SANCTION SCANNER

2024 - 2025

Finansal Suçlar ve Uyumluluk Raporu

SANCTION SCANNER

Rapor Hakkında

2024-2025 Finansal Suçlar ve Uyumluluk Raporu'nun üçüncü baskısı, küresel finansal suçlarla mücadelede kapsamlı analizler ve sektör içgörüleri sunmayı hedefliyor. Bu rapor, dünya genelinde gelişen tehditlere, yasal düzenlemelere ve uyumluluk süreçlerine dair kritik bilgileri, sektör liderlerinin güncel verilerle desteklenen görüşleri ışığında bir araya getiriyor.

Sanction Scanner olarak misyonumuz, finansal sistemlerin güvenliğini sağlamak ve sektör paydaşlarına, finansal suçlara karşı etkin bir savunma hattı oluşturmada rehberlik etmektir. Okuyacağınız rapor, sadece bugünün değil, yarının da uyum stratejilerini geliştirmeye yönelik bir kaynak sunarak finans dünyasının hızla değişen dinamiklerine ayak uydurulmasına katkı sağlamayı amaçlamaktadır.

İÇİNDEKİLER

HAKKIMIZDA

Sanction Scanner, 2019 yılında kurulan kara para aklamayı önleme ve risk çözümleri sağlayıcısıdır. Şahısları ve işlemleri 220'den fazla ülkenyi kapsayan bir veritabanı aracılığıyla tarar. Ayrıca, her işlemi gerçek zamanlı olarak izleyen ve şüpheli işlemleri tespit eden bir işlem izleme çözümü sağlar. Özetle, verileri anında analiz eden ve 360° risk değerlendirmesi sağlayan hepsi bir arada bir uyumluluk yaklaşımı sunar.

Sanction Scanner, her ülkenin değişen düzenlemelerine uygun olarak finansal riskleri en aza indirmeyi amaçlıyor. Bankacılık, yatırım, finans, sigorta, ödeme, fintek, kripto, para transferi, finansal kiralama ve faktoring gibi çeşitli sektörlerden müşterilere hizmet veriyor.

Yılın Değerlendirmesi

Yılın Değerlendirmesi

2024'ün son günlerine yaklaşırken, bu yılın finansal suçlar ve uyum dünyası için sıradan bir yıl olmadığını net bir şekilde görüyoruz. Şaşırtıcı mali suç istatistikleri, gelişen düzenlemeler ve artan jeopolitik gerilimler, finans dünyasını yeniden şekillendirdi. Bu değişimlerin etkisi dünya genelinde hissedilirken, hem acil müdahaleleri hem de uzun vadeli stratejileri zorunlu kıldı.

Durumu net bir şekilde değerlendirecek olursak, geçtiğimiz yıl küresel finans sistemi üzerinden yaklaşık **3.1 trilyon dolar** değerinde yasa dışı fon hareket etti. Bu muazzam rakamın yaklaşık **782.9 milyar** doları uyuşturucu kaçakçılığından, **485.6 milyar** doları dolandırıcılıktan, **346.7 milyar** doları insan kaçakçılığından, **11.5 milyar** doları ise terörün finansmanından kaynaklanıyor. Bu veriler, sorunun büyüklüğünü ortaya koymakla kalmıyor, aynı zamanda dünya genelindeki finans kuruluşlarının yenilikçi çözümlere duyduğu kritik ihtiyacı da gözler önüne seriyor.

2023 yılında küresel finans sistemi üzerinden yaklaşık 3.1 trilyon dolarlık yasa dışı fon akışı gerçekleşti.

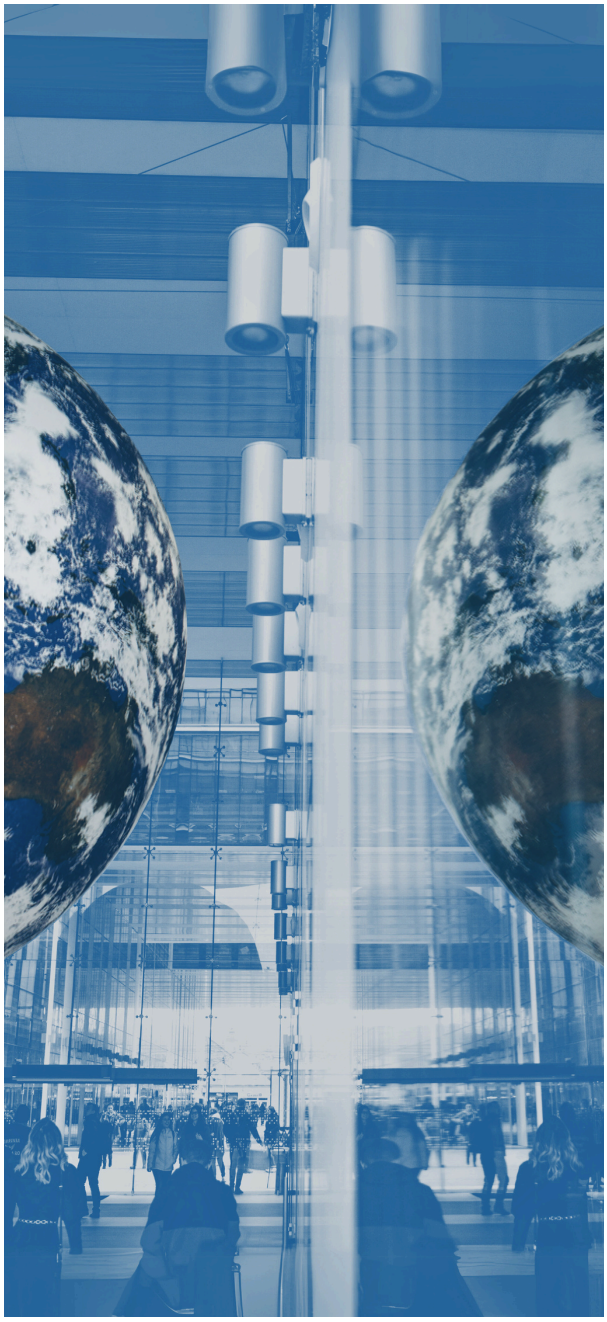
Uyuşturucu kaçakçılığıyla elde edilen **782.9 milyar dolar**

Dolandırıcılık yoluyla elde edilen **485.6 milyar dolar**

İnsan kaçakçılığıyla elde edilen **346.7 milyar dolar**

Terörün finansmanı için kullanılan **11.5 milyar dolar**

Jeopolitik gelişmeler durumu daha da karmaşık hale getirmiştir. Batı Şeria ve Gazze'de devam eden olaylar, terörizmle bağlantılı finansal işlemler ile insani yardımların kötüye kullanımını daha sıkı denetim altına almayı gerektirmektedir. Yaptırımların uygulanmasının daha kolay olduğu Rusya-Ukrayna çatışmasının aksine, Orta Doğu'daki durum daha karmaşık ve belirsiz bir zorluk teşkil etmektedir. Bu bağlamda, durumu suistimal eden kişileri tespit etmek ve aksiyon almak çok daha zor olduğundan derinlikli bir yaklaşım gerektirmektedir. Dolayısıyla, kurumların bölgedeki faaliyetlerini ve olası yaptırımlara ne kadar hazırlıklı olduklarını kapsamlı bir şekilde değerlendirmeleri zorunludur.



Ekonomik zorluklar durumu daha da karmaşık hale getirmiştir. Mali sıkıntıların yaşandığı dönemlerde, toplumlar artan istikrarsızlık ve öngörülemezlikle mücadele ederken, perde arkasında gizli kara para aklama tehditleri de yoğunlaşmaktadır. Küresel ekonomi yavaşlayıp bütçeler daraldıkça, finansal kurumlar büyük baskı altında kalmakta ve ekonomik sıkıntıların suç faaliyetlerindeki artan etkisiyle başa çıkmaya çalışmaktadır. Bu durum, daha verimli çözümlere ve daha akıllı kaynak yönetimine duyulan ihtiyacı ivedilikle aksiyon alınması gereken projeler olarak yapılacaklar listesine almamızı sağlamıştır.

Diğer taraftan, teknoloji bu zorlukların üstesinden gelmek için hızla gelişmiştir. Örneğin, yapay zeka, analiz ve izleme için gelişmiş araçlar sunarak mali suçların tespit edilmesi ve önlenmesinde önemli bir müttefik olmuştur. Ancak, bu ilerleme yeni riskleri de beraberinde getiriyor; suçlular yapay zekayı kullanarak sofistike sahtecilikler ve sentetik kimlikler oluşturarak, kurumların gelişen tehditlere ayak uydurma çabalarını zorlaştırmaktadır.

Uyum görevlilerinin
%38'i
2024'teki en büyük zorluğun yaptırımların karmaşıklığı olduğunu düşünüyor.

2024, sınır ötesi mali suçların artışı, yeni dolandırıcılık trendleri ve yüksek riskli ülkelerdeki değişikliklerle hızlı ve zorlu bir yıl oldu. Sanction Scanner tarafından yapılan anket, uyum görevlilerinin %38'inin, yaptırımların 'karmaşıklığını' 2024'teki en büyük zorluk olarak tanımladığını gösterdi.

Jeopolitik Mercekten Mali Suçlar

Jeopolitik Mercekten Mali Suçlar

Amerika

Amerika Birleşik Devletleri, mali suçlarla küresel mücadelede odak noktası olmaya devam etmekte ve karmaşıklığı artan çok yönlü bir tehdit ortamıyla karşı karşıya kalmaktadır. A.B.D'de yılda tahminen **300 milyar dolar** aklanmakta ve bu miktar, küresel kara para aklama faaliyetlerinin **~%15-%38'ini** oluşturmaktadır. Bu durum, finansal suçlarla mücadelede karşılaşılan tehditlerin son derece ciddi olduğunu gösteriyor.

Yasa dışı finansın yarattığı zorluklar, teknolojideki hızlı ilerlemeler, değişen düzenleyici ortam ve jeopolitik gerilimlerle daha da artmaktadır. Bu bölümde, ABD'de 2024 yılında mali suç ortamını şekillendiren önemli gelişmeler ele alınmakta; mevzuatın, düzenleyici denetimin ve ortaya çıkan tehditlerin etkileri incelenmektedir.

> ABD uyum ortamındaki yoğun düzenleyici gereklilikler göz önüne alındığında, çoğu zaman en iyi yol en basit olanıdır. Risk Tabanlı Yaklaşım, kurumunuz, programınız, müşteri tabanınız ve ürünleriniz hakkında kapsamlı bir bilgi edinmenin önemli bir ilk adımıdır. İyi planlanmış bir risk değerlendirmesi, sürdürülebilir bir AML programı için temel bir gerekliliktir.

