



# Türkiye Bankacılık Sektörü Dolandırıcılıkla Mücadele Araştırması

**Daha Güçlü Savunma için 5 Temel Öneri**



# İçindekiler

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Önsöz                                                                           | 03 |
| <b>01</b> Sektör Ötesi İttifak:<br>Dolandırıcılıkla Mücadelede Yeni Paradigma   | 05 |
| <b>02</b> Ortak İlkelerle Güçlenen Mücadele:<br>Kapsamlı Standartlar Oluşturmak | 09 |
| <b>03</b> Banka İçi Yönetişim Dönüşümü:<br>Stratejik Risk Mimarisini Kurmak     | 12 |
| <b>04</b> Algoritmaların Ötesinde:<br>Teknolojiyi Stratejik Ortağa Dönüştürmek  | 15 |
| <b>05</b> Bilinçli Müşteri:<br>Mücadelenin Stratejik Ortağı                     | 18 |
| Sonuç                                                                           | 21 |

# Önsöz



**Dr. Gökhan Yılmaz**  
Şirket Ortağı,  
PwC Türkiye

Dijitalleşmenin hızla ilerlediği, tehditlerin sınır tanımadığı bir çağdayız. Bankacılık sektörü, inovasyonun sunduğu fırsatlarla büyürken, giderek sofistike hale gelen dolandırıcılık ve sosyal mühendislik saldırılarıyla da yoğun bir mücadele veriyor. Bu ortamda yalnızca kurumların değil, tüm ekosistemin birlikte hareket etmesi artık bir zorunluluk.

Bu çalışma, Türkiye bankacılık sektöründe dolandırıcılıkla mücadeleyi mevcut tablo ve geleceğe yönelik yol haritasıyla ele alıyor. Araştırmamız; bankacılık yöneticilerinin deneyimleri, güncel veriler ve uluslararası iyi uygulamalar ışığında, yalnızca sorunları değil, çözüm yollarını da ortaya koyuyor.

Amacımız; kurumlar arası iş birliği, kurumsal kapasite ve teknolojik yatırımların nasıl daha etkin kullanılabileceğine dair stratejik öneriler sunmak. Ortak bir savunma hattı kurmak, bilgi paylaşımını artırmak ve ulusal ölçekte entegre çözümler geliştirmek bu mücadelenin en kritik unsurlarıdır.

Katkı sağlayan tüm sektör temsilcilerine teşekkür eder, bu çalışmanın Türkiye bankacılık sektörünün daha güvenli, dirençli ve geleceğe hazır bir yapı kurmasına ilham olmasını dilerim.

Saygılarımla,



**Bankacılık sektörü, her geçen gün artan dolandırıcılık vakalarıyla ciddi bir sınavdan geçiyor. Sadece finansal kayıplar değil, aynı zamanda müşteri güveninin sarsılması ve bankaların itibarının zedelenmesi de bu sürecin en önemli sonuçları arasında.**

Elinizdeki bu çalışma, Türkiye’de bankacılık alanında dolandırıcılıkla mücadeleye öncülük eden yöneticilerle yaptığımız detaylı ve tamamen anonim görüşmelere dayanıyor. PwC’nin hem sektördeki tecrübesi hem de uluslararası birikimiyle harmanladığımız bu araştırma, dolandırıcılıkla mücadelede güncel tabloya ve öne çıkan risklere ışık tutmayı amaçlıyor.

Sektörün aktif büyüklüğünün büyük kısmını temsil eden bankaların paylaştığı görüşlerle hazırlanan bu raporda; kurumların karşılaştığı zorluklara, sahadaki uygulamalarda iyileştirme gereken noktalara ve yetkinliklerini geliştirmeleri için atılması gereken adımlara samimi bir bakış sunmaya çalıştık.

# Sektör Ötesi İttifak: Dolandırıcılıkla Mücadelede Yeni Paradigma

Finansal dolandırıcılıkla mücadele artık sadece bankaların kendi başına altından kalkabileceği bir konu olmaktan çıktı; pek çok farklı sektör ve paydaşın dahil olduğu, karmaşık ve çok katmanlı bir alana dönüştü. Türkiye’de de bugün bankalar, finans kuruluşları, teknoloji, telekom ve e-ticaret firmaları, kolluk kuvvetleri, yargı ve düzenleyici kurumlar hep birlikte bu mücadelede yer alıyor.

