların işlerliğini sağlaması gerekmektedir, ancak finansal sektördeki birçok faaliyet yıkıcı ve verimsiz kabul edilmektedir. Görevi kötüye kullanma (*kötü yönetim*) ve piyasa yetersizlikleri salt bireysel finansal hizmetlerde değil, tedarik zincirinin her aşamasında (*yatırım bankacılığı ve kurumsal fon yönetimindeki çıkar çatışmaları, sektörel verimsizlikler ve değer kayıpları, libor manipülasyonu gibi*) söz konusudur. Bu nedenle, yeni düzenlemelerin geliştirilmiş kurumsal yönetim ve iş etiği ile birlikte piyasa güçlerini dizginlemesi, piyasanın başarısız olmasına neden olan temel nedenlere erken müdahale edilmesini sağlaması, cezalar ve ödüller arasında sağlıklı bir orantılılık (*hastalıklı davranışları ve piyasa verimsizliklerini cezalandırmak ve doğru davranış, gerçek rekabet ve yeniliği ödüllendirmesi*) kurması, risk ve getiri arasında uygun bir orantılılık oluşturmasına gereksinim bulunmaktadır. Daha sıkı düzenlemeler olmadan salt kurumsal yönetim, etik ve gerçek rekabet ile zorunlu ilerleme sağlanabileceğine ilişkin çok az kanıt görülmekte, geçmişte kötüye kullanıldığı için öz düzenleme güvenilir kabul edilmemektedir. (Wehinger, 2013:81, 83-6) Hile ile ilgili yasal düzenlemeler asgarî standartları belirlemekte, kurumlara ve kurumların ilgili birimlerine kendi hile stratejilerini belirlemeleri için inisiyatif tanımaktadır. Dolayısıyla her bir kurum hangi düzeyde korumaya sahip olduğu ve sahip olması gerektiğine kendisi karar vermektedir. (Excell, 2012:9) Burada önemli bir nokta, düzenleme ve denetim ile banka riski arasındaki ilişkilerin tüm bankalar için aynı olmamasıdır; düzenleme ve denetim düşük riskli bankalar üzerinde değil, yüksek riskli bankalar üzerinde etkili olmaktadır. (Klomp ve de Haan, 2012:3208)

Kamu düzenlemelerine ek olarak, merkez bankalarının da ticari bankaların yeterli sermayeye sahip olması ile finans sektöründe kurumsallaştırma ve sterilizasyon çalışmaları konusunda kararlı olmaları tüm yerli ve yabancı banka müşterileri ve yatırımcılarının sektöre güvenini pekiştirmektedir. Ancak yasa ve kuralların uygulanması sadece düzenleyici kurumlardan beklenmeden devletin tüm ilgili kurumları işbirliği içinde, korkusuzca ve kimseyi kayırmadan yasa ve kuralların uygulanmasını gözetmelidir. Yapılanlar ve yapılabilecekler arasındaki yaşamsal bağlantı noktası, siyasetin yasaları uygulamak ve yasa dışı durumları cezalandırmak konusunda kararlı olması ve bunu taahhüt etmesi olmaktadır. Düzenleyici (*kamu*) ve uygulamacıların (*bankalar*) birlikte hileleri azaltmayı ve yok etmeyi taahhüt etmeleri durumunda bu yapısal sorun önemli ölçüde ortadan kaldırılabilmektedir. (Idolor, 2010:76) Ayrıca bankalar, düzenleyici kuruluşlar ve para otoritelerinin hile inceleme birimleri kurmaları, gerek kamu, gerekse özel kesimin saydamlık ve hesap verilebilirlik konusunda topluma rol modeli oluşturmaları ve uluslararası hile şebekelerinin ortaya çıkarılması ve ülke bağlantılarının saptanabilmesi için uluslararası toplum ve kuruluşlarla işbirliğine gidilmesi bankacılık sisteminin sağlamlığına ve bankacılık sistemine güvenin yeniden kazanılmasına katkıda bulunabilecektir. (Balogun vd, 2013:260)

Sonuç olarak, hile tehditleri ucuz bir alışveriş yapmak isteyen müşteriden sistemin zayıf noktalarını arayan ve suçu meslek haline getirenlere kadar çeşitli kaynaklardan gelebilmesi ve müşterilerin kolaylıkla yalan söylemelerine olanak veren yeni kanalların ortaya çıkması dolayısıyla finansal kuruluşların hileyi ortaya çıkarma yöntemleri hiçbir zaman statik kalmamakta ve hilekarlardan bir adım önde olmak için sürekli gözden geçirilmeye ihtiyaç duymaktadır. Bu nedenle, hile ile mücadele etmek için tek bir yöntem başarılı olmamaktadır; doğru yaklaşım iyi ticaret uygulamaları, eğitim, önleme ve ortaya çıkarma faaliyetlerinin uygun bir bileşimini bulmayı (Ajah ve Inyiama, 2011:17) ve dolayısıyla tek bir bileşene ya da yönteme güvenmek yerine tüm caydırma, önleme, ortaya çıkarma, telafi etme, analiz, inceleme, soruşturma ve yargılama bileşenlerinin eşzamanlı olarak uygulanması, bütünleştirilmesi ve güncellenmesini gerektirmektedir. (Rahman ve Anwar, 2014:102) Hileyi önleme hedefi hareketli bir hedef konumunda olduğu (Ash, 2011:16) ve suçlular bankaların zayıf noktalarını kapatmak için yaptıkları savunma mekanizmalarını sürekli yokladıkları için bankaların da söz konusu mekanizmaları sistematik olarak yeniden değerlendirmeleri ve yapılandırmaları gerekmektedir. (Ginovsky, 2013:21)

4.2. Özel Amaçlı Bankacılık Hilesi Saptama ve Önleme Yöntemleri

4.2.1. Kredi Hilelerinin Saptanması ve Önlenmesi

Kredi hilelerinin ortaya çıkmasında uygun ortam ya da koşullar birinci derecede önem taşımaktadır. (Khanna ve Arora, 2009:1-3, 5, 10-1) Bu çerçevede, yetersiz ve zayıf iç kontroller, iç kontrollerin uygulanmasında gevşek kurumsal kültür, gerekli risk kontrollerinin eksikliği ya da yokluğu, ilgili personelin duyarsızlığı ya da kendine aşırı güvenmesi özellikle anılmaktadır. Dolayısıyla, hile ile mücadele etkin bir iç kontrol sistemi kurmak ve kurum içinde mevcut sistemlerin açıklarının belirlenmesi ile başlamaktadır, çünkü hilekarlar ilk olarak kontrol yöntem ve işlemlerindeki açıkları belirlemektedir. Örneğin zimmetine para geçiren kişilerin ortak özelliği, iç kontrollerde bir açık yakalayıp kendi yararına bunu fırsata çevirmeleri olmaktadır. Kontrollerin varlığı ve uygulanması potansiyel hilekar için yönetimin işini takip ettiği konusunda bir işaret oluşturmakta ve böylelikle olası hile fırsatlarını caydırıcı olabilmektedir. Bu nedenle, kamu ve düzenleyicilerce önceden belirlenmiş güvenlik amaçlı önlemlere en yüksek uyum iç kontrol uygulamalarında (*yöneticilerde %93 uyum*) görülmüştür. Bu tür hilelere karşı alınacak temel önlem ise kredi müşterisini iyi tanımak, hem yeni, hem de mevcut müşterileri olabildiğince yakından tanımak (*due diligence investigation*) amacıyla politikalar belirlemek ve bu politikaları özenli ve titiz biçimde uygulamaktır. Bankalar kamunun parası ile uğraştıklarından kendi içinde hile ile mücadelede güvenlik bilincini yükseltmek ve çalışanlarını gerekli özen ve titizliği gösterecek ve belirli bir kuralın neden uygulanması gerektiği ve tam olarak uygulanmaz ise sonuçlarının ne olabileceğini anlayacak biçimde eğitmek durumundadır. Nitelikli eğitim, bankaların yalnızca işleriyle ilgili yeteneklerini geliştirmelerine yardımcı olmamakta, aynı zamanda potansiyel performanslarını en yüksek noktaya çıkarmaları ve bankacılık ilke ve uygulamalarını anlamaları için sağlam bir

bilgi tabanı sağlamaktadır. Ayrıca çalışanlar için ay içinde zorunlu izin uygulaması başlatılması durumunda, yolsuzluğa karışan banka çalışanlarının yapmış olabileceği kural ve etik dışı işler onların yokluğunda daha kolay ortaya çıkarılabilmektedir. Banka çalışanlarının kişisel yaşam biçimi de zaman zaman gözden geçirilmekte, gelirleri ile harcamaları arasındaki tutarsızlıklar belirlenmektedir. Öte yandan, görevdeki banka çalışanının yolsuz olması hilelerin en önemli nedenlerinden birisi olduğundan işe alma sürecinde genel yetenek, mülakat ve tıbbi incelemeye ek olarak bankacılık hizmetlerine yönelik psikiyatrik ve psikolojik testler yapılması yararlı olmaktadır. Konulan kurallara tam uyumun sağlanması için personel sayısını yeterli düzeye getirmek, banka yönetici ve çalışanları arasındaki iletişim sürecini hilelere ilişkin bilginin yayılmasını sağlayacak biçimde iyileştirmek ve finansal kuruluşlar ve bankalar arasında hilekarın davranışları, tercihleri ve tipolojileri konusunda daha çok bilgi paylaşımı sağlamak da önem taşımaktadır. Bu durum özellikle bilgisayar kullanımının çok yoğun olduğu ve bilgi teknolojilerinin hızla değiştiği alanlarda giderek önem kazanmaktadır. Son olarak imza her zaman sahteciliğe açık olduğu, bankacılık sektörü giderek kişisel ilişkilere dayalı olmaktan çıktığı, banka müşteriyi fiziksel olarak görmediği ve sadece müşterinin imzasını tanıdığı için kredi verme zincirinde yer alan çalışanların ve kredi müşterisinin imzalarıyla birlikte parmak izi görüntülerinin de alınması ve karşılaştırılması da hile ile etkin mücadeleye katkıda bulunabilmektedir. Bu nedenle müşteri uzun ve belirgin imzalar atmaya özendirilmeli, zaman içinde imzalar değişebileceği için her beş yılda bir örnek imzalar yeniden alınmalı, banka çalışanlarına imzaları karşılaştırma konusunda yeterli eğitim verilmelidir.