Mario M. Duron
Chief Compliance Officer

Terörizm ve Diğer Yasa Dışı Finansmanlarla Mücadele Ulusal Stratejisi

ABD Hazine Bakanlığı'nın 2024 Terör ve Diğer Yasa Dışı Finansmanlarla Mücadele Ulusal Stratejisi, kritik mali suç tehditleriyle etkili bir şekilde mücadele etmek için kapsamlı bir çerçeve sunmaktadır. Bu strateji, 2024 Ulusal Risk Değerlendirmeleri temel alınarak, büyük ölçekli dolandırıcılık, fidye yazılımı saldırıları ve terörizmin finansmanı gibi önemli risklere odaklanmaktadır.

Belirtilen tehditleri ele alan strateji, dört temel önceliğe odaklanmaktadır:

1. İlk olarak, intifa hakkı sahipliği kaydını işler hale getirerek ve gayrimenkul ile yatırım danışmanlığı gibi yüksek riskli sektörlere yönelik kuralları kesinleştirerek yasal ve düzenleyici boşlukları kapatmak.

2. İkinci olarak, daha net rehberlik ve daha iyi kaynak tahsisi yoluyla verimliliği ve etkinliği artırmak amacıyla ABD AML/CFT düzenleyici çerçevesini geliştirmek.

3. Üçüncü olarak, yasa dışı aktörlerin güvenli sığınaklar bulmasını önlemek için kolluk kuvvetleri ve ilgili kurumların operasyonel yeteneklerini güçlendirmek.

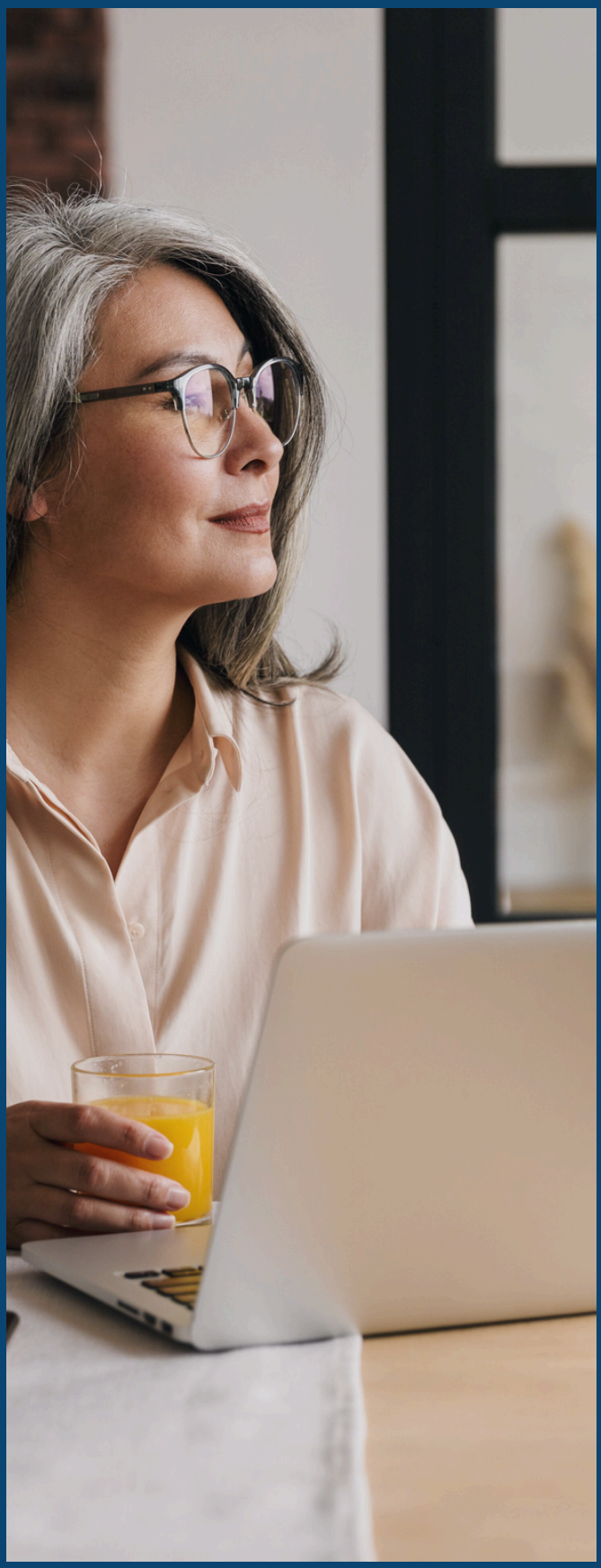
4. Son olarak, ödeme teknolojilerini ve uyum mekanizmalarını geliştirmek için teknolojik yenilikleri benimseyerek gelişen tehditlerin önüne geçmek.

Strateji, kamu ve özel sektör çabalarını uyumlu hale getirerek yasa dışı finansman riskini azaltmaya yönelik ortak bir yaklaşım sağlamayı hedeflemektedir. Şeffaflığı, düzenleyici etkinliği ve teknolojik çözümleri artırmayı hedefleyen 2024 Stratejisi, ABD finans sisteminin sofistike mali suçlara karşı direncini güçlendirmeyi amaçlamaktadır.

İntifa Hakkı Sahipliğinin Şeffaflığının Artırılması

Kurumsal Şeffaflık Yasası'nın (CTA) 1 Ocak 2024 tarihinde yürürlüğe girmesi, Amerika Birleşik Devletleri'nin mali suçlarla mücadele çabalarında önemli bir kilometre taşını temsil ediyor. CTA'nın 2021'deki ilk kabulü ve 2023'te yapılan kritik değişiklikler, yıllarca süren yasama çabalarının doruk noktasıdır. Bu yasa, uzun süredir kara para aklama, terörizmi finanse etme ve vergi kaçırma amacıyla yaygın olarak kullanılan paravan şirketler sorununu hedef almaktadır. FinCEN'e göre, 2016 ile 2023 yılları arasında soruşturulan kara para aklama vakalarının **%85'inde** anonim paravan şirketlerin yer alması, bu mevzuata olan ihtiyacın aciliyetini daha da netleştirmiştir.

CTA kapsamında, ABD'de faaliyet gösteren 32 milyondan fazla yerli ve yabancı kuruluşun artık intifa hakkı sahiplik bilgilerini (BOI) FinCEN'e açıklamaları gerekmektedir. Bu, tarihsel olarak kötü niyetli aktörlerin tüzel kişilikleri yasa dışı amaçlarla kullanmasına olanak tanıyan gizlilik perdesini ortadan kaldırmayı hedeflemektedir. CTA, şirketlerin gerçek sahiplerine ait tam adlar, doğum tarihleri, mevcut adresler, pasaport veya ehliyet üzerinde bulunabilecek benzersiz kimlik numaraları gibi ayrıntılı bilgiler sunmalarını zorunlu kılmaktadır. Bu gerekliliğe uyulmaması durumunda, ihlal başına 500 dolara (10.000 $'a kadar) varan ağır para cezaları ve iki yıla kadar hapis cezası öngörülmektedir.



FinCEN'in 2023 yılında geliştirdiği yeni raporlama sistemi, beklenen büyük veri akışını yönetmek üzere tasarlanmıştır. Sistemin etkinliği, kolluk kuvvetlerinin yasa dışı fonların izini sürmesi, suç şebekelerini tespit etmesi ve suçluları sorumlu tutması açısından kritik öneme sahiptir. CTA'nın başarısı, FinCEN'in BOI verilerini etkin bir şekilde yönetme ve analiz etme becerisinin yanı sıra işletmelerin yeni düzenlemelere uyum sağlamasına da bağlı olacaktır.

Kripto Düzenlemeleri

Kripto para birimlerinin hızlı büyümesi, düzenleyiciler için yeni zorluklar doğurmuştur. 2024 yılı, hem dijital varlıkların benimsenmesinde hem de buna bağlı mali suç risklerinde önemli bir artışa tanıklık etti.

Sadece 2023 yılında, küresel kripto para piyasa değeri **yaklaşık 2,6 trilyon dolara** ulaşmış ve ABD, bu piyasanın **yaklaşık %40'ını** oluşturmuştur.

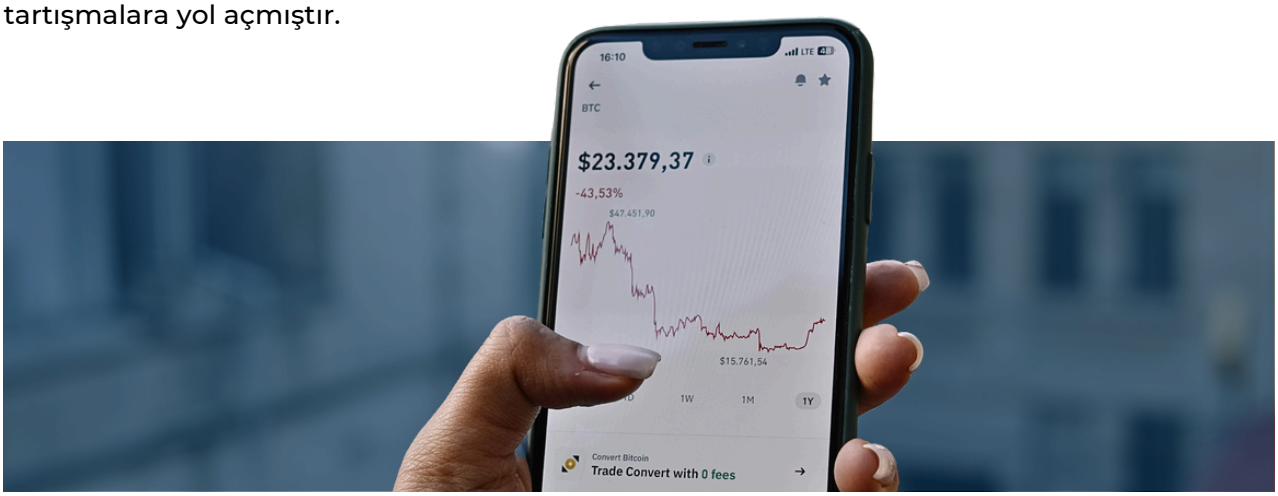
Ancak bu hızlı büyüme, kripto paraları kara para aklama, dolandırıcılık ve terör finansmanı için birincil hedef haline getirmiş ve düzenleyici incelemelerde keskin bir artışa yol açmıştır.

Finans Endüstrisi Düzenleme Kurumu (FINRA), kripto varlık iletişimlerine yönelik incelemeler yürüttü. FINRA, incelediği kripto iletişimlerinin yaklaşık %70'inin, çoğunlukla yanıltıcı veya aldatıcı ifadelerle ilgili potansiyel ihlaller içerdiğini tespit etmiştir. Bu bulgular, 2024 yılında düzenleyici standartlara uymayan şirketleri hedef alan agresif yaptırım eylemleri için zemin hazırlamaktadır.