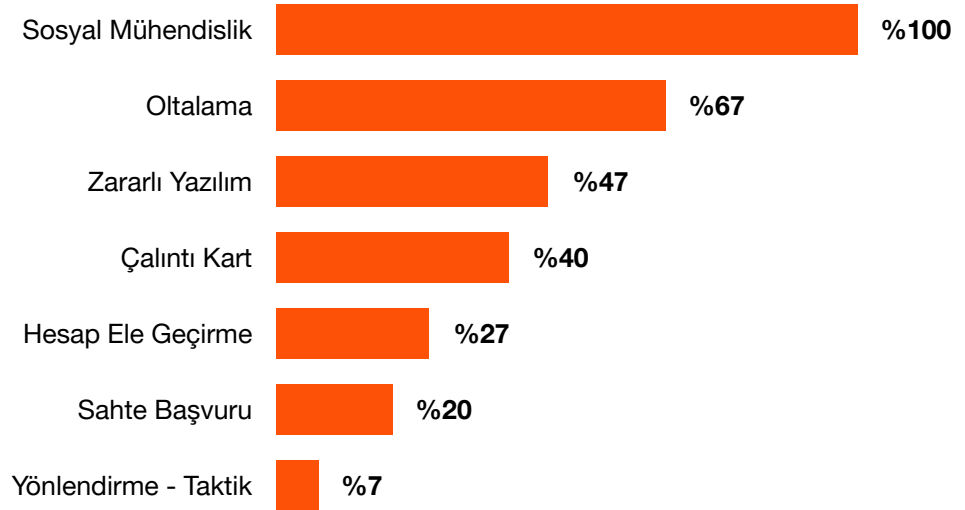
Özellikle son yıllarda, sosyal mühendislik odaklı saldırıların çeşitliliği ve karmaşıklığı iyice arttı. Üstelik bu tehditler sadece bankacılık dünyasıyla sınırlı kalmıyor, hemen her sektöre yayılıyor. Örneğin müşterilere gönderilen sahte SMS’ler ya da sahte çağrı merkezi aramaları yüzünden insanlar banka bilgilerini dolandırıcılara kaptırabiliyor. Bu tip durumlarda, saldırının başlangıcı genellikle bankacılık dışında geliştiği için, bankaların tek başına müdahale edebileceği alan da doğal olarak kısıtlı kalıyor.

Benzer bir durumu e-ticaret ve online ödeme platformlarında da görüyoruz. Kötü niyetli satıcılar veya sahte siteler aracılığıyla ele geçirilen kimlik, hesap ve kart bilgilerinin kullanılması, bugün dolandırıcılık vakalarının en büyük kaynaklarından biri. Tüm bu örnekler gösteriyor ki; finansal dolandırıcılık artık bankacılık sınırlarının çok ötesine geçmiş durumda ve bu sorun tek bir bakış açısıyla çözülecek gibi değil.

Geçtiğimiz yıl boyunca karşılaşılan dolandırıcılık yöntemlerinin başında sosyal mühendislik, ortalama ve zararlı yazılım geliyor. Özellikle sosyal mühendislik, dolandırıcıların insan psikolojisini hedef alıp bilgi çalmak için başvurduğu en sık senaryo olarak öne çıkıyor. Ortalama ve zararlı yazılım saldırılarındaki artış, işin teknik boyutunun da giderek karmaşıktığını gösteriyor. Bunun yanında çalıntı kart ve hesap ele geçirme vakaları da dijital kimliklerin giderek daha fazla tehdit altında olduğunu ortaya koyuyor.

### Şekil 1: En Yaygın Dolandırıcılık Yöntemleri

Son 1 yıl içerisinde en sık karşılaşılan dolandırıcılık yöntemleri nelerdir?



Birden fazla seçim yapılabilmesi nedeniyle toplam %100'ü aşmaktadır.

Dolandırıcılık yöntemleri her geçen gün daha karmaşık ve akıllıca kurgulanıyor. Bu da demek oluyor ki, sadece kurum içi önlemlerle yetinmek artık yeterli değil; işin içine farklı kurumların ve sektörlerin birlikte, uyum içinde hareket etmesi gerekiyor. Uluslararası alanda da bu yönde iyi örnekler var. Örneğin, Birleşik Krallık'ta dolandırıcılık ve siber güvenlikle ilgili kurallar, tüm finans sektörü için ortak bir çatı altında birleştirilmiş durumda. Bu sayede hem bilgi paylaşımı çok daha hızlı ve düzenli ilerliyor, hem de olası tehditlere karşı hızlı müdahale etmek mümkün hale geliyor. Dahası, bu yaklaşım sadece yaşanan olaylara tepki vermekle kalmıyor; daha yaşanmadan risklere karşı hazırlıklı olmayı ve savunmayı da güçlendiriyor.

Türkiye'de de farklı kurumlar arasındaki bilgi akışını ve birlikte hareket etme kültürünü daha ileriye taşımak önemli bir fırsat sunuyor. Bankalar, teknoloji şirketleri, sektör temsilcileri ve diğer paydaşlar bir araya gelip ortak bir iş birliği zemini oluşturduğunda; dolandırıcılıkla mücadelede hem daha sağlam hem de daha proaktif bir yapı kurmak mümkün olabilir.