Kredi müşterilerinin tanınması ve doğrulanması yaşamsal önemde bir süreçtir. Bu çerçevede müşterilerin kimliğini bankalar kendisi doğrulatmaktadır. Kredi müşterisinin finansal varlıklarının banka ya da başka bir kuruluş tarafından ayrıca doğrulatılması gerekmektedir. Kredi müşterisinin izni ile müşterinin hesap bilgilerini doğrulayan ve bankalara bu bilgileri anlık biçimde veren varlık doğrulama teknolojileri (*account check*) bulunmaktadır. Bu teknolojiler sadece müşterinin finansal tablolarını bulup çıkarmaktan ibaret olmayıp müşterinin ortalama bakiyeleri, toplam para yatırış ve çekişlerini hesaplamakta, nakit sıkıntısına düşme ve bunun maliyetlerine katlanma durumlarını da saptayabilmektedir. Düzenleyiciler ise kredi dosyalarının kalitesini arttırmayı, kredi müşterilerinin borçlarını geri ödemesini güvence altına almayı ve genel olarak yeni bir finansal krizden kaçınmayı istemektedir. Kredi oluşturma sürecinden elle ve geleneksel olarak yapılan ne kadar çok temas noktası uzaklaştırılabilir ise, hile ve hata olasılığı o kadar azaltılabilmekte ve bir kredinin yaşam süresinde yapılabilecek tasarruflar o kadar yükseltilebilmektedir. Böylelikle kredi kuruluşları güvenli ve elektronik doğrulamalar yapabilmekte, güncel finansal tabloları bulmaya çalışmamakta ve basit hesaplamalar için zaman ayırmaktan kurtulmaktadır. Uzun vadede ise varlık doğrulama teknolojileri doğrudan bilgi kaynağından birincil veri sağlaması ve doğru kredi dosyalarının hazırlanmasına destek olarak daha çok ipotekli konut satışı ve daha çok kredi ile sonuçlanabilecektir. Varlık doğrulama teknolojileri özellikle kredi dosyasında kasıtlı olmayan yanlış hesaplamalar ya da basit insani yanlışlıkları krediyi geri satın almaya (buying back the loan) ya da ipotekli konutu haczetmeye oranla çok daha az maliyetle giderebilmektedir. (Chandler, 2014:82 ve 87)

Çeşitli müşterilere hizmet vermek isteyen bankaların kredi kararları çeşitli ve büyük miktarda veri kullanımı ve bu verileri işlemek amacıyla uzun zaman gerektirdiğinden kredi değerleme ve risk yönetim sistemleri otomasyona tâbi tutulmaktadır. (Ajah ve Inyiama, 2011:1-4, 7-9, 10-1, 17) Otomasyonun ilk düzeyi, kredi kararını destekleyen elektronik (*online*) sorgulamaların kredi değerleme sistemine verilmesi ve bankanın not karnesinde başvuru sahibinin değerlenmesidir. Banka bu sayede kredi portföyünü en az zarar ve kabul edilebilir getiri çerçevesinde ve gelişmeler meydana gelmeden önleyici nitelikte yönetebilmektedir. Etkili bir kredi yönetim sisteminde olması gereken başlıca teknolojiler kimlik kartında biyometri (*biometrics*), sayısal sinir sistemi (*digital nervous system*), yapay zeka teknolojisi (artificial neural networks), akıllı ajanlar (intelligent agents), veri madenciliği ve grafik bilgi sistemleridir. İkinci düzeyde bankalar, sağlıklı bir kredi değerlendirme sürecine (*loan processing*) sahip olmak zorundadır. Bunun için kredi kararının verilmesi ve onaylanması, görevli banka çalışanının kişisel inisiyatifine bağlı olmaktan çıkarılmakta ve standart bir kredi risk yönetim sistemi kurulmaktadır. Finansal kuruluşlar kredi inceleme sürecinin başlangıcında

kapsamlı bir ön inceleme (*a thorough background investigation*) yaparak sorunlu kredi ve karşılıklarla karşılaşma olasılığını düşürmektedir. Müşterilerin mali geçmişlerinde görülen İflaslar, ödenmeyen krediler, farklı adlar daha derin soruşturma gerektiren risk faktörleridir. Bankalar bu amaçla kredi risk yönetim süreçlerinin müşterinin kredi bilgilerini birçok veri tabanından toplayabilecek ve bankanın kendi izleme ölçütlerine göre bu verileri bir tür not karnesinde izleyebilecek düzeye gelmesini sağlamaktadır. Bu notlar daha ileri düzeyde inceleme gerektiren alanları risk yöneticilerine göstermeye yardımcı olmakta, deneyimli bir bankacı çeşitli tipte müşterilerin temerrüt risklerini doğru değerlendirebilmektedir. Kredi faaliyetleri üzerinde etkili bir yönetsel kontrol için doğru ve gerçek zamanlı bilgilerin hızlı ve nesnel biçimde analiz edilmesi zorunluluğu bulunmaktadır. Bu amaçla bankalar kredi risk yönetimi grupları oluşturmakta ve bunlara bir dizi sorumluluk (*kredi yaşam döngüsünün yönetimi, uygun risk dağılımının güvence altına alınması, portföy risk ölçümlerinin geliştirilmesi, riske dayalı performansın arttırılması gibi*) yüklemektedir. Bu gruplar yoğunlaşma görülen noktalarda risk aralıklarını, dayanıklılık (*stress*) sınırlarını ve sermaye gerekliklerini sektör, piyasa ve faaliyet dalı temelinde belirlemekte, bu amaçla gerek banka içindeki, gerekse banka dışındaki risk yönetim ağları ile düzenli olarak iletişime geçmektedir. Risk ağları ile doğrudan bağlantı içinde olmak bankaların sözleşme koşullarını piyasaların beklentilerine uydurmasına olanak vermekte, dolayısıyla banka risk bilincini arttırmakta ve risk fiyatlama sürecini iyileştirmektedir.

4.2.2. Hesap Hilelerinin Saptanması ve Önlenmesi

Bu tür hilelere karşı en etkili araç, borçlunun (*müşterinin*) tanınmasına (*customer identification*) yönelik bir politikaya (*know-your-customer*) sahip olmaktır. Sürdürülebilir ve etkili bir ödeme sistemi olan bankalar borçları borçlular ile ilişkilendirme yeteneğini, başka bir deyişle ilişkide oldukları müşterileri tanımalarını sağlayan yeterli kontrol ve kuralları belirlemek ve uygulamak zorundadır. (Hartman-Vendels vd, 2009:348-50, 357) Bu çerçevede, bankalar müşterinin kimliğini saptamak için gerekli olan tüm bilgileri ve özellikle yasadışı olarak elde edilmesi ya da sahtecilik yapılması çok zor olan belgeleri almaya zorlanmaktadır. Ayrıca bankalardan hiçbir zaman yeni bir müşteri görüşmeye gelemediği için kimlik belirleme ve doğrulama ile ilgili kuralları kısaltarak uygulamaktan kaçınması istenmektedir. Yüz yüze olmayan müşteriler için etkili bir kimlik belirleme yöntemi, saygın üçüncü bir tarafın bağımsız bir doğrulama yapması olmaktadır. Almanya'da internet bankacılığı yapan herkesin güvendiği bir mekanizma, Alman Posta İdaresi'nin verdiği kimlik tanıma sistemi olmuştur. Öte yandan, hile riskinin demografik ve sosyo-ekonomik değişkenlere (*uyrukluk, cinsiyet, medeni durum, yaş, meslek, kentleşme gibi*) yüksek düzeyde duyarlı olduğu saptandığı için söz konusu değişkenlerin hile ile mücadele politikalarının oluşturulmasında dikkate alınması gerekmektedir. Son olarak, hesap açma başvurusu ile eşzamanlı yapılan hesaptan fazla para çekme (*limiti aşma*) başvurusu hile riskini olağanüstü arttırmaktadır. Bankalar hesap hilelerine karşı önlem olarak yoğun biçimde otomasyon modelleri kullanmaktadır. Burada amaç, her bir hesap başvurusu için yanlış kimlik riskini değerlendirmektir. Hesap hilesi riskine karşı umut veren bir çözüm önerisi de, olası hilekarı hilekar olmayanlardan ayıran tarama kurallarına benzer biçimde, yeni hesap başvurusu yapanların kredi değerlemesini yapacak yöntemleri geliştirmek olmaktadır. Bu çerçevede, bankalar uyrukluk, cinsiyet, medeni durum, yaş, mesleki durum ve kentleşme gibi başvuru formlarında yer alan göreli olarak ucuz ve eldeki hazır bilgileri (*hile tahminleyicileri, risk faktörleri*) hesap hilesi riskinin değerlendirilmesinde yüksek doğruluk derecesiyle kullanabilmekte ve başvuru sahiplerini hile risk kümelerinde sınıflandırabilmektedir. Ancak başvuru formlarına dayalı tahminleme amaçlı tarama kurallarının çok gizli tutulması gerekmektedir.