Düzenleyici ortamı etkileyen dönüm noktası niteliğindeki bir dava, bir zamanlar dünyanın en büyük kripto para borsalarından biri olan FTX'in eski CEO'su Sam Bankman-Fried'in yargılanmasıdır. FTX'in 2022'nin sonlarında çökmesi, yatırımcılar için 10 milyar doları aşan kayıplara yol açmış ve kripto endüstrisinin doğasında bulunan düzenlenmemiş risklerin bir sembolü haline gelmiştir. SBF'nin 2024 yılının başlarında sonuçlanan davasında dolandırıcılık, kara para aklama ve komplo suçlamalarından suçlu bulunması, bu yüksek profilli davanın, terör örgütleri tarafından kripto para birimlerinin artan kullanımıyla birleştiğinde, ABD hükümetinin kripto düzenlemesine yaklaşımını önemli ölçüde şekillendirmiştir.

Bu gelişmelere yanıt olarak Biden yönetimi, 2024 yılında dünyanın ilk Merkeziyetsiz Finans (DeFi) Yasa Dışı Mali Risk Değerlendirmesi'nin yayınlanmasıyla kararlı adımlar atmıştır. Bu değerlendirme, 2023 yılı boyunca geliştirilmekte olan DeFi platformlarının Kuzey Koreli aktörler tarafından 1 milyar doları aşan meblağlarda para aklama adına kullanılması ve yalnızca 2023 yılında ABD'li işletmelere yaklaşık **600 milyon dolara** mal olan fidye yazılımı saldırılarının kolaylaştırılmasındaki rolleri de dahil olmak üzere oluşturduğu riskleri vurgulamaktadır. Rapor, Kongre'de DeFi platformları için KYC ve AML gereklilikleri de dahil olmak üzere daha sıkı düzenlemelere duyulan ihtiyaç hakkında tartışmalara yol açmıştır.

Bir diğer önemli yasal gelişme ise, 21. Yüzyıl için Finansal Yenilik ve Teknoloji Yasası'nın (FIT21) Temsilciler Meclisi'nde kabul edilmesidir. 2023 yılında tanıtılan ve 2024 yılında kabul edilen FIT21 Yasası, dijital varlıklar için kapsamlı bir düzenleyici çerçeve oluşturmayı ve kripto pazarında çok ihtiyaç duyulan netliği sağlamayı hedeflemektedir. Yasa, kripto yatırımlarıyla ilişkili riskleri azaltmak ve dijital varlıkların finansal sisteme güvenli ve şeffaf bir şekilde entegre edilmesini sağlamak amacıyla yeni tüketici koruma önlemleri ve kayıt rejimlerinde güncellemeler önermektedir.



Yatırım Danışmanlarına Yönelik Uyum Baskıları

Dünya genelinde **tahmini 110 trilyon dolarlık** varlığı yöneten yatırım danışmanları, özellikle kara para aklama riskleri açısından Amerika Birleşik Devletleri'nde giderek daha fazla inceleme altına alınmaktadır. ABD Hazinesi tarafından 2023 yılında gerçekleştirilen kapsamlı bir risk değerlendirmesi, yatırım danışmanlarının **yaklaşık %20'sinin** yetersiz AML programlarına sahip olduğunu ve bu durumun onları suçlular tarafından istismara açık hale getirdiğini ortaya koymuştur.

Bu risklerin farkına varan FinCEN, 2023'ün sonunda, 2024'te yürürlüğe koymak üzerek yeni düzenlemeler önerdi. Bu düzenlemeler, yatırım danışmanlarını diğer finansal kurumlarla aynı AML ve CFT yükümlülüklerine tabi olmalarını hedeflemektedir. Yeni kurallar, yatırım danışmanlarının güçlü AML ve CFT programları uygulamalarını, düzenli risk değerlendirmeleri yapmalarını ve şüpheli faaliyetleri FinCEN'e bildirmelerini gerektirmektedir.

Bu gerekliliklerin, ABD'de toplamda 100 trilyon doların üzerinde varlığı yöneten yaklaşık 14.000 kayıtlı yatırım danışmanını etkilemesi beklenmektedir. Düzenlemelere uyulmaması durumunda, FinCEN ve Menkul Kıymetler ve Borsa Komisyonu'nun (SEC) 2024 yılında yaptırım çabalarını artırması nedeniyle önemli para cezaları ve diğer yaptırımlar söz konusu olabilir.

Sadece 2023 yılında SEC, AML ihlalleri nedeniyle finans kuruluşlarına toplam 1,5 milyar doların üzerinde ceza kesmiştir ve bu rakamın yeni düzenlemelerin tam olarak yürürlüğe girmesiyle daha da artması beklenmektedir. Bu gelişmeler, büyük bankalardan daha küçük yatırım firmalarına kadar tüm oyuncuların en yüksek uyum standartlarına bağlı kalmasını sağlayarak, ABD finansal hizmetler sektörü genelinde finansal suç kontrollerinin sıkılaştırılmasına yönelik daha kapsamlı bir yaklaşıma işaret etmektedir.

ABD'nin önümüzdeki yıllara yönelik mali suçlarla mücadele yaklaşımı, şeffaflığı artırma, düzenlemeleri sıkılaştırma ve ortaya çıkan tehditleri ele alma gibi daha geniş bir stratejiyi yansıtmaktadır. Ülke, gelişen ortama uyum sağlamaya devam ederken, bu önlemlerin etkinliği finansal sistemin bütünlüğünün korunmasında kritik öneme sahip olacaktır. Teknoloji, düzenleme ve jeopolitiğin kesişimi, ABD'de mali suçların önlenmesinin geleceğini şekillendirmede belirleyici bir rol oynayacak ve politika yapıcıların, düzenleyicilerin ve sektör paydaşlarının çabalarında dikkatli ve proaktif olmalarını zorunlu hale getirecektir.

Birleşik Krallık

Birleşik Krallık, hem süregelen zorlukları hem de önemli ilerlemeleri yansıtacak şekilde, ekonomik suçlarla mücadele stratejilerini ve çerçevelerini geliştirmeye devam etmiştir. 2023'te başlatılan Ekonomik Suç Planı 2 (ECP2), Birleşik Krallık'ın ekonomik suçlarla mücadele kapasitesini artırmayı hedefleyen 400 milyon sterlinlik stratejik bir yatırımı temsil etmektedir.

ECP2, birkaç temel hedefe odaklanmıştır:

- Mevcut kara para aklama düzenlemelerinin etkinliğini artırmak.
- Sınır ötesi bilgi paylaşımının iyileştirilmek.
- Düzenleyici kurumlar ile kolluk kuvvetlerini daha fazla işbirliğine teşvik etmek.

Ulusal Suç Ajansı'nın (NCA) karmaşık mali suçları soruşturma ve kovuşturma kapasitesinin, genişletilmiş kaynaklar ve yasa dışı faaliyetleri tespit etmek ve engellemek için geliştirilmiş teknolojik araçlarla güçlendirilmesi ana odak noktalarından biridir. Ayrıca, planın bir diğer önemli unsuru, küresel mali suç ağlarını daha etkin bir şekilde ele almak için yerel ve uluslararası ortaklar arasında efektif koordinasyonun sağlanmasıdır.

Ekonomik Suç ve Kurumsal Şeffaflık Yasası (ECCTA) 2023, Birleşik Krallık'ın ekonomik suça yönelik yasal yaklaşımında önemli bir değişime işaret etmektedir. Bu yasa, kurumsal şeffaflığı ve hesap verebilirliği artırmak amacıyla birçok kilit reform getirmektedir.

Yasa, belirli bir mali büyüklüğe ve çalışan sayısına sahip olup dolandırıcılığı önleyemeyen firmalar için yeni bir suç tanımı getirmektedir. Ayrıca, Companies House'a ek bilgi talep etme, düzeltici tedbirleri uygulama ve verileri daha proaktif bir şekilde paylaşma konusunda genişletilmiş yetkiler verilmektedir. Bu değişiklik, kurumsal kayıtların doğruluğunu ve bütünlüğünü iyileştirmeyi ve kötüye kullanım alanlarını daraltmayı amaçlamaktadır.

Yasa, tüm şirket yöneticilerinin ve 'Önemli Kontrole Sahip Kişilerin', doğrudan Companies House ile ya da onaylı sağlayıcılar aracılığıyla kimlik doğrulamasından geçmesini gerektirerek intifa hakkı sahiplik bilgilerinin güvenilirliğini artırmaktadır. Bu reformlar, Birleşik Krallık'ın ekonomik suçlarla mücadelesini güçlendirirken, kurumsal şeffaflığı ve güveni artırmayı hedeflemektedir.

Ekonomik Suç ve Kurumsal Şeffaflık Yasası (ECCTA) 2023 çerçevesinde kayda değer güncellemelerden biri, kripto varlıklarının düzenlenmesidir. Bu yasa, dijital para birimleriyle ilişkili risklerin giderek daha fazla tanınmasını yansıtarak, suç faaliyetleriyle bağlantılı kripto varlıklarına el koymak ve bunları kurtarmak için yeni yetkiler getirmektedir.

Söz konusu hüküm, kripto varlıkların yasa dışı amaçlarla kötüye kullanımını ele almayı ve düzenleyici çerçevenin teknolojik gelişmelerle birlikte ilerlemesini sağlamayı amaçlayan daha geniş bir çabanın parçasıdır.

HM Treasury'nin Mayıs 2024'te yayımladığı 2022-2023 AML/CTF denetim raporu, Birleşik Krallık'ın düzenleyici ortamının 2024'te nasıl geliştiğini gösteriyor. Rapor, sektördeki ilerlemeleri ve karşılaşılan zorlukları ana hatlarıyla ortaya koyuyor. Düzenlemeye tabi işletmelerin yaklaşık %10'unun yüksek riskli olarak değerlendirildiği belirtiliyor.

Ek olarak, bu dönemde uygulanan toplam para cezasının **197 milyon sterlin** olduğunu, bir önceki yıl bu rakamın **504 milyon sterlin** olduğunu vurguluyor. FCA, **19,4 milyon sterlin** ile en yüksek ortalama para cezasını kesen kurum olarak en aktif denetleyici olmayı sürdürüyor. Rapor ayrıca, perakende ve toptan bankacılık, varlık yönetimi ve kripto varlık firmaları gibi ekonomik suça karşı özellikle savunmasız sektörleri de kapsıyor. Yetersiz risk değerlendirmeleri, yetersiz personel eğitimi ve yetersiz kayıt tutma gibi AML politikalarında karşılaşılan sorunlar, AML kontrollerinde sürekli bir ihtiyat ve iyileştirme gereğini vurguluyor. Bu durum, düzenleyicilerin ve işletmelerin, ekonomik suçlarla mücadelede daha etkili stratejiler geliştirmeleri gerektiğini göstermektedir.