## Neler Yapılmalı?

### Ulusal koordinasyonun sağlanması

Birleşik Krallık gibi ülkelerde finansal dolandırıcılıkla mücadelede başarıya ulaşan temel unsur; regülatörler, bankalar ve kolluk kuvvetleri arasında kurulan güçlü iş birliği ve hızlı bilgi paylaşımıdır. Bu yapı sayesinde, dolandırıcılık vakalarına anında müdahale edilebiliyor ve tehditler karşısında esneklik sağlanıyor.

Türkiye’de de bankalar dışında finansal teknoloji şirketleri, ödeme kuruluşları, e-ticaret siteleri, telekom şirketleri ve kamu kurumlarının birlikte hareket edebileceği, güvenli bilgi ve veri paylaşımına dayalı bir ulusal koordinasyon modeli kurulmalı. Çünkü dolandırıcılık riskleri artık tek bir sektörü değil, tüm ekosistemi ilgilendiriyor.

### Proaktif ve dayanıklı bir ekosistem oluşturmak

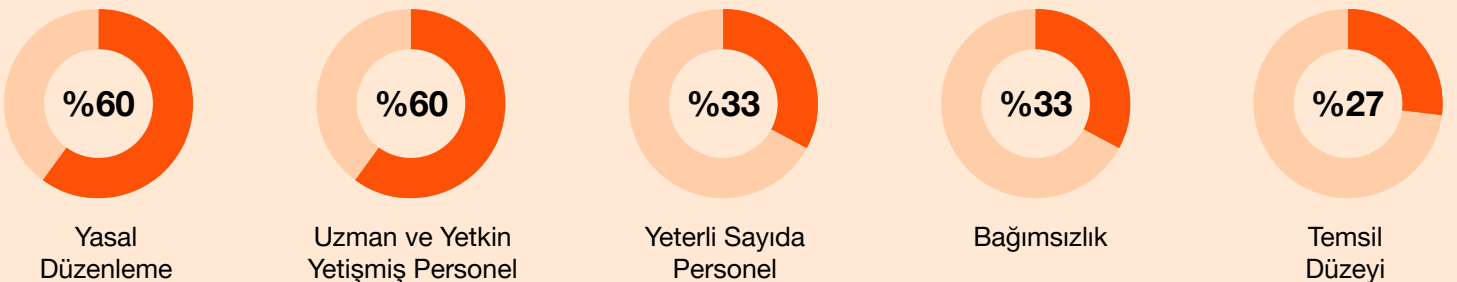
Böyle bir model, yalnızca gerçekleşen vakalara tepki vermek için değil; riskleri önceden tespit edip erken uyarı sistemleriyle müdahale edebilmek için de kritik öneme sahip. Sektörler arası ortak standartlar ve iyi uygulamalarla desteklenen bir ekosistem kurulduğunda, Türkiye’nin finansal sistemi dijital tehditlere karşı çok daha güçlü ve esnek bir hale gelecektir.

## Ortak İlkelerle Güçlenen Mücadele: Kapsamlı Standartlar Oluşturmak

Bankacılıkta dolandırıcılıkla mücadelede başarılı olmanın yolu, güçlü bir kurumsal yapı kurmaktan ve herkesin uyması gereken ortak standartlar belirlemekten geçiyor. Türkiye’de bankalar bu konuda zaten önemli adımlar atıyor ve pek çok düzenleme de mevcut. Yine de işin teknoloji altyapısı, organizasyon ve operasyonların nasıl tasarlandığı, yönetim biçimi ile çalışanların yetkinlikleri gibi alanlarda hâlâ daha fazla standartlaşma ve kurumsallaşma fırsatı var. Kısacası, sektör olarak ortak hareket edebilirsek ve çıtayı biraz daha yükseltebilirsek, dolandırıcılıkla mücadelede çok daha güçlü bir noktaya gelebiliriz.

### Şekil 2: Organizasyonel İhtiyaçlar

Dolandırıcılık ile mücadele bölümlerinin organizasyonel sorunları nelerdir?



Birden fazla seçim yapılabilmesi nedeniyle toplam %100’ü aşmaktadır.

Her bankanın ya da kurumun kendi başına geliştirdiği uygulamalar elbette sektöre zenginlik katıyor. Ama işin sürdürülebilirliği ve savunmanın gücü için belli başlı beklentilerin ve asgari standartların net şekilde ortaya konması şart. Böylece, herkesin uyması gereken ortak bir çerçeveye savunma hattı çok daha sağlam ve dengeli hale gelebilir. Ortak standartlar sadece regülasyonlara uyumu kolaylaştırmakla kalmaz, aynı zamanda bankaların kendi yaptığı işleri de daha düzenli, karşılaştırılabilir ve sürdürülebilir kılar. Sonuçta, bankalar arasında bilgi paylaşımı ve iş birliği de çok daha kolay olur, riskleri önceden tespit etmek ve önlem almak mümkün hale gelir.