Kredi değerleme sürecinde kimlik hilelerine karşı en iyi savunma, önleme faaliyetleridir. (Ghosh, 2010:12-3) Bu faaliyetler genel olarak kurumsal hile politikalarının tasarlanması, ihbar sistemleri, hile olaylarının kamuya duyurulması, özelde ise yeni müşterilerin daha yakından tanınması, istatistiksel modeller yardımıyla yeni başvuruculuların bilgilerinin kara listeye alınmış müşteri bilgileriyle eşleşip eşleşmediğinin önceden kontrol edilmesi, müşteriyi satış sonrasında da tanımaya ve kimliğini doğrulamaya yönelik işlemler, aynı müşterinin sisteme farklı bilgilerle girişinin sınırlandırılması, hizmet tutarının sınırlandırılması ve kredi değerlendirme politikalarının sıkılaştırılması belirtilmektedir. Önleme faaliyetleri etkisiz kalır

ise, ilk savunma hattı saptama faaliyetleridir; hilelerin erken teşhis edilmesi yaşamsal önemdedir, çünkü hilelerin hızı ve büyüklüğü geometrik olarak artmakta ve hileler ortaya çıkarılmadığı sürece hilekarlar kendilerine güven kazanmaktadır. Özellikle gerçek zamanlı hile saptama sistemleri bir dizi kural motoru ve davranışsal teknolojiler ile birlikte kullanıldığında yasal işlemleri yavaşlatmadan hileleri erken aşamalarda ortaya çıkarmakta çok etkili olabilmektedir. Hile ortaya çıkarıldıktan sonra tahmini hile risklerinin kim tarafından yaratıldığı, hilenin nasıl, ne zaman ve neden yapılabileceği ise araştırma faaliyetlerini oluşturmaktadır. Son olarak, bir sonuca varmak amacıyla geçmiş, bugün ve gelecekteki hile güdüleri ile davranışlar arasında ilişki kurarak çözüm önerileri bulunmaya çalışılmaktadır. Bu tür hilelere karşı mücadelenin diğer bir ayağı kullanıcılar ile birlikte operatörlerin bilinçlendirilmesi olmaktadır. Bu durum hem müşteriler, hem de şirketler (*bankalar ve tacirler*) için geçerlidir. İşletme içinde operatörler hile saldırılarına karşı korunmak için bir hile yönetim yapılanması oluşturmaktadır. Bu yapılanmanın üç kurumsal dayanağı süreç (*hilekarlar için hiç boşluk bırakmayan ya da bunları asgari düzeye indiren iyi tanımlanmış ve işletmeye özgü tasarlanmış kurallar*), araçlar (*işletme ağlarına ve süreçlerine uygun bir hile yönetim sistemi ve teknolojisi*) ve insanlar (*iyi donanımlı ve eğitimli bir hile ile mücadele ekibi*) olmaktadır. Bu bağlamda, kamu politika oluşturucuları, tüketicilerin çıkarlarını korumak için operatörler ile el ele vermek durumundadır. Hesap hileleri kapsamında ele alınabilecek zimmet hilelerinde Idolor (2010:66), önleme etkinlikleri yanında özellikle müşterilerin banka hesaplarının mutabakatlarının yapılmasını önermektedir.

4.2.3. Plastik Kart Hileleri ve Kartsız Hilelerinin Saptanması ve Önlenmesi

Plastik kart hileleri ile savaşım belirli zorluklar içermektedir. (Krivko, 2010:6070-1) Bir kez, plastik kart çıkaran şirketler tarafından her gün gerçekleştirilen işlem hacmi yüksektir ve her bir işlem 70'den çok kodlanmış bilgi alanı içermektedir; işlem verileri heterojendir ve hesapların kendi içinde ve hesaplar arasında zamana göre değişkenlik göstermektedir; eğilimler ve modeller farklı tacir, coğrafi bölge ve tatil dönemleri arasında önemli derecede farklılık göstermektedir. Başka bir zorluk, bu tür hilelerde genel kabul görmüş hile oranı %0,1-0,2 düzeyinde olup hile olasılığı çok düşük görünmektedir. Bu durum, gerçekte hile saptama sistemleri tarafından hile potansiyeli olan işlem olarak belirlenen işlemlerin çoğunun yasal işlemler olduğunu göstermektedir. Bu tip hatalar olumlu yanlışlar (*false positive*) olarak nitelenmekte, bunların sayısı arttıkça da ilgili maliyetler ve müşteri memnuniyetsizliği artmaktadır. Ayrıca hile saptama sistemlerinin üzerine kurulduğu veriler sağlıklı olmayabilmektedir. Bu sistemlerin yakalayamadığı hile olayları, kart sahibi hesabına gizlice girildiğini fark ettiğinde kart çıkaran şirketlere rapor edilmekte, bu ise aylarca sürebilmektedir. Dolayısıyla her bir durumun doğru tanılanması gecikmekte, kimi zaman bu bile mümkün olmamaktadır.

Bu koşullar altında, hileleri caydırmak ve hileden kaynaklanan maliyetleri azaltmak için bankacılık sektörü ve bireysel olarak bankalar chip, pin, kart okuyucu güvenliği ve güvenlik doğrulatma soruları gibi çeşitli sistemler kullanmaktadır. Hile saptama sistemleri, önleme faaliyetleri başarısız olunca ve kural ihlâllerini engelleyemeyince devreye girmektedir. Hile saptaması, genellikle işlem düzeyinde sınıflandırmaya ve hileli/hilesiz işlemlerden oluşan örneklemlerden hareket edilerek olası yeni olaylar için atama yöntemlerine dayanmaktadır. Hile saptama sistemleri tarafından verilen uyarılar hile inceleme bölümüne aktarılmaktadır. Uyarı sayısının hile incelemecisi ve analizcileri tarafından ele alınabilecek düzeyde tutulması zorunluluğu bulunmaktadır. Şüpheli durumlar banka politikaları gereği işlemin doğrulanması için kart sahibi ile iletişime geçilerek izlenebilmektedir. (Krivko, 2010:6070-1)

Özel ve kamu kuruluşları günümüzde daha çok kredi kartı hile girişimi ile karşılaştığı, kart sahiplerinin kartla ilgili hile, hırsızlık ve kayıp bildirimlerinin güvenilir bulunmadığı ve analizci çalışan için büyük sayılı örneklemler, çoklu boyutlar, gerçek zamanlı güncellemeler ve simgeleşmiş işlem veri kümelerinden yola çıkarak hile modellerini ortaya çıkarmak kolay olmadığı için hileli davranışın ortaya çıkarılmasında kayıt altına alınan işlemlerin otomatik analizine ve otomasyon sistemlerine gereksinim duymaktadır. (Dal Pozzola vd, 2014:4915-6) Buna göre, kredi kartı her kullanıldığında, işlem verileri (*kredi kartı tanıtıcısı, işlem tarihi, alıcı, işlem tutarı gibi*) bir dizi özelliğiyle birlikte hizmet sağlayıcının (*bankanın*) veri tabanlarında saklanmaktadır. Ancak tek bir işlemin

bilgisi hilenin saptanması için yeterli olmamakta, yapılacak analizde anakütle ile ilgili ölçüler (*günlük harcama tutarı, haftalık işlem sayısı, ortalama işlem tutarı gibi*) de göz önüne alınmaktadır. Bu çerçevede, etkili hile saptama algoritmalarının tasarımı hileli kredi kartı işlemlerinden kaynaklanan büyük kayıpları azaltmak için kilit önem taşımaktadır. Söz konusu algoritmalar hileyi araştıranlara yardımcı olmak üzere gelişmiş makina öğrenme tekniklerine daha çok dayanmaya başlamıştır.

Kredi kartı hilelerinde Bayesgil çıkarım yöntemi de otomasyon sistemleri kapsamında ele alınabilmektedir. Burada hile uzmanlarının yeterli düzeyde deneyime sahip olması önemlidir, çünkü hile nadir görülen bir olaydır, belirli bir veri kümesinden seçilerek yapılmamıştır ve dolayısıyla salt geçmiş gözlemlere dayanmak birçok hile türünün gözden kaçırılmasına neden olmaktadır. Ancak alanında uzman kişilerin sezgileri de geçmiş veri kümelerine eklenir ise, daha geniş bir potansiyel hile alanını kucaklamak mümkün olabilmektedir. (Excell, 2012:10) Aynı kapsamda, potansiyel hile olaylarını ortaya çıkarmak için gerçek zamanlı hile saptama yöntemleri gibi yenilikçi yaklaşımlar söz konusudur. (Quah ve Srinagesh, 2008:1721-2) Bunlar hileleri bulmak amacıyla tüketicinin harcama davranışı ve kalıplarını ortaya koymakta, filtrelemekte ve analiz etmektedir. Araştırmalara göre, hileli işlem tarihi ile kredi kartı geri ödemesi bildirim tarihi arasında geçen ortalama sürenin 72 gün olması hilekarlara büyük maliyetler yaratmaları için uzun bir zaman vermektedir. Dolayısıyla hileleri gerçek zamanlı saptamanın önemi giderek artmıştır. Son olarak geliştirilmiş ve kullanımda olan teknikler arasında işlemlerin ileri düzeyde taranması, tüketici davranışı ve harcama kalıplarının izlenmesi gibi yöntemler hem tacirler, hem de kart çıkaran bankalar tarafından kullanılmaktadır. Aynı şekilde, adres doğrulama sistemleri (*address verification systems*) müşteri adres posta kodunu, kart doğrulama yöntemi (*card verification method*) ve kişisel kimlik numarası (*personal identification number*) ise müşterinin tuşlayacağı sayısal bir kodu doğrulatmaktadır. Biyometri imza ya da parmak izinin doğrulanmasını gerektirebilmektedir. Kural temelli yöntemler ya da müşterilerin beyaz/kara listelerinin tutulması da uygulamada kullanılmaktadır. Veri madenciliği (*data mining*) ve kredi değerleme (*credit scoring*) yöntemleri, hileleri ortaya çıkarmak için istatistiksel analizlere ve tüketici davranış kalıplarının ortaya çıkarılmasına dayanmaktadır. Sinir ağları (*neural networks*), müşterinin geçmişte yaptığı işlemlerden kalıplar türetme yeteneğine sahip bulunmaktadır ve değişen koşullara ve hile yöntemlerine uyarlanabilmektedir.