2024, yaptırımlar açısından önemli aksiyonların alındığı bir yıl oldu. En dikkat çekeni ise Gamesy Operations Limited'in, yeterli AML kontrolleri yapmadığı için Ocak ayında Kumar Komisyonu tarafından **6 milyon sterlin** para cezasına çarptırılmasıydı. Öte yandan FCA da aktif olarak çalışmış ve yetersiz AML kontrolleri nedeniyle kripto kayıt başvurularının **%88'inden fazlasını** reddederek düzenleyicinin finansal kurumların katı AML gerekliliklerine uymasını sağlama konusundaki kararlı duruşunu göstermiştir.

FCA,
19,4 milyon sterlin
ile en yüksek ortalama para cezasını kesen kurum

Birleşik Krallık Kumar Komisyonu, daha geniş düzenleyici ortamın bir parçası olarak finansal risk kontrolleri hakkında önemli bir güncelleme sağlamıştır. 22 Şubat'ta yayımlanan güncellemeler, iflas kararları ve ödenmemiş müşteri borçları gibi risklerin belirlenmesine odaklanarak kumar sektöründeki finansal kırılganlığı ele almak için atılacak adımları özetlemiştir. Bu adımlar, hükümetin çeşitli reformları içeren Kumar Beyaz Kitabı'nı takip etmektedir. Ayrıca, Birleşik Krallık hükümeti 25 yaş ve üzeri yetişkinler için 5 sterlinlik bir bahis üst limiti ve 18-24 yaş arası kişiler için online slot oyunlarında 2 sterlinlik bir üst limit getirmiştir. Bu sınırlar, dürtüsel kumar riskini azaltmayı ve sorumlu oyun uygulamalarını güçlendirmeyi amaçlamaktadır.

Ocak 2024'te Birleşik Krallık, Kara Para Aklama Yönetmelikleri'nde (MLRs) değişiklikler yaparak PEP'lere yönelik muameleyi yeniden tanımlamıştır. Güncellenen yönetmelikler, yurt içindeki PEP'lerin Gelişmiş Durum Tespiti'ne tabi olacağını ancak genel olarak denizaşırı PEP'lere göre daha düşük riskli kabul edileceğini belirtmektedir. Ayrıca, "yüksek riskli üçüncü ülkeler" tanımı, FATF tarafından belirlenen ülkelerle uyumlu hale getirilerek, küresel ölçekte daha koordineli AML/CFT yaklaşımına doğru bir geçişin sinyalleri verilmiştir. Hükümetin MLR reformuna ilişkin istişaresinin, müşteri durum tespitini daha profesyonel hale getirmeyi hedefleyerek Birleşik Krallık'ın AML çerçevesine daha fazla iyileştirme getirmesi beklenmektedir.

Buna paralel olarak, Birleşik Krallık Hukuk Komisyonu'nun dijital varlıkların kişisel mülkiyet olarak tanınmasına yönelik istişaresi önemli bir gelişme göstermektedir. 2024'ün başlarında başlatılan bu teklif, geleneksel mülkiyet tanımlarına uymayabilecek dijital varlıkları kapsayacak yeni bir kişisel mülkiyet kategorisine ihtiyaç olduğunu ortaya koymaktadır. İstişare, bu sınıflandırmanın dijital varlıklara nasıl uygulanabileceğini ve özellikle mülkiyet, haksız fiil ve ilgili çözüm yollarıyla ilgili olarak ortaya çıkabilecek potansiyel yasal hak ve sorumlulukları araştırmaktadır. Bu gelişen yasal çerçeve, Birleşik Krallık'ın potansiyel suistimallere karşı koruma sağlarken yeni teknolojileri düzenlemeye yönelik çabalarını göstermektedir.

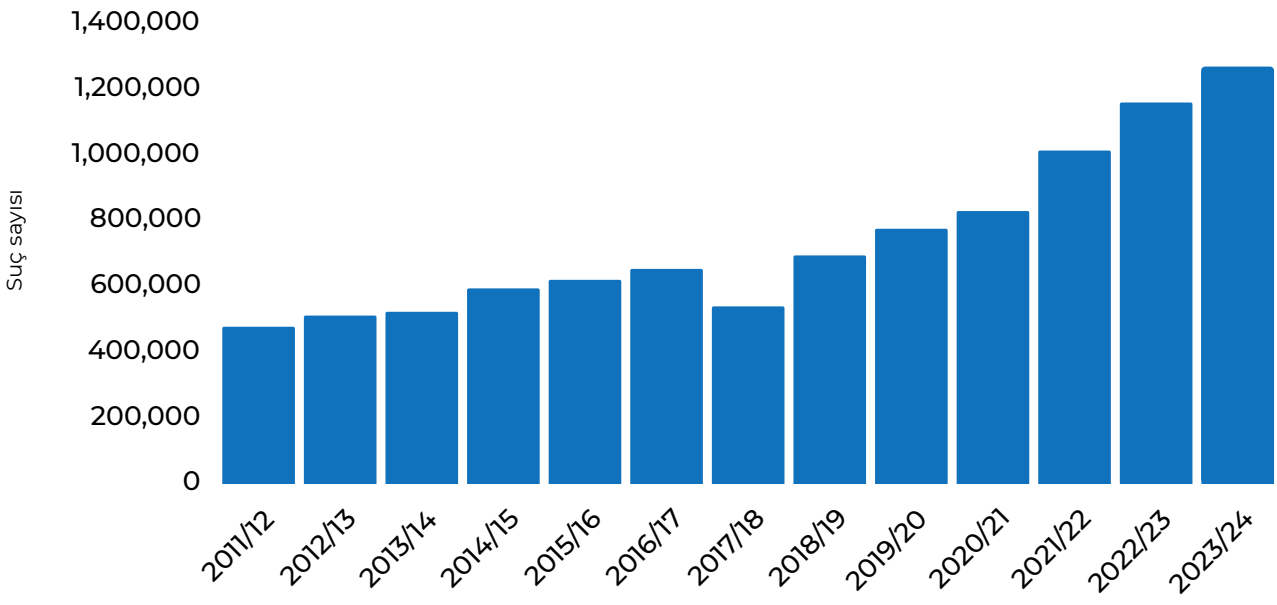
Bir diğer gelişme, Çevre Ajansı'nın yasa dışı mali akışlarla giderek daha fazla bağlantılı hale gelen atık sektöründe kara para aklama ile mücadeleye odaklanan Ekonomik Suç Birimi'ni kurmasıdır. Bu birim, hedefe yönelik soruşturmalar yürütmeyi, varlık reddi önlemlerini takip etmeyi ve sektördeki mali suçlarla başa çıkmak için diğer uygulayıcı kurumlarla işbirliği yapmayı amaçlamaktadır.

Dolandırıcılık, Birleşik Krallık'taki en önemli sorunlardan biri olmaya devam etmektedir. 2023 Yarı Yıl Dolandırıcılık Raporu, Yetkili Anında Ödeme (APP) dolandırıcılığının **%77'sinin** çevrim içi platformlardan kaynaklandığını ve dolandırıcılık kayıplarının **%45'inin** telekomünikasyon dolandırıcılığına dayandığını ortaya koymaktadır. Hükümet, Mayıs 2023'te dolandırıcılık ve siber suçları 2025 yılına kadar %10 oranında azaltmayı hedefleyen yeni bir strateji uygulamaya koymuştur.

Çevrim içi Dolandırıcılık Tüzüğü'nün 2023 yılı sonunda yürürlüğe girmesi, 12 büyük teknoloji şirketinin daha sıkı dolandırıcılık önleme tedbirleri almayı taahhüt etmesiyle önemli bir adım olarak görülmektedir.

Zorlu duruma rağmen Birleşik Krallık her geçen gün istikrarlı bir ilerleme kaydetmektedir. UK Finance, tüketicilerin 2023 yılında dolandırıcılık ve sahtekârlık nedeniyle **1,168 milyar sterlin** kaybettiğini ve bunun bir önceki yıla göre **%4'lük bir azalma** olduğunu bildirmiştir. Yetkili dolandırıcılık, özellikle APP dolandırıcılığı, bankaların eğitim, teknoloji ve dolandırıcılık tespit sistemlerine yaptığı yatırımların sonuç verdiğini göstererek kayıplarda **%5'lik bir düşüş** kaydetmiştir. Ancak, modern finansal suçların karmaşıklığı göz önüne alındığında, dolandırıcılıkla mücadelede ivmenin korunması için daha dikkatli olunması ve teknoloji odaklı çözümlere yatırım yapılmaya devam edilmesi gerekmektedir.

2011-2024 arası İngiltere'deki dolandırıcılık suçlarının sayısı.



Kaynak: statista.com

Avrupa Birliği

Avrupa Birliği, kara para aklama, terörün finansmanı ve diğer mali suçlarla mücadele için düzenleyici çerçevesini geliştirmek adına önemli adımlar atmıştır. 2024 yılı sonuna kadar, AB, finansal sisteminin bütünlüğünü koruma konusundaki kararlılığını yansıtan pek çok önemli düzenleyici tedbiri hayata geçirecektir.

Kara Para Aklama ile Mücadele Düzenlemelerinin Güçlendirilmesi

Avrupa Birliği'nin AML ve CFT konusundaki yaklaşımı, Altıncı Kara Para Aklamayı Önleme Direktifi'nin (6AMLD) kabulü ve AML için tek bir kural kitabının oluşturulmasıyla önemli ölçüde iyileşmiştir. Bu güncellemeler, bankalar, varlık yöneticileri ve kripto varlık hizmet sağlayıcıları (CASP'ler) dahil olmak üzere, AML yükümlülüklerini yerine getiren tüm kuruluşlar için müşteri kimliklerinin doğrulanması ve durum tespiti yapılmasına yönelik daha katı önlemler getirmektedir.

Dikkat çeken yeni gerekliliklerden biri, AML yükümlülüklerinin üst düzey profesyonel futbol kulüpleri nezdinde genişletilmesidir. 2024'ten itibaren, oyuncu transferleri ve sponsorluk anlaşmaları gibi önemli finansal işlemlere dahil olan müşterilerin kimliklerini doğrulamaları zorunlu hale gelecektir. Ayrıca, direktif, yüksek değerli işlemlerde sıklıkla istismar edilen boşlukları kapatmayı amaçlayarak ultra yüksek net değere sahip bireyler üzerinde daha fazla dikkat gerektirmektedir.

Bu düzenlemeler, üye devletlerde bu kuralların uygulanmasını denetleyecek olan Kara Para Aklamayla Mücadele Kurumu'nun (AMLA) kurulmasını da içeren daha geniş bir paketin parçasıdır. Bu düzenlemelerin tam olarak uygulanması için kesin tarihler henüz belirlenmemiş olsa da AMLA'nın 2029 yılına kadar faaliyete geçmesi ve AB genelinde AML standartlarının tutarlı bir şekilde uygulanmasını sağlaması beklenmektedir.