Dünyadaki iyi örnekler de aslında hep bu noktayı işaret ediyor. Örneğin Singapur'da Para Otoritesi (MAS), dolandırıcılık ve siber tehditlerle mücadele için operasyonel kontrolleri, teknoloji kullanımını ve raporlamayı belli standartlara bağlamış durumda. Ayrıca bankalarda bu iş için özel ve uzman ekiplerin kurulmasını teşvik ediyor; bu ekiplerin yetki ve görev tanımları da çok net belirleniyor. Böylece kurumlar, sadece kendi iç kaynaklarıyla değil, aynı zamanda sektör genelinde belirlenen standartlar sayesinde çok daha güçlü ve sürdürülebilir savunma mekanizmaları kurabiliyor.

Birleşik Krallık'ta ise sektörün önde gelen kuruluşları sayesinde bankalar ve ödeme kuruluşları arasında ortak hedefler ve performans ölçütleri tanımlanıyor. Suudi Arabistan'da, Merkez Bankası (SAMA), finansal kurumlar için dolandırıcılık yönetimine dair çok detaylı kurallar ve beklentiler yayınlıyor, kurumların bu alanda ekipler kurmasını ve yeni teknolojiler kullanmasını teşvik ediyor. Üstelik kurumlar arası toplantılar ve bilgi paylaşımı da düzenli şekilde yapılıyor.

Türkiye'de de bu tür iyi uygulamalar referans alınarak sektör genelinde iş birliği ve standartlaşmanın güçlendirilmesi, dolandırıcılıkla mücadelede ortak bir yaklaşım ve daha uyumlu bir yapı oluşturulmasına katkı sağlayacaktır. Böylece kurumların kendi inisiyatifiyle yürüttüğü çalışmalar, sektör genelinde daha tutarlı ve etkili sonuçlar doğuracaktır.

## Neler Yapılmalı?

### Ortak standartların oluşturulması

Dolandırıcılıkla mücadelede sektörde güçlü ve dengeli bir savunma hattı kurmak için ortak standartların belirlenmesi büyük önem taşıyor. Kurumların kendi çabaları değerli olsa da belli başlı gerekliliklerin ve beklentilerin netleştirilmesi, tüm sektörde daha tutarlı ve etkili bir yaklaşım sağlar.

Uluslararası iyi uygulamalara bakıldığında, dolandırıcılıkla mücadele standartlarının genellikle yönetim ve organizasyon yapısı, risk değerlendirme süreçleri, teknolojik altyapı ve veri analitiği, çalışan eğitimi ve farkındalık, müşteri güvenliği, olay bildirim ve müdahale prosedürleri ile kurumlar arası bilgi paylaşımı gibi ana başlıkları kapsadığı görülüyor. Bu başlıklar, dünya genelindeki başarılı modellerde de ortak noktaları oluşturuyor.

### Sektör genelinde uygulama

Türkiye’de de sektör genelinde iş birliği ve yukarıdaki ana başlıklar etrafında standartlaşmanın güçlendirilmesi, kurumların savunma kapasitesini ve risklere karşı hazırlığını artıracaktır. Böylece, dolandırıcılıkla mücadelede daha bütüncül, proaktif ve dirençli bir yapı kurmak mümkün hale gelecektir.



## Banka İçi Yönetişim Dönüşümü: Stratejik Risk Mimarisini Kurmak

Dolandırıcılıkla mücadele birimlerinin organizasyon içindeki konumları, sahip oldukları insan kaynağı kapasitesi, raporlama süreçleri ve üst yönetimle kurdukları iletişim, bu ekiplerin bağımsızlığını, karar alma hızını ve etkinliğini doğrudan etkiliyor.

Bankacılık sektöründe farklı organizasyon modelleri bulunsa da çoğu zaman bu birimlerin operasyon veya bilgi güvenliği departmanlarına raporladığı görülüyor. İdeal yapı olarak ise bilgi güvenliği, iç sistemler ya da risk yönetimi gibi daha stratejik birimlerle bir arada olması gerektiği görüşü hakim. Bu bulgu, operasyonel reflekslerin ötesinde kurumsal risk yönetimi bakış açısının önemini ortaya koyuyor.

Birimin organizasyon içindeki temsil seviyesi de önemli bir unsur. Üst yönetime veya yönetim kuruluna doğrudan raporlayan yapılar, genellikle daha proaktif savunma kapasitesi oluşturuyor ve kurumsal güvenlik kültürünün yaygınlaşmasını sağlıyor. Ayrıca, üst yönetim düzeyinde özel komitelerin oluşturulması ve bu komiteler aracılığıyla düzenli bilgilendirme ile koordinasyonun sağlanması, kurum genelinde farkındalık ve sahiplenmeyi artırıyor. Türkiye bankacılık sektöründe ise, dolandırıcılıkla mücadele birimlerinin çoğunlukla Genel Müdür Yardımcısı seviyesinin bir ya da iki kademe altında temsil edildiği görülüyor. Üst yönetimin yer aldığı bir dolandırıcılıkla mücadele komitesine sahip olan kurumların oranı ise %43. Bu tablo, dolandırıcılıkla mücadelenin pek çok kurumda hâlâ ağırlıklı olarak operasyonel düzeyde ele alındığını gösteriyor.