Kartların gerçek mi, sahte mi olduğunu anlamak ve doğrulamak ödeme kartları ile ilgili hileler ortaya çıkarılırken büyük önem taşımaktadır. (Souvignet vd, 2014:144) Bunun için sihirli bir değnek olmasa da, iki faktörlü ve yönlü doğrulama (*two factor, two-way authentication*) çözümleri interneti bankacılık için güvenli bir kanal durumuna getiren kilit bir uygulama niteliğindedir. (CTT, 2006:11) Elektronik ödemelerin artması ile birlikte elektronik işlemlerle ilgili tüketici bilincinin artması ve bankalar üzerinde müşteriyi kaybetmeme baskısı etkili doğrulamanın önemini arttırmıştır. (Brunswick, 2009:12-3) Bu çerçevede, bankaların bütün ödemeler alanını kapsayan güvenlik önlemleri alıp uygulamaya geçirmeleri ve MasterCard ve Visa'nın daha güvenli elektronik alışveriş ortamı yaratmalarına yönelik girişimlerini desteklemeleri gerekmektedir. Nitekim İngiltere'de çoğu banka güvenli elektronik bankacılık için MasterCard ve Visa'nın doğrulama programını (*Chip Authentication Programme, CAP*) destekleyen yazılım ve donanımlara (*kart okuyucularına ya da CAP uyumlu kartlara*) yatırım yapmıştır. CAP ya da mobil doğrulamanın her ikisi de, tüm elektronik işlemler için şifreli ve güvenli bir ortamda kullanıcının daha büyük olasılıkla doğrulanması için ortak bir platform olarak kullanılabilmektedir. Müşterilerin kendilerini bağlantısız akıllı bir kart okuyucu ve kendi banka kartlarını kullanarak etkili biçimde doğrulamalarına olanak vermek suretiyle bankalar, transferler yapılmadan önce kimlik doğrulamasını zorunlu duruma getirmiş olmaktadır. Akıllı bir kart ya da CAP okuyucuların kullanılması bankalara iki adımlı bir doğrulama (*two-factor authentication*) olanağı sağlamaktadır.

Hile ile mücadelede etkili ve ekonomik çözümler bulmak gerekmekte, bu ise işlemlerin izlenmesi ve gözden geçirilmesi maliyeti ile hile olaylarının maliyeti arasında bir denge noktası bulunması anlamına gelmektedir. İşlemlerin daha kapsamlı olarak kontrol edilmesi ve gözden geçirilmesi hile maliyetlerini önemli derecede azaltmaktadır, ancak bu uygulama kontrol ve tarama maliyetlerini de önemli ölçüde arttırmaktadır. Herşeye karşın, hileye karşı yazılım kullanmamanın maliyeti,

2005'de 60 milyar dolar olarak tahmin edilmiştir. Toplam maliyetleri asgariye çekmenin kilit noktası, işlemleri sınıflandırmak ve sadece hile potansiyeli taşıyan işlemleri ve olayları kontrol etmek olmaktadır. Bu ise aşamalı tarama, filtreleme ve kontrol mekanizmalarını içermektedir. (Quah ve Srinagesh, 2008:1722)

4.2.4. Çek Hilelerinin Saptanması ve Önlenmesi

Bu tür hilelerin ortaya çıkarılması ve önlenmesi için genellikle ilgili belgelerin (*iptal edilen ya da kayıp çekler, banka hesap bildirimleri ve mutabakatlar dahil*) yakından incelenmesi en etkili araç olmaktadır. (Golden vd, 2006:240) Çeklerde çift imza zorunluluğu, harcamalarla çeklerin karşılaştırılması, satıcı ya da tedarikçi çizelgelerinin güncellenmesi, iptal edilen çeklerin incelenmesi, yasal defterler üzerinde yapılan düzeltmelere dikkat edilmesi, çok hareket gören ve çok az incelenen hesaplara yapılan kayıtların gözden geçirilmesi, satıcı ya da tedarikçi şikayetlerinin ciddiyetle araştırılması diğer etkili önlem ve araçlardır. (Wells, 2008:142-7). Ticari bankalar tarafından sağlanan elektronik hizmetlerden yararlanılması da çek hilelerini azaltabilmektedir. Bu çerçevede, işletmeler bankaya her dönem çeklerin tarihi, lehdarı ve tutarını gösteren bir elektronik dosya teslim etmektedir. Ödenecek çek dosyada belirtilenlerden biri değil ise, banka çeki kabul etmeden önce işletmeden onay almaktadır. Öte yandan, çekler kayıtlara geçen bir ödeme aracı oldukları için denetimde iz sürülebilmekte ve işlemden aylar ve hatta yıllar sonra dahi parmak izi ve el yazısından sonuca gidilebilmektedir. Ayrıca bankada yüz yüze ilişkiye girilmesi ve kimlik gösterme zorunluluğu olduğundan sürülecek izler çoğalmaktadır. (Biegalman ve Bartov, 2006:172-3)

Çek hileleri, eğitim, hesapların izlenmesi, imzaların doğrulanması ve düzenleyici ve diğer kamu kuruluşlarıyla bilgi paylaşılmasını gerektirmektedir. Bu aşamada, şube yöneticileri önceden tanımlı sistem ve kurallara bağlılığı güvence altına almada temel sorumluluğu taşısa da, iç denetçiler çek hilelerinin ortaya çıkarılması ve önlenmesinde özel bir konumda bulunmaktadır. Bu tür hilelerin en önemli nedenlerinden biri, üst yönetim tarafından önceden konulan sistem ve usullere uyulmasında gösterilen dikkatsizlik ve kayıtsızlık olmaktadır. Kamu düzenleyicileri tarafından konulmuş ve zamanla sınanmış korunma önlemlerinin uygulanmasında yetkili kişilerin gösterdiği ilgisizlik de, etik davranmayan bileşenler tarafından kötüye kullanılabilmektedir. Nitekim kamu ve düzenleyicilerin belirlediği güvenlik amaçlı önlemlere %100 uyum sağlandığı görülmemekte, kural ve usullere en az uyum ise çek defteri ve banka cüzdanlarında gözlenmektedir. Oysa iyi tanımlanmış bir sistem ve usullerden çok küçük bir sapma bile bankalara çok büyük zararlar verebilmektedir. Dolayısıyla, yapılması gereken kamuda ya da düzenleyici/denetleyici kuruluşlarda bir araştırma birimi kurmak ve buralarda çok deneyimli insanlar istihdam etmek ya da bunlara bağlı yeni ve daha yetkili karmaşık örgütler oluşturmak değil ve fakat banka yönetimi ve çalışanları tarafından kontrollerin kararlı biçimde uygulanması ve analiz edilmesi olmaktadır. (Khanna ve Arora, 2009:3-5)

Hileleri önleme çalışmalarında başarı oranını yükseltmek için kanıtlanmış çözümler bulunmakta, işletme içinde bir hile uyarı yönetim sistemi kurmak ve hile potansiyeli taşıyan şüpheli çekleri tarayan hile sistemleri ile tahminleyici mantıklar yürütmek bunların en başında gelmektedir. Bir finansal kuruluşun hilekarlar paraları kaçırmadan önce hileyi önlemede tepkici ya da önleyici olduğu, bir kurumsal hile uyarı yönetim sistemine yatırım yapıp yapmamasından ve tahmin amaçlı analizleri çeklere uygulayıp uygulamamasından anlaşılmaktadır. Herhangi bir işletme hile uyarı yönetimi sisteminde ne denli çok veri biriktirilir ise, hilelerin erkenden bulunması olasılığı o denli artmaktadır. Bunun yanı sıra, hilekarın finansal kuruluşların parasını alıp kaçması öncesinde hızlı ve bilgiye dayalı kararlar vermek için çek hileleri ile ilgili verileri toplu olarak değerlendirmek yerine, hesap ve daha iyisi müşteri temelinde verilerin sunduğu şüpheli durum ve belirtilerin toplanması ve değerlendirilmesi uygun olmaktadır. Elle yapılan işlemleri ve süreçleri otomasyona tabi tutmak etkili olmakta ve otomasyon sistemleri kendini 8-10 ayda amorti etmektedir. Finansal kuruluşların bu alandaki çalışmaları sonucunda, 2008'de İngiltere'de bankalardaki mevduat hesaplarına karşı gerçekleştirilen 11,4 milyar $'lık çek hilesi girişimlerinin büyük çoğunluğu (%91'i) önleme sistemleri ya da risk azaltıcı iç süreçler aracılığıyla finansal kuruluşlar zarara uğramadan engellenmiştir. Bu yenilikçi yaklaşımlara çalışanların çapraz eğitimi ve ek çalışmalar da dahil edildiğinde, hilelerin azaltılması ve bu yatırımdan ek getiriler elde edilmesi beklen-

mektedir. (Sarra, 2011:290-1) Bu kapsamda banka çalışanlarının özellikle çekler ve para transferleri ile ilgili hilelerin ortaya çıkarılmasındaki yeteneklerinin iş başında ve dışında yapılacak eğitimlerle arttırılması gerekmektedir. Bankalar tüm makbuz, çek, para çekme fişi ve ödemelerini günlük olarak kontrol etme politikası uyguluyor ise, sahte çekler kullanılarak yaptırılan sahte ödemelerin ortaya çıkarılması kolay olmaktadır. (Idolor, 2010:68, 76) Son tahlilde, çeklerin doğrulanması süreci ibraz edilen hiçbir çalıntı çek ödenmeyecek biçimde güçlendirilmeli ve titizlikle bu sürece uyulmalıdır. (Balogun, 2013:260)