6AMLD'nin Temel Hükümleri

- **Kara Para Aklamanın Genişletilmiş Tanımı:** 6AMLD, kara para aklama tanımını daha geniş bir faaliyet ve yöntem yelpazesini kapsayacak şekilde genişletmektedir. Buna sadece yasa dışı fonları gizlemeye yönelik klasik yöntemler değil, aynı zamanda dijital ve finansal yeniliklerle ortaya çıkan yeni teknikler de dahildir. Direktif, bireyin katılım düzeyine bakılmaksızın, kara para aklama planlarına katılma eylemini açıkça suç haline getirmektedir.

- **Cezaların Uyumlaştırılması:** 6AMLD'nin en önemli yönlerinden biri de cezaların üye ülkeler arasında uyumlaştırılmasıdır. Direktif, üye devletlerin kara para aklamaya karışan kişi ve kuruluşlar için etkili, orantılı ve caydırıcı cezalar oluşturmasını zorunlu kılmaktadır. Bu şekilde, daha yumuşak yasal ortamlar arayan suçlular tarafından istismar edilebilecek yargı yetkisi tutarsızlıklarının önlenmesi amaçlanmaktadır.

- **İntifa Hakkı Sahipliğine Daha Fazla Odaklanma:** 6AMLD, gerçek hak sahiplerinin belirlenmesi ve doğrulanmasına daha güçlü bir vurgu yapmaktadır. Finansal kuruluşların, işlemlere dahil olan kuruluşların nihai olarak sahibi olan veya kontrol eden kişileri ortaya çıkarmak için kapsamlı bir durum tespiti yapmasını gerektirir. Bu önlem, yasa dışı fonların gerçek sahiplerini gizlemek için paravan şirketlerin ve diğer karmaşık yapıların kullanılmasıyla mücadele etmek için tasarlanmıştır.

- **Zorunlu AML Eğitimi:** Direktif, finansal kuruluşların ve belirlenmiş finansal olmayan işletmelerin çalışanları için düzenli AML eğitimi uygulamalarını zorunlu kılmaktadır. Bu, personelin şüpheli faaliyetleri tanımak ve bildirmek için iyi donanımlı olmasını sağlayarak AML önlemlerinin genel etkinliğini artırır.

- **Güçlendirilmiş İş birliği ve Bilgi Paylaşımı:** 6AMLD üye devletler, düzenleyici otoriteler ve finansal kuruluşlar arasında güçlendirilmiş işbirliği ve bilgi paylaşımını teşvik eder. Bu, sınır ötesi kara para aklama tehditlerine karşı daha koordineli bir müdahaleyi kolaylaştıran intifa hakkı sahipliği ve şüpheli faaliyetlerle ilgili bilgi alışverişini kapsamaktadır.

- **Yüksek Riskli Alanlara Daha Fazla Odaklanma:** Direktif, kara para aklama için giderek daha fazla istismar edilen sanal para birimleri ve ön ödemeli kartlar gibi yüksek riskli alanları özellikle hedef almaktadır. Finansal kuruluşların, ilgili riskleri azaltmak için bu sektörlerde gelişmiş durum tespiti tedbirleri uygulamaları gerekmektedir.

Uygulama ve Etki

6AMLD'nin uygulanması, üye devletlerin ulusal mevzuatlarını direktifin hükümleriyle uyumlu hale getirecek şekilde değiştirmelerini gerektirmektedir. AML çerçevelerinin güncellenmesi, uyum prosedürlerinin iyileştirilmesi ve uyumsuzluğa yönelik cezaların etkili ve caydırıcı olmasının sağlanması bu kapsamda yer almaktadır.

6AMLD'nin etkisinin derin olması beklenmektedir. Direktif, AB genelinde AML uygulamalarını ve cezalarını standartlaştırarak, ulusal düzenlemelerdeki tutarsızlıklardan yararlanma olasılığını azaltmayı amaçlamaktadır. İntifa hakkı sahipliği ve yüksek riskli alanlara daha fazla odaklanılması, finans kuruluşlarının kara para aklama faaliyetlerini tespit etme ve önleme konusunda daha donanımlı olmalarını sağlamaktadır.

Ayrıca, eğitim ve bilgi paylaşımına yapılan vurgu, AML'ye yönelik daha bilinçli ve iş birlikçi bir yaklaşımı teşvik etmektedir. Finansal kuruluşlar daha net kılavuz ilkelerden ve daha ortaklaşmış bir düzenleyici ortamdan faydalanacak, bu da uyumluluğun artmasına ve mali suçlara karşı daha güçlü bir savunma mekanizmasını mümkün kılacaktır.

Güçlü yönlerine rağmen, 6AMLD'nin uygulanması zorluklar içermektedir. Finansal kurumlar, özellikle Geliştirilmiş Durum Tespiti (EDD) ve personel eğitimi gibi alanlarda yeni gerekliliklere uyum sağlamada zorluklarla karşılaşabilir. Ayrıca, direktifin etkinliği, hükümlerinin üye ülkeler arasında tutarlı ve titiz bir şekilde uygulanmasına bağlıdır.

Kripto Varlıkların Düzenlenmesi

Avrupa Birliği, büyüyen kripto varlık piyasasıyla ilişkili riskleri ele almak için proaktif bir yaklaşım sergilemiştir. Avrupa Bankacılık Otoritesi (EBA), CASP'ler için kara para aklama ve terörün finansmanı ile ilgili riskleri tanımlayıp azaltmalarına yardımcı olmak amacıyla kapsamlı kılavuzlar yayımlamıştır. Bu kılavuzlar, CASP'lerin AML çabalarını etkili bir şekilde uyarlamak için müşteri profilleri, ürün teklifleri ve coğrafi operasyonlar gibi çeşitli risk faktörlerini dikkate almaları gerektiğini vurgulamaktadır.

Ayrıca, EBA, şeffaflık ve izlenebilirliği artırmak adına CASP'lerin ve ödeme hizmeti sağlayıcılarının kripto varlık transferlerinin kaynakları ve yararlanıcıları hakkında bilgi alışverişinde bulunmalarını zorunlu kılan “Seyahat Kuralı”nın uygulanmasına yönelik istişarelere başlamıştır.

Bu süreçle paralel olarak, Avrupa Menkul Kıymetler ve Piyasalar Otoritesi (ESMA), Kripto Varlık Piyasaları Yönetmeliği (MiCA) çerçevesinde CASP'ler için yetkilendirme sürecine dair ayrıntılı teknik standartlar yayımlamıştır. Bu standartlar, kripto varlık hizmetleri sunmak isteyen finansal kuruluşlar için gereklilikleri ve müşteri şikayetlerini ele alma prosedürlerini açıklığa kavuşturmaktadır. Bu tedbirlerin 2024 yılı sonuna kadar tam olarak uygulanması ve Avrupa'da daha düzenli ve güvenli bir kripto varlık piyasasına doğru önemli bir adım atılması beklenmektedir.

Finansal Piyasalarda Şeffaflık: MiFIR ve MiFID II

Avrupa Birliği, finansal piyasalarının bütünlüğünü güçlendirmek amacıyla Finansal Araç Piyasaları Yönetmeliği (MiFIR) ve Finansal Araç Piyasaları Direktifi'nde (MiFID II) önemli değişiklikler yapmıştır. Bu değişiklikler, piyasa verilerinin şeffaflığını artırmayı ve yatırımcıların bilinçli karar vermesi için gerekli olan konsolide piyasa verilerine erişimini sağlamayı hedeflemektedir. AB, bu düzenlemelerin güçlendirilmesiyle, tüm piyasa katılımcıları için eşit bir oyun alanı oluşturmayı ve sermaye piyasalarının küresel rekabet gücünü artırmayı amaçlamaktadır.

MiFIR ve MiFID II'de yapılan revizyonlar, finansal piyasaların hızlı dijitalleşmesi ve bu süreçle birlikte işlemlerin karmaşıklığının ve hacminin artması ışığında büyük bir öneme sahiptir. Geliştirilmiş şeffaflık önlemleri, yatırımcılara piyasa dinamikleri hakkında daha net bir görüş sunarak, piyasanın kötüye kullanılma riskini azaltmayı ve bu zorlukları etkili bir şekilde ele almayı hedeflemektedir.

Avrupa Dijital Kimliği ve AB Yapay Zeka Yasası

Avrupa Birliği, finansal düzenlemeler alanındaki çabalarının yanı sıra, Avrupa Dijital Kimlik (eID) çerçevesi ve AB Yapay Zeka (AI) Yasası'nın kabul edilmesiyle dijital alanda da önemli ilerlemeler kaydetmiştir. Tüm üye devletlerin 2026 yılına kadar vatandaşlarına dijital kimlik cüzdanı sağlamasını zorunlu kılan eID çerçevesi, Avrupa genelinde birleşik bir dijital kimlik sistemine doğru atılan önemli bir adımı temsil etmektedir. Bu dijital cüzdanlar, AB sakinlerine gelişmiş güvenlik özellikleriyle, ücretsiz e-imza ve işlem gösterge tabloları gibi araçlarla kamu ve özel hizmetlere hem çevrim içi hem de çevrim dışı erişim imkanı sunacaktır.

Artık bir yasa haline gelen AB Yapay Zeka Yasası, yapay zeka sistemlerini risk düzeylerine göre sınıflandırmakta ve buna uygun çeşitli uyum yükümlülükleri getirmektedir. Örneğin, “yüksek riskli” olarak tanımlanan AI sistemleri, sağlam veri yönetişimi, şeffaflık ve hesap verebilirlik gibi sıkı düzenleyici gerekliliklere tabi tutulmaktadır. Bu düzenleme, AB'nin AI teknolojilerinin etik ve Avrupa değerleriyle uyumlu bir şekilde geliştirilmesini ve kullanılmasını sağlamayı amaçlamakta, aynı zamanda AI'ın küresel yönetişiminde liderlik etme stratejisinin bir parçası olarak öne çıkmaktadır.

Zorluklar ve Gelecek Yönelimleri

Bu ilerlemelere rağmen, Avrupa Birliği, AML ve mali suç düzenlemelerini tam olarak uygulama ve yürürlüğe koyma konusunda devam eden zorluklarla karşı karşıyadır. Örneğin, Avrupa Komisyonu, bazı üye devletlerin, özellikle İrlanda, Fransa ve Letonya'nın 4AMLD ve 5AMLD'yi ulusal hukuklarına doğru bir şekilde aktarmadıkları için bu devletlere çağrıda bulunmuştur.