### Şekil 3: Dolandırıcılık Yönetimi: Raporlama ve Organizasyonel Yapı

Dolandırıcılıkla mücadele bölümü organizasyonda nereye raporlamaktadır?

**%50**

Operasyon

**%43**

Bilgi Güvenliği

**%7**

İç Sistemler

**%0**

Risk Yönetimi

Dolandırıcılıkla mücadele bölümü organizasyonda nereye raporlamalıdır?

**%0**

Operasyon

**%47**

Bilgi Güvenliği

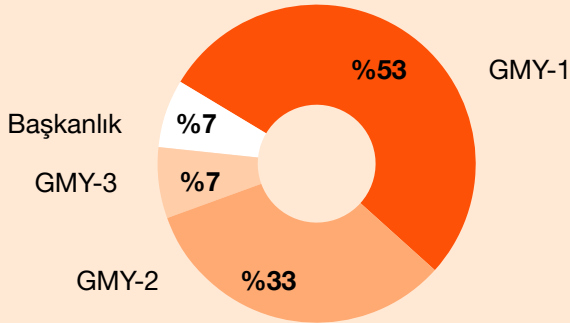
**%33**

İç Sistemler

**%20**

Risk Yönetimi

Dolandırıcılıkla mücadele bölümü organizasyonda hangi seviyede temsil edilmektedir?



Üst yönetimin katıldığı bir dolandırıcılıkla mücadele komitesi komitesi mevcut mudur?

**%43**

Evet

**%57**

Hayır

Günümüzde tehditler giderek çeşitlenip karmaşılaşırken, dolandırıcılıkla mücadele ekiplerinin sadece operasyonel görevlerle sınırlı kalmaması, aynı zamanda stratejik bir rol üstlenmesi gerekiyor. Çünkü dolandırıcılık riskleri yalnızca finansal kayıplarla sınırlı değil; itibar kaybı ve hizmetin sürekliliğinde yaşanacak sorunlar da önemli sonuçlar doğurabiliyor. Bu nedenle risklerin, kurumun genel stratejisine entegre şekilde ele alınması büyük önem taşıyor.

Bu noktada, dolandırıcılıkla mücadele birimlerinin bilgi teknolojileri, hukuk, uyum, müşteri deneyimi, siber güvenlik ve kriz yönetimi gibi farklı alanlarla yakın iş birliği içinde çalışması ve gelişmiş veri analitiği ile teknoloji altyapısından faydalanması kritik. Böyle bir yapı sayesinde riskler daha erken tespit edilebiliyor ve hızlıca müdahale edilebiliyor. Sonuçta, dolandırıcılıkla mücadele faaliyetlerinin kurumun stratejik planlarıyla bütünleşmesi, şirket genelinde daha güçlü ve dirençli bir yapı oluşturulmasını sağlıyor.

## Neler Yapılmalı?

### Üst Yönetim Temsili ve Raporlama

Dolandırıcılıkla mücadele birimlerinin şirkette nerede konumlandığı, kime rapor verdikleri ve organizasyondaki temsil düzeyleri, bağımsızlık ve karar alma hızı üzerinde doğrudan etkili olur. Bu nedenle, bu ekiplerin daha üst düzeyde temsil edilmesi ve doğrudan üst yönetime veya stratejik komitelere raporlama yapması, etkinliği artıracaktır.

### Stratejik İletişim ve Proaktiflik

Stratejik olarak konumlandırılmış ve üst yönetimle yakın çalışan dolandırıcılıkla mücadele ekipleri, sadece mevcut riskleri yönetmekle kalmaz, aynı zamanda potansiyel tehditlere karşı daha hazırlıklı olur ve daha hızlı aksiyon alabilir. Burada, ekibin düzenli olarak üst yönetimle iletişimde kalması ve kritik gelişmeleri hızla paylaşması önemlidir.

### Disiplinlerarası İş Birliği

Dolandırıcılıkla mücadelede en iyi sonuçlar, ekiplerin hukuk, bilgi teknolojileri, müşteri deneyimi, siber güvenlik ve kriz yönetimi gibi farklı alanlarla iş birliği yapması ve gelişmiş veri analitiği ile teknolojik altyapıdan yararlanmasıyla alınır. Bu nedenle, kurumlar arası disiplinlerarası iş birliği teşvik edilmeli ve teknolojik entegrasyon güçlendirilmelidir.