4.2.5. Akreditif Hilelerinin Saptanması ve Önlenmesi

Bankalar akreditif hilelerinde yeterli deneyim sahibi olmadıklarından akreditif başvurularını incelemek amacıyla sıkı ve kapsamlı kurallara gereksinim bulunmaktadır. (Chehashim ve Mahdzan, 2014:232-5) Bu kurallar öncelikle belgelerin sahteliğini ortaya çıkarma becerisini arttıracak yeterlilikte olmalıdır, çünkü baskı teknolojisindeki ilerlemeler belgelerin kolaylıkla sahtelerinin üretilebilmesini sağlamakta ve kuşkucu davranmayan bankacıya yasal bir belge olarak görünebilmektedir. Sözgelimi başvuru sahiplerinin bankada bir hesap açtırması ve kredi kullanma olanaklarına (*fazla ve limit üstü çekim ya da sabit kredi gibi*) sahip olması zorunlu tutulabilecektir; mevcut müşteriler kredi ve yasal inceleme sürecinin gereklerini yerine getirmeli, bankada olumlu bir kredibiliteye sahip olmalı, kredi kullanan müşteriler genellikle yıllık incelemelere tabi tutulmalıdır, çünkü iyi bir kredibiliteye sahip müşterilere akreditif çerçevesinde fon tahsis eden (*kredi kullandıran*) bankalar bu şekilde daha güvenli hareket edebilecektir; akreditif başvurusunu kabul etmeden önce müşteriyi tanıma yaklaşımı da olası bir çözüm olabilmektedir. Bankaların akreditif hilelerinden şüphelendikleri zaman en çok başvurdukları yöntemler görülme sıklığına göre Tablo 5'de özetlenmiştir. Başka bir risk azaltma önlemi, ticaret yapılan yabancı ülkelerin siyasal ve ekonomik durumlarını yakından izlemek olmaktadır. Finansal ve ekonomik bunalım yaşayan ülkelerle bağlantılı akreditiflerde bankalar çok dikkatli olmakta ve hatta çoğu zaman işlem yapılmamaktadır. Özel durumlarda, bu tür ülkeler ile bağlantılı akreditifler alıcının bankasının oluru ile kabul edilebilmekte ya da koşulları pazarlığa tabi tutulabilmekte, böyle olması durumunda bankalar Uluslararası Denizcilik Bürosu'ndan yükleme belgesinin geçerliliğini onaylamasını istemektedir. SWIFT (*Society for Worldwide Interbank Financial Communication*) kullanımı da riski azaltan bir uygulama niteliğindedir, çünkü bunlar uluslararası ticareti kolaylaştırmak için verilen standart, basit ve güvenilir iletilerdir. Bu alanda yalnızca banka üst yönetimleri yetkili kılındığından SWIFT iletileri aracılığıyla verilen akreditiflerin güvenilirliği ve gerçekliği daha üst düzeyde değerlendirilmektedir. Buna karşılık faks, teleks ve uçak postası aracılığıyla verilen akreditifler konusunda bankalar daha uyanık olmak durumundadır.

Tablo 5. Akreditif Hilelerine Karşı Alınan Önlemler (%)

Ayrıntılı Belge İncelemesi	45,0
Müşteri Hesabını Dondurma	25,0
Uluslararası Denizcilik Bürosu'ndan Destek Alma	30,0
Güvenlik Birimlerine Bildirim	10,0

4.2.6. Bilgisayar Hilelerinin Saptanması ve Önlenmesi

Bilgisayar ya da bilgi sistemleri güvenliği bilgisayar hilelerini azaltmak için bir zorunluluktur; en azından bazı temel güvenlik süreçleri ile yazılım ve donanımlara sahip olunması gerekmektedir. Bilgisayar güvenliği, üç temel işleve ayrılmaktadır: Sisteme (*yazılıma, veri tabanlarına ve dosyalara*) erişimin kontrol edilmesi, bireysel hesap verebilirlik (*her bireyin ya da yazılım etkinliklerinin ayrı ve özel olarak belirlenmesi*) ve denetim işlevi (*olanları saptamak için gereken tarihsel kayıtlar*). Bilgisayar güvenlik işlevleri, fiziksel güvenlik, personel güvenliği, idari güvenlik, iletişim güvenliği, ihtimaliyat planlaması (*yıkımların giderilmesi ve risk yönetimi*) gibi ortak süreç ve sistemleri içermektedir. Amaç gizlilik, doğruluk ve güvence sağlamaktır. Bu kapsamda bilgi korunmakta ve salt bilgiye gereksinim duyulduğunda kullanılmaktadır. Hile karşıtı bir programı destekleyen bir bilgisayar güvenlik programının amacı, şirketin ve müşterilerin tüm ihtiyaçlarını karşılarken hileleri ve diğer riskleri uygun maliyetle ve çalışma düzenine en az etkide bulunarak asgariye indirmektir. Ancak iyi bir bilgisayar güvenlik programı ile bütünleştirilmiş iyi bir hile ile mücadele programı ve sıkı bir gözetim ile bu amaca ulaşmak olanaklı görünmektedir. (Kovacich, 2009:13-4)

4.2.7. Kara Para Aklamanın Saptanması ve Önlenmesi

Diğer yasadışı ticaret türlerinde olduğu gibi kara para işlemlerinde de, her iki taraf bu işin gerçekleşmesini istemektedir, ki bu durum kara para ile mücadeleyi daha da zorlaştırmaktadır. Kara para ile mücadele, mağdurun alarm verdiği hile ya da hırsızlık türleri ile mücadeleden daha güç saptanmaktadır. Bankaların kara para ile mücadelesi ülkeden ülkeye değişkenlik göstermektedir. Sözgelimi, Peru'da yöneticiler özel bir eğitimden geçirilmiş, ABD ve Orta Amerika'daki bankalar ile bilgi değişim programları düzenlemiştir. Çoğu banka ABD ve AB'deki bankacılık standartlarını karşılamak amacıyla ve devletin teşviki ile kara paraya karşı teknolojileri uygulamaya geçirmiştir. Bu teknolojiler potansiyel olarak sorunlu müşteriler ya da şüpheli işlem davranış modellerini belirleyebilecek yüksek maliyetli yazılımları (*social network analysis gibi*) da içermiştir. (Buchanan, 2010:59-60)

4.2.8. Ponzi Hilelerinin Saptanması ve Önlenmesi

Finansal hizmetler endüstrisi doğası gereği yüksek riskli bir ortama sahiptir, çünkü hile yapmak için büyük fırsatlar bulunmaktadır. Dolayısıyla, söz konusu özel ortama uygun olarak tasarlanmış sağlam bir hile saptama sisteminin hileli eylemi işaret eden risk faktörlerini ya da anomalileri özellikle içermesi gerekmektedir. (Drew ve Drew, 2010:55-6, 66-8) Bu faktörler anomalilerin (*normlardan sapmaların*) saptanması amacıyla kullanılmaktadır. Bu tür anomaliler davranışsal (*olağandışı davranış biçimleri*), istatistiksel (*göze çarpan istatistiksel ölçümler, aykırılıklar ve tutarsızlıklar*) ve kurumsal (*genel kabul gören en iyi uygulamalar ve geleneksel standartlardan önemli derecede farklılaşan kurumsal özellikler*) olabilmektedir. Anomalilerin her üç türünün de eşzamanlı kullanılması (*çok boyutlu yaklaşım*), yapılan faaliyetin (*üretim, satış, yatırım gibi*) amaca uygunluğunu ve gerçekliğini anlamak isteyen yatırımcılar, analistler (*due diligence experts*), düzenleyiciler ve politika oluşturucular (*devlet*) için gerekli bir karar bileşeni niteliği kazanmıştır. Bu kapsamda, olağanüstü yüksek ve inanılması güç (*too good to be true*) getiriler, değişkenliği çok az getiriler ve emsalleriyle karşılaştırılması zor getiriler ve bunlara karşılık görünen hiçbir riskin olmaması (*yüksek getirinin yüksek riskli olmaması*) potansiyel bir risk faktörüdür. Ölçüt seçimi (*benchmark selection*) ya da performansın makul bir göstergesinin (*reasonable proxy against which to evaluate performance*) bulunması tartışmalı bir konu olmakla birlikte, bu konuda benzerlere dayalı (*peer-based*) ve daha geleneksel referans oranlar performans özelliklerinin değerlendirilmesinde bir bakış açısı kazandırabilmektedir. Hileyi anomalilerden yola çıkarak ortaya çıkarmak isteyenlerin hem finansal analiz, hem de hile incelemesi alanında yeterliliğe sahip olması beklenmektedir. Bunlardan bir sonuç elde ediliyor ise, derinliğine araştırma yapılması ve sonrasında eyleme geçilmesi zorunludur. Düzenleyici kuruluşların uzmanlaşmış, karmaşık finansal işlemleri analiz edebilecek bilgiye ve beceriye sahip deneyim ve becerilere sahip finans ve muhasebecileri işe almak, finans şirketlerini risk odaklı olarak incelemek, çalışanları hile incelemesi ve finansal analiz konusunda özel olarak eğitmek, ilgili alanlarda daha çok çalışan istihdam etmek ve risk faktörlerini derinliğine incelemek amacıyla ek kaynak ve ödenek bulmak konusundaki planlarının yaşama geçirilmesi de hile ile mücadelenin önemli bir parçası olmak durumundadır.