Ayrıca, Europol'ün Avrupa'daki mali ve ekonomik suçlara ilişkin tehdit değerlendirmesi, suç şebekelerinin artan karmaşıklığını ve organize suç ile yaptırımların delinmesi arasındaki yakınlaşmayı gözler önüne sermektedir. Rapor, suç şebekelerinin **yaklaşık %70'inin** temel kara para aklama tekniklerini kullandığını ortaya koyarak, teknolojideki ilerlemelere rağmen geleneksel yöntemlerin hâlâ yaygın olduğunu açıkça göstermektedir. Dahası, suçların **%80'i**, yasa dışı fonların gerçek kaynağını gizlemek için sıkça kullanılan paravan şirketler, karmaşık yapılar ve nakit yoğun işletmeler gibi yasal iş yapılarının kötüye kullanılmasını içermektedir. Raporda, bu suçların **%60'ının** bir tür yolsuzluk içerdiği vurgulanarak, yolsuzluk uygulamalarının mali suçları kolaylaştırmadaki etkisi ön plana çıkarılmaktadır.

Bu sorunları ele almak için AB'nin, özellikle siber suçlar ve yeni teknolojilerin kötüye kullanımı gibi yeni ortaya çıkan tehditlere odaklanarak düzenleyici çerçevesini geliştirmeye devam etmesi gerekecektir. Ayrıca, üye devletler ve AB kurumları arasında daha fazla koordinasyon sağlamak, düzenleyici tedbirlerin Birlik genelinde tutarlı bir şekilde uygulanmasını ve etkili bir biçimde yürütülmesini sağlamak açısından önem taşımaktadır.

AB, 2025'e girerken mali suçlarla mücadelede ve teknolojik düzenlemelerde küresel çabaların öncüsü olmayı hedefliyor. Son yıllarda alınan tedbirler, Birliğin mali sistemi ve vatandaşlarını finansal suçlardan koruma kararlılığını gösteriyor. Başarı, AB'nin uygulama zorluklarını aşma ve üye devletlerin düzenlemelere uyum sağlama yeteneğine bağlı olacak. Önümüzdeki birkaç yıl, AB'nin liderliğini sürdürüp sürdüremeyeceğini belirleyecek.

Suç şebekelerinin
yaklaşık %70'i
temel kara para aklama tekniklerini kullanıyor.

Orta Doğu ve Afrika

Kültürel çeşitlilik ve jeopolitik önem bakımından zengin olan Orta Doğu ve Afrika, karmaşık uluslararası ilişkilerini ve güvenlik sorunlarını yansıtan girift bir yaptırım ağıyla karşı karşıyadır. Orta Doğu'daki siyasi çıkar çatışmaları ve süregelen çatışmalar, yaptırımların hem diplomatik baskı aracı hem de yasa dışı faaliyetleri engelleme mekanizması olarak işlev gördüğü bir ortam yaratmıştır. Öte yandan, Afrika'nın farklı ekonomileri ve siyasi iklimleri, istikrarı teşvik ederken belirli tehditleri hedef alan yaptırımlara daha nüanslı bir yaklaşım gerektirmektedir. Jeopolitik gerilimlere ve bölgesel istikrara yönelik bu iki odaklanma, yaptırımların bu dinamik bölgelerin ekonomik ve siyasi yapısını şekillendirmedeki etkisini vurgulamaktadır.

Orta Doğu'nun GSYH'sının 2029 yılına kadar **4.55 milyar dolara** ulaşması beklenmektedir.

Ekonomik çeşitliliği ve karmaşık düzenleyici ortamıyla bilinen Orta Doğu, son yıllarda kayda değer bir ekonomik ilerleme kaydetmiştir. Bölgenin 2015 yılında 2.46 milyar dolar olan Gayri Safi Yurtiçi Hasılası (GSYH), 2024 yılında **3.57 milyar dolara** yükselmiştir. Uluslararası Para Fonu'na (IMF) göre, bu artış eğiliminin devam etmesi ve 2029 yılına kadar **4.55 milyar dolarlık** bir GSYH'ye ulaşılması beklenmektedir. Bu ekonomik genişlemeye, mali suçlarla mücadele ve şeffaflığı artırmayı amaçlayan önemli düzenleyici gelişmeler de eşlik etmektedir.

Birleşik Arap Emirlikleri (BAE)

Birleşik Arap Emirlikleri'nde finans sektörü, özellikle Mali Eylem Görev Gücü (FATF) tarafından 2022'de ülkedeki AML ve CTF önlemlerindeki stratejik eksiklikler nedeniyle "gri listeye" alınmasının ardından, küresel düzenleyici kurumlar tarafından yoğun bir incelemeye tabi tutulmuştur. Ancak BAE, bu endişelere hızlı ve etkili bir şekilde yanıt vererek, Şubat 2024 itibarıyla düzenleyici ortamını güçlendirmeyi amaçlayan kapsamlı reformların ardından FATF gri listesinden resmi olarak çıkarılmıştır. Bu hamle, finansal şeffaflığı artırmayı ve yasa dışı finansal faaliyetlerle mücadele etmeyi hedefleyen bir dizi düzenleyici iyileştirmenin ardından gelmiştir.

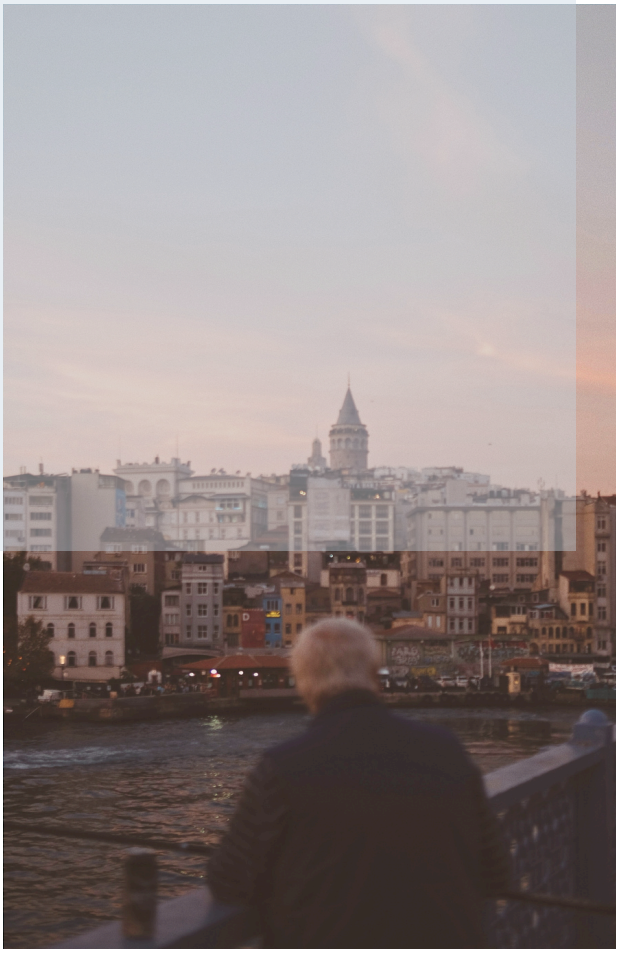
Ülkenin bu alandaki ilerlemesi, 41/2023 sayılı Muhasebe ve Denetim Hakkında Federal Kanun Hükmünde Kararname gibi reformlarla belirginleşmektedir. Bu yeni mevzuat, daha katı muhasebe standartları getirerek kurumsal yönetişim ve şeffaflığı güçlendirmeyi amaçlamakta ve finansal yanlış raporlama için daha sert cezalar içermektedir.

Finansal Hizmetler Düzenleme Kurumu (FSRA), sanal varlık sağlayıcılarına yönelik kılavuz ilkelerini FATF'ın Seyahat Kuralı ile uyumlu olacak şekilde güncelleyerek, gelişmiş müşteri durum tespiti ve işlem izleme gibi sıkı AML protokollerini zorunlu hale getirmiştir. Ayrıca, BAE Merkez Bankası (CBUAE) stabilcoinler için yeni bir düzenleyici çerçeve oluşturarak bunların tamamen BAE Dirhemleri ile desteklenmesini gerektirmiştir. Bu girişim, dijital para birimlerinin istikrarını artırmayı ve finansal riskleri azaltmayı hedeflemektedir. Genel Ticari Oyun Düzenleme Kurumu'nun (GCGRA) kurulması, BAE'nin düzenleyici denetime olan bağlılığını daha da pekiştirmiştir; bu kurum şu anda ülkenin ilk yetkili piyango operasyonunu denetlemektedir.

Türkiye

Türkiye, 2024 yılında düzenleyici ortamında özellikle kripto para sektöründe büyük bir revizyondan geçmiştir. Büyük Millet Meclisi, 2 Temmuz'da kripto varlık hizmet sağlayıcılarına lisans verilmesini zorunlu kılan kapsamlı bir yasayı kabul etmiştir. Türkiye'de yüksek düzeyde kripto para kullanımı göz önüne alındığında, bu yasa, hızla büyüyen piyasanın yapılandırılması ve küresel finansal düzenlemelere uyum sağlanması açısından son derece önemli bir adımdır.

Bu düzenleyici reform, Türkiye'nin Haziran ayında FATF Gri Listesi'nden çıkarılmasının ardındaki kilit faktörlerden biridir. Bu hamlenin, yatırımcı güvenini artırması ve ülkenin uluslararası finansal sisteme entegrasyonunu desteklemesi beklenmektedir.



İran

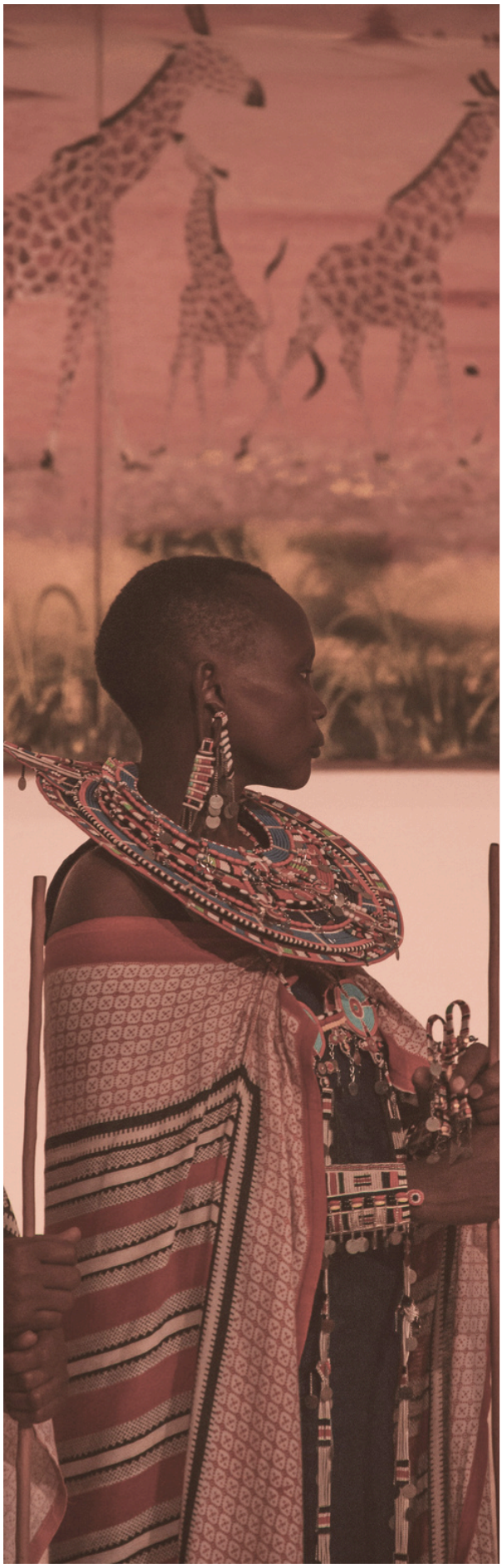
İran, ülkenin tartışmalı politikaları ve faaliyetleri nedeniyle uluslararası yaptırımların odak noktası olmaya devam ediyor. Ülke, 2024 yılı itibariyle 227 kişi ve 42 kuruluşu kapsayan geniş bir yaptırım rejimiyle karşı karşıya. Bu yaptırımlar mal varlıklarının dondurulmasını, seyahat yasaklarını, ticaret ve finansal işlemlere getirilen kısıtlamaları kapsamaktadır. AB'nin 15 Mart'ta uygulamaya koyduğu son yaptırımlar, insan hakları ihlallerine ve bölgesel istikrarsızlığa karışan kişi ve kurumları hedef almakta ve İran hükümetine bu kritik meseleleri ele alması için baskı yapmayı amaçlamaktadır. ABD de İran'ın petrol ve doğalgaz sektörünü hedef alan ve bu sektörün nükleer ve militan faaliyetleri desteklemeye yönelik mali kapasitesini sınırlamayı amaçlayan yeni tedbirler uygulamaya koymuştur.