## Algoritmaların Ötesinde: Teknolojiyi Stratejik Ortağa Dönüştürmek

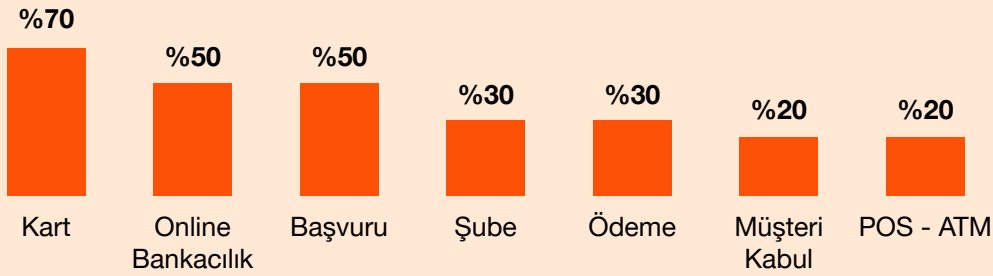
Dolandırıcılıkla mücadelede güçlü bir teknolojik altyapı ve gelişmiş analitik yetkinlikler, finansal kurumların riskleri önceden görebilmesi, anormallikleri zamanında fark edebilmesi ve hızlı harekete geçebilmesi açısından kritik bir rol oynuyor. Dolandırıcılık yöntemleri giderek daha karmaşık hale gelirken, finans sektöründe dijitalleşme de hız kazanıyor ve kurumlar teknoloji yatırımlarını artırmaya yöneliyor.

Sektördeki deneyim gösteriyor ki, eldeki veri kaynakları oldukça çeşitli olsa da bu verilerin merkezi ve entegre bir şekilde kullanılması için hâlâ önemli bir gelişim alanı var. Burada devreye, yapay zeka ve makine öğrenmesi gibi ileri teknolojiler giriyor. Bu teknolojilerin dolandırıcılıkla mücadele süreçlerine entegre edilmesi, risklerin çok daha öngörülebilir ve yönetilebilir hale gelmesini sağlıyor.

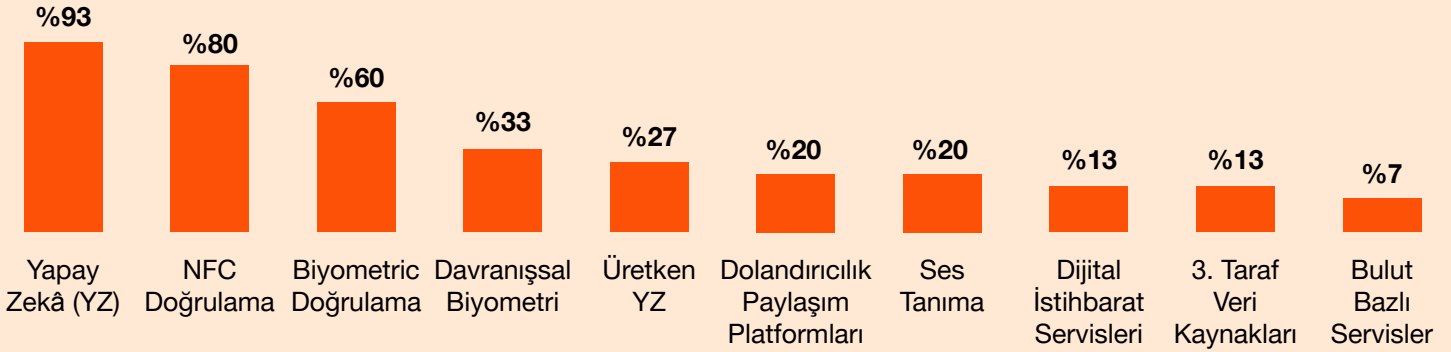
Bugün bankalar; kart işlemleri, online bankacılık ve başvuru süreçleri, şube ve ödeme sistemleri, müşteri kabul ve ATM/POS işlemleri gibi alanlarda bu modellerden yoğun olarak yararlanıyor. Önümüzdeki dönemde ise yapay zeka, NFC ve biyometrik doğrulama teknolojilerinin dolandırıcılıkla mücadelede daha fazla öne çıkması bekleniyor. Ayrıca davranışsal biyometri, üretken yapay zeka ve dolandırıcılık paylaşım platformları gibi yeni trendlerin de sektörde önemli bir yer edinmesi öngörülüyor.

#### Şekil 4: Mevcut ve Gelecek Dolandırıcılık Teknolojileri: Uygulama Alanları ve Beklenen Gelişmeler

Bankanızda hangi alanlarda dolandırıcılıkla mücadele modellerini (AI/ML) uygulamada kullanılmaktadır?



Önümüzdeki dönemde hangi dolandırıcılıkla mücadele teknolojilerinin öne çıkacağını düşünüyorsunuz?