4.2.9. Kanallar Arası (Çapraz) Hilelerin Saptanması ve Önlenmesi

Bu tür hileler iki uçlu bir yaklaşım gerektirmektedir. (Ginovsky, 2013:18-21) İlk olarak, müşterilere ve banka çalışanlarına hile riskleri ve tehditlerine ilişkin daha çok eğitim verilerek farkındalık yaratılması ve ikinci olarak doğrulama sürecini iyileştirmek ya da aynı anlama gelmek üzere sanal hırsızları ortaya çıkarmak için daha ileri teknolojik araçların kullanılmasıdır. Bu çerçevede, bankalar müşterileri banka güvenlik çözümlerinin bir parçası olduklarına ve dolayısıyla ortamı güvenli tutmak için yerine getirmeleri gereken sorumluluklar olduğuna, işlemlerin yapıldığı aygıtların güvenliğini sağlamaya ve en azından bir antivirüs programı almaya ve güncellemeye inandırmak durumundadır. Yazılı açıklamalar ya da duyuru yapmak yerine başvurulabilecek etkili bir yaklaşım, müşteriler için güvenlik eğitimleri düzenlemek, en iyi müşterileri bir araya getirerek uygun bazı araçlarla donatmaktır. Bankalar çalışanlarını ve özellikle müşterilerini kişisel bilgilerini güvenli biçimde saklamak konusunda eğitmek zorundadır, çünkü bunlar genellikle olağandışı bir müşterinin bağlantı kurmak isteyebileceği ilk hedefler konumunda bulunmaktadır. Müşterilerin eğitimi önemli bir faktör ise, hırsızlara daha etkili teknolojik

engeller koymak diğer önemli bir faktördür. Bu alanda yeni bir yaklaşım, müşterilerin bankaya giriş kanallarının her birinde nokta savunması (*point defence*) yapmak yerine, erişim sağlanmış olsa bile verilerin korunmasına odaklanmak olmaktadır. Kanallararası hilelerde çok katmanlı bir yaklaşım sıklıkla önerilmektedir. İşlemlerin tüm kanallarda ve birden çok noktada izlenmesine dayalı hile karşıtı çözümlerde risk tabanlı algoritmalar hileli işlemlerin ortaya çıkarılması yöntemlerine dahil edilmektedir. Annenin kızlık soyadı gibi ortak paylaşılan sırlar yerine, bilgi temelli doğrulama ön plana çıkmaktadır. Bu tür bir doğrulama, banka-müşteri ilişkileri ve işlemlerinden çıkarılabilecek ve ancak müşterinin bilebileceği çok ayrıntılı bilgilere dayanmaktadır. Benimsenebilecek başka bir yaklaşım, müşteri aygıtlarının belirlenmesinde ve belirli işlemlerde birden çok doğrulamaya dayanmaktadır. Her bir aygıtın (*bilgisayarın*) tanımlama bilgisinin (*cookie*) incelenmesine ek olarak, banka bilgisayarları işlemin başlatıldığı coğrafî konumu da incelemektedir. Eskiden sadece bilgisayarların belirlenmesi yeterli iken, günümüzde bilinmeyen wi-fi noktaları bankalarca belirlenip müşteriye kullanıcıyı doğrulaması için yeni sorgulamalar gönderilebilmektedir. Bant dışı doğrulama (*out-of-band authentication*) da giderek yaygınlaşmaktadır; burada banka herhangi bir kanaldan, örneğin elektronik olarak işlem ya da bir değişiklik yapma talebi almakta, başka bir kanaldan (*kısa mesaj ya da telefon ile geri arama*) müşteri ile bağlantı kurarak işlemin yasal bir işlem olup olmadığını kontrol edebilmekte ve müşterinin gerçekten kendisinin olup olmadığını anlayabilmektedir.

4.2.10. Yağmalama ve Risk Ötelemenin Saptanması ve Önlenmesi

Yağmalamanın önlenmesinde yasaları uygulamak ve onları çiğneyenler için bu eylemleri daha maliyetli hale getirmek gerekmektedir. Yağmalama yeteneği banka düzenlemelerinin amaçlanan sonuçlarına ulaşmasını zorlaştırdığı için bu düzenlemelerinin etkileri belirsiz ise de, yağmalamaya karşı cezalar genel çözüm yolu olarak görünmektedir. Yalnızca dış hissedarların olduğu koşullarda da, sermaye zorunlulukları ve yağmaya karşı ceza politikaları hem risk öteleme, hem de yağmalamaya karşı etkili olmaktadır. Bununla birlikte risk almanın daha maliyetli hale getirilmesinin de istenmeyen yan etkileri olabileceği göz önünde bulundurulmalıdır. Düzenleyicilerin riskli faaliyetlere koydukları sınırlamalar riski amaçlandığı gibi bastırsa da, yağmalamayı teşvik edebilmekte ve riske maruz kalmanın giderek artması gibi amaçlanmayan bir sonucu da yanında getirebilmektedir. Başka bir anlatımla, bir bankaya istenmeyen bir faaliyet yasaklandığında, banka daha riskli olabilen ve büyük olasılıkla daha karmaşık ve anlaşılması güç başka bir faaliyeti keşfetmekte güçlük çekmemektedir. (Boyd ve Hakenes, 2014:57-8)

4.2.11. Elektronik Bankacılık Hilelerinin Saptanması ve Önlenmesi

Elektronik bankacılık hizmetlerinde hileler zayıf kimlik doğrulama sistemlerinden yetersiz iç kontrollere kadar uzanan çeşitli güvenlik açıklarından doğmaktadır. Yetersiz güvenlik potansiyel olarak finansal zararlara, düzenleyicilerin cezalandırıcı önlemlerine ve basın-yayın organlarında itibar kaybına yol açmaktadır. (Usman ve Shah, 2013:1-9) Bu kapsamda, yeterli eğitim verilmemesi, yönetim karar alma süreçlerinde iletişim ve bilgiye zamanlı erişim sorunu, yönetici ve denetçilerin zayıf önderlik biçimleri hilelerin nedeni olabilmektedir. Elektronik bankacılıktaki hile önleme sistemlerini güçlendirmek, dolayısıyla güvenliği arttırmak ve paydaşların bu sistemlere güvenini kaybetmemek amacıyla teknoloji, iç kontroller, müşteri ve personel eğitimi gibi bir dizi başarı faktörü bulunmaktadır. Elektronik bankacılığa geçişte güvenlik, kullanıcı dostu kuyruk (*sıra*) yönetimi, erişilebilirlik, zaman ve fon transferleri gibi faktörler temeldir ve güvenlik bunların arasında en önemlisi olarak kabul edilmektedir. Biyometrik teknolojiler, tanımlamada her bir bireye özgü özellikleri kullandığı için bu tür hileleri asgari düzeye indirmek için ileri bir adım oluşturmaktadır. Parmak izi teknolojisi (*finger print technology*) yanında tuş vuruşları (*keystroke dynamics, kullanıcıların klavye girişlerini izleyerek yazı ritmi ve alışkanlıklarının analiz edilmesi*) güvenliği arttıran davranışsal biyometrik teknolojilerdir. Bununla birlikte, biyometrik doğrulamada yanlışlıkla red ve kabul uygulamaları da böyle bir teknolojinin kullanılmasının maliyetinde dikkate alınmalıdır. Ayrıca e-bankacılığın başarısı için üst yönetim desteği de çok önemli bulunmaktadır, çünkü veri şifreleme, güvenlik sistemlerinin genişletilmesi, hile önleme yazılımları, tek seferlik parolalar, çok düzeyli parolalar, akıllı kart doğrulaması gibi uygulamalar çalışma biçiminde değişiklikler gerektirmekte, bu ise üst yönetim desteği olmaksızın yapılamamaktadır. Banka müşterile-

rinin hileye açık olması da önemli bir etmendir; eğitim ve demografik özellikler bu açıklığın derecesini etkilemektedir. Dolayısıyla, yeterli eğitimi vererek müşterilerin hileye açıklık derecesini azaltmak gerekmektedir. Bu bağlamda özellikle ödeme yapılan kartlarla ilgili olarak müşterilerin kişisel bilgilerini korumak üzere eğitilmesi vurgulanmaktadır, çünkü özel bilgilerin şifreleme yoluyla korunması ve gizli tutulması (*privacy*) hile riskini etkilemektedir. İşlemlerin doğrudan banka sitemlerine bağlı olmadığı durumlarda, şifrelemeye dayalı ek bir güvenlik önlemi olarak müşteriler ve bankalar arasında aracılık yapacak kuruluşlar gizlilik ve doğrulama etkileşimlerinde yardımcı olabilmektedir. Öte yandan, hilelerin çoğunluğunun elektronik bankacılık sistemleri aracılığıyla yapılması iç kontrol sistemlerindeki zayıflıkları yansıttığı için sıkı iç kontroller hileye yönelik olarak öncelikli ve etkili bir savunma önlemi sayılmaktadır. İç kontrollerin var olması yeterli değildir, sıkı sıkıya uygulanması ve iç denetim işlevi tarafından fiili uygulamanın izlenmesi de gerekmektedir. İç denetim, genel olarak kurallara uyumun güvence altına alınmasında bir zorunluluktur. Nitekim iç denetim birimi olan (*in-house internal audit function*) kurumların olmayanlara ve iç denetim hizmetini dışarıdan alan kurumlara (*outsourcing the internal audit function*) göre hileleri ortaya çıkarma ve raporlama olasılığı daha yüksek gerçekleşmektedir, ancak iç denetim birimi dışarıdan sağlanan iç denetim hizmetine göre daha pahalı olmakta, iç denetçiler yönetim ile ilgili hileleri misilleme (*retaliation*) korkusuyla raporlamayabilmekte ve dolayısıyla daha az bağımsız görünmektedir. Başka bir önemli başarı faktörü, hileye açık olunan noktalar bağlamında yaşanan tarihten ders alınması (*kurumsal öğrenme*) ve tarihsel verilerin kullanılmasıdır. Bu uygulamalar sonucunda İngiltere'de plastik kartlarla (*kredi ve banka kartları*) yapılan hilelerin maliyeti 2010'da önceki yıla göre %10 azalırken elektronik bankacılık hile maliyetleri %24 azalmıştır. Bu sonuç, elektronik bankacılık güvenliğinde hem teknolojik (*hileyi ortaya çıkaran yazılımlar gibi*), hem de teknolojik olmayan (*artan müşteri bilinci gibi*) yöntemler ile sağlanan gelişmelerden kaynaklanmıştır.