Afrika

Afrika'nın 2024 yılındaki ekonomik görünümü, büyüme ve süregelen zorlukların bir sentezini yansıtmaktadır. Ekonomik genişlemeler ve bölgesel gelişmeler de dâhil olmak üzere kayda değer ilerlemelere rağmen kıta, mali suçlar ve yasa dışı faaliyetlerle ilgili önemli sorunlarla karşı karşıya kalmaya devam etmektedir. İnsan kaçakçılığı, özellikle Eritre, Güney Sudan ve Somali gibi ülkelerde önemli bir tehdit olmaya devam etmektedir. Bu bölgeler süregelen çatışma ve istikrarsızlıklarla boğuşmakta ve savunmasız nüfusları korumak için daha güçlü bölgesel iş birliği ve yasal çerçevelere duyulan ihtiyacın sinyallerini vermektedir.

Yasa dışı madencilik ve yaban hayatı kaçakçılığı da Afrika genelinde dikkat çeken sorunlar arasında yer almaktadır. Demokratik Kongo Cumhuriyeti (DRC), ekonomik istikrarı tehdit eden ve çevresel bozulmaya yol açan altın kaçakçılığı ve düzensiz madencilikle mücadele etmektedir. Orta Afrika'daki patlayıcı balıkçılık gibi yasa dışı faaliyetlerde patlayıcı öncüsü kimyasalların kullanılması, çevresel zararı daha da artırmakta ve mali suçları ele alma çabalarını zorlaştırmaktadır.

Afrika'daki AML ve CTF çabaları, önemli bölgesel istikrarsızlık, zayıf yönetişim ve sosyo-ekonomik eşitsizliklerle şekillenmiştir. Bu faktörler, kara para aklama, terör finansmanı ve insan kaçakçılığı gibi mali suçlar için verimli bir zemin oluşturmaktadır. Afrika, insan kaçakçılığı, silah kaçakçılığı, yaban hayatı kaçakçılığı ve altın kaçakçılığı gibi faaliyetler nedeniyle yılda tahmini **60 milyar dolar** kaybetmektedir. Kıtanın geniş doğal kaynakları ve zayıf düzenleyici ortamları, bölgeyi suç şebekeleri için cazip bir hedef haline getirmektedir.



Batı Afrika ve Sahel, terörist gruplar tarafından daha da kötüleştirilen güvenlik koşulları nedeniyle özellikle sorunludur. Bu gruplar, patlayıcı ve silah kaçakçılığı gibi yasa dışı faaliyetlerde bulunarak bölgeyi daha da istikrarsızlaştırmaktadır. Orta Afrika'da ise, DRC ve Orta Afrika Cumhuriyeti gibi ülkeler yasa dışı madencilik faaliyetleri ve değerli metallerin kaçakçılığı ile mücadele etmektedir. Bu faaliyetler, sıklıkla silahlı çatışmalarla ilişkilidir ve elde edilen gelirler, isyancı grupları ve terör örgütlerini finanse etmek için kullanılmaktadır.

Bu zorlukların ortasında, düzenleyici çerçeveleri ve uygulama kabiliyetlerini geliştirme çabaları devam etmektedir. Güney Afrika, yaban hayatı kaçakçılığı ve altın kaçakçılığına odaklanarak mali suçlarla mücadele için önemli adımlar atmıştır. 2023 yılında, önemli bir yasa dışı finans kaynağı olan yaban hayatı kaçakçılığıyla başa çıkmak amacıyla ABD ile iş birliği içinde bir görev gücü oluşturmuştur. Ülke, aynı zamanda suç çeteleri tarafından kara para aklamak ve yaptırımlardan kaçmak için kullanılan altın kaçakçılığı operasyonlarına yönelik baskılarını artırmaktadır.

Nijerya, mobil, bilgisayar ve satış noktası dolandırıcılığı gibi dijital dolandırıcılıklarda bir artış yaşamaktadır. Hükümet, siber destekli mali suçların artan tehdidiyle mücadele etmek için düzenleyici ve teknolojik önlemleri güçlendirerek karşılık vermektedir.

Afrika'nın mali suçlarla mücadelesinde uluslararası işbirliği büyük önem taşımaktadır. Avrupa Birliği ve diğer küresel güçler, başta terör finansmanı ve organize suçlarla bağlantılı olanlar olmak üzere, istikrarı bozucu faaliyetlere karışan kuruluş ve bireylere yaptırımlar uygulamaya devam etmektedir.

Asya Pasifik

Çin

Çin'in 2024'teki düzenleyici ortamı, AML önlemlerini güçlendirmeye ve mali suçlarla mücadeleye yönelik önemli ilerlemelere sahne oldu. Bu yılın en dikkat çekici gelişmelerinden biri, uluslararası bağlantıları olan kara para aklama şebekelerine karşı devam eden baskılardı. Haziran 2024'te ABD'li yetkililer, Meksikalı uyuşturucu kartelleri için **50 milyon doların üzerinde** para aklamaya karışan 24 kişiyi tutukladı. Bu operasyonlar, Çin'in sermaye kontrollerini istismar ederek vatandaşların her takvim yılı başına yurtdışına **50.000 dolardan fazla** para göndermesine yönelik sınırlamalar getirmekte ve bu durum, kartellerin yararlandığı yeraltı finans ağlarına olan talebi artırmaktadır.

Ayrıca, Çin, yerel Kara Para Aklamayı Önleme Yasası'nda (AMLL) önemli bir değişiklik yaparak AML düzenlemelerinin kapsamını genişletti. Tam olarak 2024 yılı sonunda yürürlüğe girmesi beklenen güncellenmiş yasa, finansal kuruluşlara ve gayrimenkul ile değerli metaller sektörleri de dahil olmak üzere finansal olmayan kuruluşlara yeni uyum gereklilikleri getirmektedir. Bu düzenlemenin temel hükümleri arasında daha sıkı müşteri durum tespiti, gelişmiş risk yönetimi sistemleri ve düzenleyici makamlara zorunlu hak sahipliği bildirimi bulunmaktadır.

Gerçek Sahiplik Bilgileri için İdari Tedbirler, şeffaflığı daha da güçlendirmek amacıyla Kasım 2024'te yürürlüğe girecektir. Çin Halk Bankası (PBOC) ve Devlet Piyasa Düzenleme İdaresi (SAMR) tarafından yayınlanan bu düzenlemeler, şirketlerin, ortaklıkların ve yabancı şubelerin sahiplik ayrıntılarını bildirmelerini zorunlu kılmaktadır. Yeni kurallar, özellikle yabancı kuruluşlar tarafından nihai mülkiyetin gizlenmesini hedef almakta ve karmaşık kurumsal yapılar aracılığıyla kara para aklamayı engellemeye yönelik olarak tasarlanmıştır.

Bu gelişmelere ek olarak, Çin çevrim içi oyun ve dijital varlıklara da özel bir ilgi göstermektedir. 22 Aralık 2023 tarihinde “Çevrim içi Oyunların Yönetimine İlişkin Tedbirler” kamuoyuna sunulmuştur. Bu önlemler, çevrim içi oyun endüstrisinin “refahını ve sağlıklı gelişimini” sağlamayı ve teşvik etmeyi amaçlamaktadır. Temel hükümleri, küçüklerin ve savunmasız oyuncuların korunmasına güçlü bir vurgu yaparak, teknik ekipman gereksinimlerini ve kısıtlamaları içermektedir. Bu düzenlemeler, Çin'deki çevrim içi oyun sağlayıcılarını doğrudan etkileyecektir.

20 Şubat 2024 tarihinde, Hong Kong Para Otoritesi (HKMA), Yetkili Kurumlar Tarafından Dijital Varlıklar için Saklama Hizmetlerinin Sağlanmasına İlişkin

Beklenen Standartlar hakkında bir kılavuz yayınladı. Bu kılavuz, risk değerlendirmesi, AML/CFT uyumluluğu, ifşa, kayıt tutma ve müşteri varlıklarının korunmasına yönelik hükümler içermektedir. Aracı olarak sanal varlıklarla ilgili faaliyetlerde bulunan, tokenize edilmiş ürünleri dağıtan veya bağımsız saklama hizmetleri sunan yetkili kurumlar bu düzenlemeden etkilenmektedir.

1 Haziran 2024'ten itibaren, Hong Kong'da faaliyet gösteren tüm sanal varlık alım satım platformlarının, Menkul Kıymetler ve Vadeli İşlemler Komisyonu (SFC) tarafından lisanslanması veya Kara Para Aklama ve Terörle Mücadele Finansmanı Yönetmeliği (AMLO) kapsamında "lisanslı sayılan" VATP başvuru sahipleri olması gerekmektedir. Bu düzenleme, Hong Kong'daki tüm VATP'leri kapsamaktadır.

Ayrıca, 2021'den bu yana kripto para ticaretinin yasak olmasına rağmen, Çin'de yasa dışı kripto faaliyetleri devam etmektedir. Mayıs 2024'te, Çin vatandaşları yaklaşık 90 milyar dolarlık kripto para ticareti gerçekleştirerek yaptırım çabalarının yenilenmesine yol açmıştır. Yasa dışı sanal para birimi işlemlerinin engellenmesi, özellikle sınır ötesi mali suçlarda kripto kullanımının artması nedeniyle düzenleyiciler için önemli bir öncelik olmaya devam etmektedir.