Birden fazla seçim yapılabilmesi nedeniyle toplam %100'ü aşmaktadır.

Bu teknolojik dönüşüm, dolandırıcılıkla mücadele ekiplerinde ihtiyaç duyulan yetkinlikleri de önemli ölçüde değiştiriyor. Artık veri analizi, istatistik, veri görselleştirme, risk skorlama ve makine öğrenmesi gibi teknik beceriler ekipler için olmazsa olmaz hale gelmiş durumda. Bu alanlarda yetkinliğin artırılması yapılan teknoloji yatırımlarıyla birleştiğinde kurumların dolandırıcılığa karşı daha proaktif ve sürdürülebilir bir mücadele kapasitesi geliştirmesinin önünü açıyor.

Sonuç olarak, dolandırıcılıkla mücadelede daha etkili olmak için sadece tespit sonrası müdahale etmek yeterli değil. Güçlü analitik altyapılar, entegre veri stratejileri ve ileri teknolojilerle desteklenen sistematik ve proaktif bir yaklaşım benimsemek gerekiyor. Böylece riskler daha erken fark edilebilir ve kurumlar çok daha hazırlıklı bir şekilde harekete geçebilir.

## Neler Yapılmalı?

### Teknoloji ve Strateji Entegrasyonu

Yapay zeka ve analitik çözümler, ancak kurumun genel risk iştahı, süreç tasarımı ve karar destek sistemleriyle entegre şekilde planlandığında gerçek anlamda fayda sağlıyor. Aksi halde, yapılan teknoloji yatırımlarının etkisi sınırlı kalıyor.

### Entegre ve Tutarlı Veri Mimarisi

Farklı kaynaklardan toplanan veriler, ancak entegre ve tutarlı bir yapıda işlendiğinde anlamlı hale geliyor. Verilerin güvenilir ve senaryo bazlı analizlere uygun olarak yönetilmesi, analitik modellerin doğruluğunu ve kurumun karar süreçlerini önemli ölçüde güçlendiriyor.

### Davranışsal Modelleme ve Bağlamsal Analiz

Müşteri davranışları, işlem örüntüleri ve bağlam bazlı analizlere dayalı modeller, dolandırıcılıkla mücadelede yeni nesil bir koruma düzeyi sunuyor. Bu yaklaşım sayesinde riskler daha hassas şekilde tespit edilebiliyor.

### Disiplinlerarası Analitik Yetkinlik

İleri analitik kapasite, yalnızca teknoloji yatırımlarıyla değil; risk yönetimi, uyum ve hukuk gibi alanlarla iç içe çalışan, çok disiplinli ekiplerle sağlanabiliyor. Böylece geliştirilen modeller kurumun gerçek ihtiyaçlarıyla uyumlu oluyor.

### Sürekli Öğrenen Sistemler

Dinamik tehdit ortamında başarı, sadece erken tespitle değil, aynı zamanda sürekli geri bildirim alan ve kendini otomatik olarak geliştiren sistemlerle mümkün. Bu sayede risklere karşı her zaman bir adım önde olunabiliyor.

## Bilinçli Müşteri: Mücadelenin Stratejik Ortağı

Dolandırıcılıkla mücadelede sadece kurum içindeki güvenlik önlemleri yeterli olmuyor; müşteri bilinci ve farkındalık seviyesi de en az onlar kadar kritik bir savunma hattı sağlıyor. Finansal hizmetlerin dijitalleşmesiyle birlikte, bireysel kullanıcılar daha karmaşık ve çeşitli dolandırıcılık riskleriyle baş başa kalıyor. Bu nedenle, finans kurumları için müşteri farkındalığını artırmak artık bir tercih değil, adeta stratejik bir zorunluluk haline gelmiş durumda.

Sektör temsilcileri de son bir yılda dolandırıcılık vakalarının belirgin şekilde arttığını vurguluyor. Dahası, yaşanan zararların büyük bir kısmının doğrudan müşteriler tarafından karşılanması, konunun önemini daha da artırıyor.

## Şekil 5: Dolandırıcılık Zararlarının Müşteri Üzerindeki Etkisi ve Toplam Finansal Kayıplar

Son 1 yıl içinde yaşanan dolandırıcılık adet ve tutarı artmakta mıdır?

Katılımcıların **%87** 'si dolandırıcılık vakalarının arttığını belirtmektedir.

Son 1 yıl içinde yaşanan dolandırıcılık zararı içerisinde müşteri zararının yaklaşık oranı nedir?

Vakaların **%80** 'i müşteri kayıplarından oluşmaktadır.