4.2.12. Diğer Çeşitli Hilelerin Saptanması ve Önlenmesi

Para ve para benzerlerine ilişkin hilelerin ortaya çıkarılması ve önlenmesi için en etkili yöntem, ilgili personelin gözetim altında tutulmasıdır. Gözetim, hem üst makamlar tarafından izlenmeyi, hem de görevlerin birbirinden ayrılmasını kapsamaktadır. Nakit ile ilgili belgelerin ve iptal edilen çeklerin özenle incelenmesi, müşteri ve tedarikçiler ile sistematik olarak iletişim kurularak bilgilerin doğrulanması, habersiz gerçekleştirilen denetimler, personel ve tedarikçi rotasyonu ile fiziksel güvenlik önlemlerinin etkinleştirilmesi etkili önlem ve araçlar arasında sayılmaktadır. (Coenen, 2008:79-83) Genel olarak, işletmelerde meydana gelen bütün varlıkların kötüye kullanılması hilesi olaylarının iç denetçiler tarafından kayda geçirilmesi, incelenmesi ve raporlaştırılması önemli bir noktadır, çünkü varlıkların kötüye kullanılması hileleri söz konusu olduğunda iç denetçiler daha uygun bir konumda bulunmaktadır. (Kandemir ve Kandemir, 2012a:73) Bu bağlamda iç denetim çalışmalarının yararlı bir temel oluşturabilmesi için iç denetim biriminin uzmanlaşması, doğrudan doğruya denetim kuruluna bağlanması, idari özerkliğinin güvence altına alınması, iç kontrol sistemlerinin kurulmasında ve geliştirilmesinde birinci derecede yetkili olması ve iç denetim mesleğinin bir meslek örgütü ve yasasına bağlı olarak yayımlanan standartlar aracılığıyla yönetilmesi gerekmektedir. İç denetimin yapısal kısıtlarının olanaklar ölçüsünde giderilmesi durumunda özellikle varlıkların kötüye kullanılması hilelerinin ortaya çıkarılması ve önlenmesinde daha güvenilir bir düzeye gelebileceği belirlenmiştir. (Kandemir ve Kandemir, 2013, s.41-2 ve 50-1)

5. Sonuç ve Genel Bir Değerlendirme

Hileleri insanlar yapmaktadır, ancak uygun hile ortamını ve koşullarını da büyük ölçüde kurumsal ve sistemik etkenler hazırlamaktadır. Böyle bir açıdan bakıldığında, hile bireysel ya da sektörel bir sorun değil, kurumsal ve sistemik bir sorun olarak anlaşılmalı, küçük ya da büyük ölçekli olmasına bakılmaksızın önemli ve dolayısıyla her koşulda denetlenmesi gereken bir sorun olarak kabul edilmelidir, çünkü hile yapılmakta ise sistemi kuralsızlığa ve düzensizliğe iten güdü ve koşulların geçerli ve etkili olduğu varsayılabilmektedir. Hile en geniş anlamda düzensizlik (*irregularity*) olarak tanımlanınca, ki zorunlu denetimin kurumsal ve yasal bir uygulama durumuna geldiği koşullarda hile bu şekilde tanımlanmaktadır, öncelikle kurallara uymamayı içermektedir. Konunun bir yönü küreselleşme ideolojisi ile girilen aşırı serbestleş-

tirme ve daha doğru bir anlatımla kuralsızlaştırma ise, diğer yönü mevcut kurum ve kurallar düzeninin boşluklarının kötüye kullanılması olmaktadır. (Kandemir ve Kandemir, 2012b:102-3) Dolayısıyla, hile ile mücadelede başlangıç noktası tüm kurum, ekonomi ve toplumların kurallı kurum, ekonomi ve toplum olması olmak gerekmektedir. Bu aşamada kurallara uymanın ve daha demokratik, insani, rasyonel kurallar yapmanın aynı sürecin bileşenleri olduğu akılda tutulmalıdır. Ayrıca kontrol ve denetimlere sistem karşıtı ya da yıkıcı bileşenler olarak yaklaşmayan bir kurumsal ve toplumsal kültüre sahip olmak da aynı sürecin bir parçası olarak düşünülmek durumundadır.

Böyle bir ortamda yapılmakta olan bankacılık hilelerine karşı en etkili iki silâh, nitelikli insan ve yüksek teknoloji olmaktadır. Yüksek teknolojinin yüksek insan bilinci ve bilgisinin maddeleşmiş hali olduğu kabul edildiğinde, zorluk düzeyi yüksek bu savaşın ancak ve ancak nitelikli insan ile kazanılabileceği anlaşılmaktadır. Hileleri kural dışı, etik dışı ve hukuk dışı ve haksız olarak algılayacak bir insan bilincinin yaratılması yaşamsal önemdedir. Hileli malı, faaliyeti, ticaret ve sistemi ayıplı mal, faaliyet, ticareti ve sistem olarak değerlendirip tüm ayıpları yok etmek ve sonuçta ayıpsız yaşamak isteyen bir insan bilincinden söz edilmektedir. Böyle bir bilincin yaratılmasında her türlü eğitimin (*genel, yüksek ya da hizmet içi*) yadsınamayacak bir rolü olduğu kuşkusuzdur, ancak daha da önemlisi insanlığın en önemli etkinliği olan üretimin ve bölüşümün (*kazanmanın*) kurallı, etik, hukuki ve adil olmasını sağlayacak bir ekonomik ve mali sistem kurmak belirleyici öneme sahip bulunmaktadır. Bu bağlamda, ilk olarak ekonomik karar alma sürecinin sosyal amaçlar ve insani değerlerle uyumlu ve bütünleşik olması için bu sürece sosyal ve ekonomik değerlerin de katılması, ekonomik ölçütlerle sosyal değerlerin bütünleştirilmesi gerekmektedir. Amaç, ekonomik etkinliklerde sosyal ve çevresel dengelerin gözetilerek insan mutluluğunun (*dışsal faydaların*) maksimizasyonu ve dünyaya, doğaya ve topluma verilen zararın (*dışsal maliyetlerin*) minimizasyonu olmalıdır. (Kandemir, 2014:67-8) Sosyal ve ekonomik sistemin bir bütün olarak yukarıda tanımlanan yönde değişmeye zorlanması durumunda insanın da bu değişim sürecine ayak uydurması başka bir anlatımla ekonomik altyapının ilke ve kurallarını değiştirince sosyal üstyapının tüm birey ve kurumlarının da değişmesi beklenmektedir. Nitelikli insan ve yüksek teknolojiye yapılan yatırımların sağlayacağı faydalar, iflaslar ve itibar kaybına kadar giden dayanılması güç hile maliyetleri de göz önünde bulundurulduğunda her durumda maliyetlerini aşacağı ve kısa süre içinde kendisini amorti edeceği düşünüldüğünden, hile ile mücadelede insana ve teknolojiye yatırım yapmak ekonomik ve sosyal bir zorunluluk ve giderek bir önkoşul durumuna gelmektedir.

Çoğunluğu yolsuzluk olaylarından oluşan ve banka varlıklarının kötüye kullanılmasını hedefleyen bankacılık hilelerinin önlenmesi ve ortaya çıkarılmasında iç kontrol sistemlerinin varlığı birinci derecede önemli bir güvenlik duvarı oluşturmaktadır. Kontrol sistemlerinin kurulması ve etkinliğinin sağlanması hileler ile mücadelede bir önkoşul olmakla birlikte hilelerin karmaşıklığı, örgütlü olarak gerçekleştirilmesi ve kontrol sistemlerini atlatmak üzere tasarlanabileceği olgusu karşısında mücadelenin elde mevcut bütün araç ve yöntemler kullanılarak yapılması gerekmektedir. Bu kapsamda, etkinliği sınanmış anonim ihbar hatları başta olmak üzere göreli olarak özerk bir iç denetim, bağımsız bir dış denetim, hile incelemesi, adli muhasebe gibi araçların birlikte ve eşgüdüm kullanılması uygun değerlendirilmektedir. Yasalara uyum, işletme çalışan ve yöneticilerinin dürüstlüğü, toplum ve doğaya saygı, finansal bilgilerin yasal gereklilikleri karşılayacak düzeyde değil, kamunun uygun ve yerinde kararlar almalarına yetecek kapsamda açıklanması ve kar maksimizasyonu değil, katma değer optimizasyonunun işletme politika ve kurumsal kültürlerinin bir parçası durumuna getirilmesi de büyük önem taşımaktadır. İşletmelerin sözü edilen mikro düzeydeki değişim sürecinin başarılı olabilmesi ise ancak ve ancak sektörel, endüstriyel ve ulusal düzeyde paralel çalışmaların yapılmasına bağlı olduğu için siyaset ve ekonomi dünyasının demokratik kitle örgütleri ile uyum içinde ortak amaçlara yönelik olarak hareket etmesi gereksinimi ortaya çıkmaktadır. Hilelerin ve genel olarak yolsuzluğun azaltılması yönündeki toplumsal taleplerin karşılanması, ekonomi ve siyasette bireyci kültürden daha demokratik, etik ve sosyal bir kültüre doğru dönüşüm geçirmeyi zorunlu kılmaktadır. Bu değişim süreci ancak kamunun, ekonominin, siyasetin ve bürokrasinin aynı yönde değişmek istemesi durumunda başarı ile yönetilebilecektir. (Kandemir ve Kandemir, 2012c:39-40) Oligopolcü piyasaların ve bu arada bankacılık piyasalarının bu süreç doğrultusunda düzenlenmesi daha saydam ve hesap verebilir

banka ve şirketler ortaya çıkaracak, bu ise hilelerin ve neden olduğu sosyal ve ekonomik maliyetlerin azaltılmasına katkı sağlayabilecektir.

Kaynakça

ACFE (2014); Association of Certified Fraud Examiners); Report to the Nation on Occupational Fraud and Abuse: Global Fraud Survey, Austin, USA.

AJAH, Ifejinwa,INYIAMA, Chibueze; (2011), "Loan Fraud Detection and IT-Based Combat Strategies", Journal of Internet Banking and Commerce, August, Vol.16, No.2, pp.1-13.

ASH, Duncan; (2011),"The UK fraud landscape for financial services", Computer Fraud & Security", April, pp.16-7.

BALOGUN, Shyngle K., SELEMOGWE, Morekwe, AKANFALA, Femi; (2013), "Fraud and Extravagant Life Styles among Bank Employees: Case of Convicted Bank Workers in Nigeria", Psychological Thought, Vol. 6(2), pp.252-63.

BENSTON, George J.; (2004), "What's Special about Banks ?", The Financial Review, 39, pp.13-33.