Siber dolandırıcılık yöntemlerinin giderek daha ikna edici hale geldiği günümüzde, müşterilere yönelik iletişim, eğitim ve bilgilendirme çalışmalarının sadece farkındalık yaratmakla kalmaması, aynı zamanda dijital kanalların güvenli kullanımını teşvik edecek şekilde tasarlanması büyük önem taşıyor. Bu noktada, kullanıcı dostu güvenlik arayüzleri, çok katmanlı kimlik doğrulama sistemleri ve işlem sırasında verilen risk bildirimleri öne çıkan uygulamalar arasında yer alıyor.

Öte yandan, dolandırıcılığa maruz kalan müşterilerin yaşadığı süreçlerin hassasiyetle ve destekleyici bir müşteri deneyimiyle yönetilmesi, finans kurumlarına olan güvenin korunmasında kritik bir rol oynuyor. Şikâyet süreçlerinin ne kadar etkin ve bildirimlerin ne kadar hızlı yanıtlanmışlığı hem kurumsal itibarı hem de müşteri memnuniyetini doğrudan etkiliyor. Burada en önemli denge, güvenlik önlemlerini artırırken müşteri deneyimini zorlaştırmamak. Karmaşık ve kullanıcıyı zorlayan güvenlik adımları bir yandan koruma sağlarken diğer yandan müşteri memnuniyetini olumsuz etkileyebiliyor. Bu yüzden, güvenlik kadar müşteri deneyimini de merkeze alan, erişilebilir ve güvenilir dijital çözümlerle bu dengeyi yakalamak gerekiyor.

## Neler Yapılmalı?

### Müşteriyi stratejik savunma hattına dönüştürmek

Dijital dolandırıcılık risklerinin bireyleri doğrudan hedef alması, müşteri farkındalığını ve güvenlik davranışlarını artık şirket içi kontroller kadar stratejik bir savunma unsuru haline getiriyor. Bu nedenle, eğitim ve bilgilendirme faaliyetleri yalnızca farkındalık kazandırmakla kalmamalı; aynı zamanda dijital güvenlik alışkanlıklarını sürdürülebilir kılacak şekilde kurgulanmalı.

### Kullanıcı dostu güvenlik çözümleri geliştirmek

Güvenlik arayüzleri ve önlemleri, kullanıcıyı dışlamadan, deneyimi zorlaştırmadan tasarlanmalı. Çok katmanlı kimlik doğrulama, işlem sırasında çıkan uyarılar ve kişiye özel risk bildirimleri gibi çözümler hem güvenliği artırıyor hem de dijital müşteri memnuniyetini destekliyor.

### Mağdur müşteriyi şeffaf ve empatik iletişim kurmak

Dolandırıcılığa maruz kalan müşterilerle yürütülen iletişim ve süreç yönetimi, kurumun güvenilirlik ve şeffaflık algısını doğrudan etkiliyor. Empatiyle ve etkin bir şekilde yönetilen müşteri deneyimi, kriz anında bile müşteri sadakatinin ve marka itibarının korunmasına yardımcı oluyor.



# Sonuç

**Dijitalleşmenin ve teknolojinin hızla geliştiği günümüzde, bankacılık sektörü her zamankinden daha karmaşık dijital tehditler ve sosyal mühendislik odaklı dolandırıcılık senaryolarıyla karşı karşıya kalıyor.**

Artık dolandırıcılıkla mücadele, sadece tek bir kurumun kendi başına üstesinden gelebileceği bir konu olmaktan çıktı; farklı paydaşların ortak hareket ettiği güçlü bir ekosistem ve iş birliği anlayışı gerektiriyor.

Bu nedenle hem sektör hem de kurum bazında geliştirilecek kapsamlı stratejilerin; paydaşlar arası etkili iş birliği, ulusal ölçekte güçlü bir koordinasyon ve güncel düzenleyici çerçevelerle desteklenmesi, sürdürülebilir sonuçlar elde edilmesini sağlayacaktır.

Ayrıca, dolandırıcılıkla mücadelenin kurum stratejilerinin ayrılmaz bir parçası haline gelmesi; teknolojik altyapıların ve analitik yetkinliklerin geliştirilmesi ve müşteri farkındalığını artıracak uygulamaların hayata geçirilmesi, risklerin çok daha proaktif ve öngörülebilir şekilde yönetilmesine yardımcı olacaktır. Sektör genelinde kalıcı ve güçlü bir direnç oluşturmak için bu bütüncül yaklaşım ortak hedef olarak benimsenmeli.





## İletişim



**Dr. Gökhan Yılmaz**  
Şirket Ortağı, PwC Türkiye  
gokhan.yilmaz@pwc.com

**pwc.com.tr**

© 2025 PwC Türkiye. Tüm hakları saklıdır. Bu belgede PwC ifadesi, PwC ağını veya PwC ağının üyesi olan bağımsız ve farklı tüzel kişiliklerden oluşan PwC Türkiye'yi ifade etmektedir. Daha detaylı bilgi için [www.pwc.com/structure](http://www.pwc.com/structure) adresini ziyaret edebilirsiniz.