BIEGALMAN, Martin T., BARTOV, Joel T; (2006), Executive Roadmap to Fraud Prevention and Internal Control: Creating a Culture of Compliance, John Wiley & Sons, Hoboken, New Jersey, USA.

BOUMEDIENE, Salem Lotfi; (2014), "Detection and Prediction of Managerial Fraud in the Financial Statements of Tunisian Banks", Global Conference on Business and Finance Proceedings, Volume 9, Number 1, pp.421-426.

BOYD, John H., HAKENES, Hendrik; (2014), "Looting and risk shifting in banking crises", Journal of Economic Theory 149, pp.43-64.

BRUNSWICK, Steve; (2009), "e-Commerce fraud-time to act ?", Card Technology Today, January, pp.12-13.

BUCHANAN, Ronald; (2010), "Banking Security: Banks on Guard", Latin Trade, 09-10, pp.58-60.

CFS (Computer Fraud & Security); (2012), "Banking fraud down in 2011", Computer Fraud & Security, April, p.3.

CFS (Computer Fraud & Security); (2014), "Online attacks push up fraud rates in England and Wales", Computer Fraud & Security, May, p.3.

CHANDLER, Brent; (2014) "Fraud, Scams and Paper Bank Statements-Why Go There ?", Mortgage Banking, September, pp.82-87.

CHEHASHIM, Rosmawani, MAHDZAN, Nurul Shahnaz; (2014), "Fraud in letter of credit transactions: The experience of Malaysian Bankers", International Journal of Law, Crime and Justice 42, pp.224-236.

COENEN, Tracy; (2008), Essentials of Corporate Fraud, John Wiley & Sons, New York, USA.

COMPIN, Frederic; (2008), "The role of accounting in money laundering and money dirtying", Critical Perspectives on Accounting, 19, pp.591-9.

CTT (Card Technology Today); (2006), "A Smart Answer to online fraud ? Smart Technology Solutions", Card Technology Today, May, pp.10-11.

DREW, Jacqueline M., DREW Michael E.; (2010), "The Identification of Ponzi Schemes: Can a Picture Tells a Thousand Frauds ?", Griffith Law Review Vol 19, No 1, pp.51-70.

EXCELL, David; (2012), "Bayesian Inference-the future of online fraud protection", Computer Fraud & Security, February, pp.8-11.

GHOSH, Mahuya; (2010), "Mobile ID fraud: the downside of mobile growth", Computer Fraud & Security, December, pp.8-13.

GINOVSKY, John; (2013), "More channels, more fraud risk", ABA Banking Journal, December, pp.18-21.

GOLD, Steve; (2014), "The evolution of payment card fraud", Computer Fraud & Security, March, pp.12-17.

GOLDEN, Thomas W., SKALAK, Steven L., CLAYTON, Mona M; (2006), A Guide to Forensic Accounting Investigation, John Wiley & Sons, New York, USA.

GREEN, Brian P., REINSTEIN, Alan; (2004), "Banking Industry Financial Statement Fraud and the Effects of Regulation Enforcement and Increased Public Scrutiny", Research in Accounting Regulation, Volume 17, pp.87-106.

GUARDIAN ANALYTICS; (2013), "Best Practices for Detecting Banking Fraud", Illinois Banker, Resource Guide, pp.6-7.

HARTMAN-WENDELS, Thomas, MAHLMANN, Thomas, VERSEN, Tobias; (2009), "Determinants of bank's risk exposure to new account fraud-evidence from Germany", Journal of Banking & Finance 33, pp.347-357.

HIGGINS, Huang Ngo; (2012), "Learning Internal Controls from a Fraud Case at Bank of China", Issues in Accounting Education, American Accounting Association, Vol.27, No.4, pp.1171-1192.

IDOLOR, Eseoghene Joseph; (2010), "Bank Frauds in Nigeria: Underlying Causes, Effects and Possible Remedies", African Journal of Accounting, Economics, Finance and Banking Research, Vol.6, No.6, pp.62-80.

KANDEMİR, Canol; (2016), "Muhasebenin Yolsuzluk Amaçlı Kötüye Kullanımı: 2000 Sonrası Banka İflâslarında Türkiye Deneyimi", Marmara Üniversitesi Öneri Dergisi ,Cilt 12, Sayı 45, Ocak, ss.235-286.

KANDEMİR, Canol; (2014), "Muhasebenin Ekonomi Politiği: Dış Dinamikler", Gazi Üniversitesi Sosyal Bilimler Dergisi, Cilt 1, Sayı 1,2014, ss.38-74.

KANDEMİR, Canol; (2013), "Türkiye'de Bağımsız Denetçilerin Hile Risk Faktörleri Etki Değerlemesi", Muhasebe ve Denetime Bakış, Haziran, ss.83-108.

KANDEMİR, Canol, KANDEMİR, Şenol; (2012a), "Muhasebe Hilelerinin Önlenmesive Ortaya Çıkarılmasında Kullanılan Geleneksel Araç ve Yöntemler", Malî Çözüm, Eylül-Ekim, ss.39-77.

KANDEMİR, Canol, KANDEMİR, Şenol; (2012b), "Enron Olayı'nı Doğru Okumak-II: Kıssadan Hisseler", Muhasebe ve Denetime Bakış, Kasım, ss.85-106.

KANDEMİR, Canol, KANDEMİR, Şenol, (2012c), "Muhasebe Hilelerini Önlemede Çözüm Yolu Olarak Kullanılacak Stratejilerin Bileşenleri", Malî Çözüm, Mayıs-Haziran, ss.15-41.

KANDEMİR, Canol, KANDEMİR, Şenol; (2013), "Muhasebe Hata ve Hilelerinin Ortaya Çıkarılmasında Bağımsız Denetçilerin Sorumluluğunu Etkileyen Faktörlere İlişkin Algılamaları", Muhasebe ve Bilim Dünyası, MÖDAV 2013/1, ss.29-54.

KANNA, Ashu, ARORA, Bindu; (2009), "A Study to investigate the reasons of bank frauds and the implementation on preventive security controls in the Indian banking industry", International Journal of Business Science and Applied Management, Volume 4, Issue 3, pp.1-11.

KLOMP, Jeroen, DE HAAN, Jakob; (2012), "Banking risk and regulation: Does one size fit all ?", Journal of Banking & Finance, 36, pp.3197-3212.

KOVACICH, Gerald; (2009), "Introduction to Computer Fraud-Part 2", Computer Fraud & Security, August, pp.10-14.

KRIVKO, M. (2010), "A hybrid model for plastic card fraud detection systems", Expert Systems with Applications, 37, pp.6070-6076.

MAZUR, Michael; (2014), "Fraud grows, but new tools help check it", ABA Banking Journal, January, p.11.

NABHAN, Reem Abdul Latif, HINDI, Nitham M.; (2009), "Bank Fraud: Perceptions of Bankers in the State of Qatar", Academy of Banking Studies Journal, Volume 8, Number 1, pp.15-38.

POZZOLA, Andrea Dal, CAELEN, Oliver, BORGNE, Yann-Ael, WATERSCHOOT, Serge, BONTEMPI, Gianluca; (2014), "Learned lessons in credit card fraud detection from a practitioner perspective", Expert Systems with Applications 41, pp.4915-4928.

QUAH, Jon T.S., SRIGANESH, M.; (2008), "Real time credit card fraud detection using computational intelligence", Expert Systems with Applications, 35, pp.1721-1732.

RAHMAN, Rashidah Abdul, ANWAR, Irda Syahira Khair; (2014), "Effectiveness of fraud prevention and detection techniques in Malaysian Islamic Banks", Procedia-Social and Behavioral Sciences, 145, pp.97-102.

RAMOS, Michael; (2008), Wiley Practioner's Guide to GAAS, John Wiley & Sons, Hoboken, New Jersey, USA.

RUDESILL, Gary G., RUDESILL, Charryll; (2001), "An Investigation into fraud prevention and detection of small businesses in the United States: Responsibilities of auditors, managers, and business owners", Accounting Forum, Vol 25, No 1.

SARRA, Silvia; (2011), "Innovative solutions to leverage resources and maximize efficiency in the battle against cheque fraud", Journal of Payments Strategy & Systems, Volume 5, Number 3, pp.289-297.

SCANIA, Salvatore, LUDWIG, Robert W.; (2013), "Surging, Swift and Liable ? Cybercrime and Electronic Payments Fraud Involving Commercial Bank Account : Who Bears the Loss ?", Journal of Internet Law, April, pp.3-13.

SINGLETON, Tommie W., SINGLETON, Aaron, BOLOGNA, G.Jack,LINDQUIST, Robert J.; (2006), Fraud Auditing and Forensic Accounting, John Wiley & Sons, New York, USA.

SOUVIGNET, Thomas, HATIN, Julien, MAQUS, Fabrice, TESNIERE, Damien, LEGER, Pierre, HORMIERE, Romain; (2014), "Payment card forensic analysis: From concepts to desktop and mobile analysis tools", Digital Investigation, 11,pp.143-153.

SULLIVAN, Carol, WEBB, Kimberly; (2011), "The Kosse Bank Catastrophe: Anatomy of a Big Fraud in a Small Town", Journal of Accounting and Finance, Vol.11 (3), pp.62-64.

USMAN, Ahmad Kabir, SHAH, Mahmood Hussain; (2013), "Critical Success Factors for Preventing e-Banking Fraud", Journal of Internet Banking and Commerce, August, Vol.18, No.2, pp.1-15.

WEHINGER, Gert; (2013), "Banking in a challenging environment: Business models, ethics and approaches toward risks", OECD Journal: Financial Market Trends, Volume 2012/2, pp.79-88.

WELLS, Joseph T.; (1990), "Six Common Myths about Fraud", Journal of Accountancy, February, pp.82-88.

WELLS, Joseph T.;(2008), Principles of Fraud Examination, John Wiley & Sons, New York, USA.

YUNSEN CHEN, Zu, SONG WANG, Yutao; (2011), "Corporate Fraud and Bank Loans: Evidence from China", China Journal of Accounting Research, 4, pp.155-165.