İleriye dönük olarak, Çin'in 2024'teki düzenleyici sıkılaştırması, uluslararası AML standartlarına uyum sağlama ve finansal gözetimi güçlendirme niyetini yansıtmaktadır. PBOC ve diğer düzenleyici kurumlar tarafından yönlendirilen bu reformlar, Çin'in hem yurt içinde hem de uluslararası işbirliği yoluyla mali suçlarla mücadele konusundaki kararlılığını göstermektedir.

Singapur

Haziran 2024'te Singapur, gelişen mali suç tehditleri ışığında kara para aklama çerçevesini güçlendirmeyi amaçlayan önemli bir gelişme olarak güncellenmiş Kara Para Aklama Ulusal Risk Değerlendirmesi'ni (ML NRA) açıkladı. Bu güncellenmiş değerlendirme, Şüpheli İşlem Raporlama Ofisi'nden (STRO) alınan verileri ve hem yerel hem de uluslararası paydaşlardan gelen geri bildirimleri entegre etmektedir. Singapur'un ekonomik açıklığı ve gelişmiş mali altyapısı, suçlular tarafından yasa dışı fonları aklamak için kullanıldığı bir uluslararası finans merkezi ve ticaret merkezi olarak rolünün yarattığı zorlukları ortaya koymaktadır.

Güncellenmiş ML NRA, Singapur'un başlıca kara para aklama tehditlerinin siber destekli dolandırıcılık, yabancı suçlar, organize suçlar, yolsuzluk, vergi suçları ve ticarete dayalı kara para aklama olduğunu vurgulamaktadır. Değerlendirme, yerli ve yabancı siber destekli dolandırıcılığın, sofistike suç örgütleri tarafından yönlendirilen önemli bir risk olmaya devam ettiğini göstermektedir. Ayrıca, yasa dışı fonların Singapur'un bankacılık sistemine akışı, paravan şirketler gibi tüzel kişilerin kötüye kullanımı ve yasa dışı fonların gayrimenkul ve değerli metaller gibi yüksek değerli varlıklara yerleştirilmesi gibi temel kara para aklama tipolojileri tanımlanmaktadır.

Belirlenen bu tehditlere yanıt olarak, Singapur'un düzenleyici ortamı önemli ölçüde revize edilmiştir. 1 Nisan 2024'te Singapur Para Otoritesi (MAS), finansal kurumlar arasında müşteri bilgilerinin güvenli paylaşımını geliştirmek için tasarlanmış merkezi bir dijital araç olan COSMIC platformunu başlattı. Altı büyük banka ile iş birliği içinde geliştirilen bu platform, kurumların şüpheli faaliyetler hakkında veri alışverişinde bulunmasına olanak tanıyarak risk değerlendirmelerinin isabet oranını önemli ölçüde artırmaktadır. Bu girişim, MAS'ın AML ve CFT önlemlerini güçlendirmeye yönelik daha geniş kapsamlı çabalarının bir parçasıdır.

Ayrıca, 2 Nisan 2024'te MAS, Ödeme Hizmetleri Yasası'nda (PSA) 4 Nisan 2024 tarihinden itibaren aşamalı olarak yürürlüğe girecek değişiklikleri duyurdu. Bu değişiklikler, en son FATF standartlarıyla uyumlu olarak, dijital ödeme belirteci (DPT) hizmet sağlayıcılarını da içerecek şekilde düzenleyici kapsamı genişletmektedir. Revize edilen PSA, artık DPT'ler için saklama hizmetleri, DPT iletimlerinin kolaylaştırılması ve sınır ötesi para transferleri gibi faaliyetleri kapsamaktadır.

Bu düzenleyici güncellemelerin yanı sıra, Singapur'un uygulama çabaları da önemli olmuştur. MAS, Ocak 2022'den Haziran 2023'e kadar, 2019'da MAS İcra Raporlarının başlatılmasından bu yana en yüksek olan **7,88 milyon dolarlık** mali para cezaları ve kompozisyonlar dahil olmak üzere toplamda **12,96 milyon dolarlık** sivil ceza uygulamıştır. Bu cezaların **7,10 milyon doları**, özellikle AML ve CFT gerekliliklerinin ihlaliyle ilgilidir.

Jeopolitik Türbülans

Jeopolitik Türbülans:
Küresel Gerilimler Mali Suçları Nasıl Şekillendiriyor?

Yaptırımlar ve Dalga Etkileri

Yaptırımlar, ülkelerin dış politika hedefleri doğrultusunda başkaları üzerinde ekonomik baskı uygulamak için kullandıkları modern jeopolitik ortamın en önemli araçlarından biri haline gelmiştir. Bu önlemlerin kapsamı, ölçeği ve sonuçları son yıllarda, özellikle daha hedefli ve geniş kapsamlı stratejilere olanak tanıyan karmaşık finansal sistemlerin ortaya çıkmasıyla birlikte önemli ölçüde artmıştır.

Bu eğilim, Şubat 2022'de başlayan Rusya ve Ukrayna örneğindeki gibi küresel gerilimler ile daha da hız kazanmıştır. Ekonomik baskı unsurları, hedef alınan ülkelerin kabiliyetlerini zayıflatmak için tasarlanmış olsa da genellikle hedeflenen sınırların çok ötesine geçen geniş çaplı etkiler yaratarak ekonomik, siyasi ve insani sonuçlar doğurmaktadır.

Rusya-Ukrayna'daki duruma verilen küresel tepki, modern tarihin en büyük ve kapsamlı ekonomik yaptırım kullanımına işaret etmektedir. Şubat 2022'den bu yana, Amerika Birleşik Devletleri, Avrupa Birliği, Birleşik Krallık ve Kanada gibi Batılı ülkelerden oluşan bir koalisyon tarafından Rusya'ya **16.500'den fazla** yaptırım uygulamıştır. Bu uygulamalar, Rus ekonomisinin enerji, finans ve savunma gibi kilit sektörlerini hedef alırken, oligarklar ve Kremlin'e yakın isimleri de içererek, Devlet Başkanı Vladimir Putin'in rejimini destekleyen mali ağları çözmeyi amaçlamıştır.

Bu baskıların önemli bir bölümü, Rusya'nın yaklaşık 350 milyar dolarlık döviz rezervlerinin dondurulmasını kapsamaktadır. Bu durum, ülkenin ekonomisini istikrara kavuşturma ve savaş çabalarını finanse etme kapasitesini önemli ölçüde sınırlandırmıştır. Ek olarak, Batılı ülkeler Rus bankalarının varlıklarının %70'ini dondurmuş, birçok bankayı uluslararası SWIFT sisteminden çıkarmış ve silah üretimi için hayati öneme sahip teknolojilere sıkı ihracat kontrolleri getirmiştir. Mali kısıtlamalara ek olarak, G7, Rusya'nın enerji ihracatından elde edeceği geliri sınırlandırmak amacıyla petrolüne varil başına 60 dolarlık bir fiyat tavanı uygulamaya koymuştur.

Bu kapsamlı önlemlere rağmen, yaptırımların etkinliği hala tartışmalı bir konudur. Uluslararası Para Fonu'na (IMF) göre, 2022 yılında Rus ekonomisi **%2,1** oranında küçülmüştür. Ancak, beklenen çöküşün aksine, Rusya ekonomisi 2023 yılında **%2,2** oranında büyüme kaydederek dirençli olduğunu göstermiş ve 2024 için **%1,1'lik** bir büyüme öngörülmektedir. Bu dayanıklılık, Rusya'nın özellikle Çin ve Hindistan ile ticari ilişkilerini yeniden düzenlemesinden kaynaklanmaktadır. Çin ve Hindistan, Rus petrol ve doğalgaz ithalatını önemli ölçüde arttırmış; Hindistan, Rus ham petrolünün başlıca alıcısı olurken, Çin de Batılı tedarikçilerin boşluğunu doldurmak için teknoloji ve mallar sağlamıştır.

Yaptırımların karmaşık etkilerinin arkasındaki temel nedenlerden biri, yaptırım uygulanan ülkelerin genellikle bu kısıtlamaları aşmanın yollarını bulabilmesidir. Örneğin Rusya, petrolünü fiyat sınırının üzerinde ihraç etmek için tankerlerden oluşan bir "gölge filo" kullanmış ve Kazakistan, Kırgızistan ile Belarus gibi ülkeler aracı olarak görev yaparak yaptırım uygulanan malların Rusya'ya kaçırılmasını sağlamıştır. Bu tür geçici çözümler, yaptırımların uygulanmasındaki zorlukları gözler önüne sermektedir: Küreselleşmiş tedarik zincirleri, alternatif rotaların ve kaçakçılık ağlarının gelişmesine olanak tanımakta ve mal ile hizmetler, daha pahalı ve verimsiz yollarla da olsa hedef ülkeye ulaşmaya devam etmektedir.

Komşu ülkeye yaptırımlar, bölgedeki ticareti **ortalama %9 azaltıyor**

Yaptırımların ana amacı, hedef ülkelerin yönetimleri üzerinde baskı kurmak olsa da, genellikle komşu ülkeler üzerinde istenmeyen yan etkiler yaratmaktadır. 1989-2015 yılları arasında uygulanan yaptırımları inceleyen bir araştırma, komşu bir ülkeye yönelik yaptırımların, komşu ülkelerdeki ticareti ortalama **%9** oranında azalttığını ortaya koymuştur. Bunun temel nedenleri arasında ticaret yollarındaki kesintiler, artan nakliye maliyetleri ve önemli ticaret ortaklarının kaybedilmesi yer almaktadır.

Örneğin, 1990 yılında Kuveyt'i işgal etmesinin ardından Irak'a uygulanan yaptırımlar, aralarında Ürdün ve Türkiye'nin de bulunduğu 21 komşu ülke için ekonomik zorluklar yaratmıştır.

Ancak bazı durumlarda komşu ülkeler, yaptırımların ekonomik etkilerinden kazanç elde etmiştir. Örneğin, 1987'de Haiti'ye yaptırım uygulandığında, Dominik Cumhuriyeti'nin ithalat ticareti önemli ölçüde artmış; bu durum, sınır ötesi kaçakçılık ve ticaret akışlarının yeni yönlere kaymasıyla açıklanmıştır.

Benzer biçimde, 1992'de Somali'ye yaptırım uygulandığında Kenya'nın ticaret hacmi genişlemiştir. Bu örnekler, yaptırımların yalnızca hedef ülkeyi değil, komşu ülkelerde beklenmedik ekonomik fırsatlara da zemin hazırlayabileceğini göstermektedir. Rusya örneğinde ise, yaptırımlardan kaçınmak isteyen Rus şirketlerinin üretim tesislerini Kazakistan'a taşıması, bu ülkenin ticaretinde kayda değer bir artışa neden olmuştur.

Yaptırımların kapsamlı uygulanması, ekonomik sonuçların ötesinde ciddi insani riskler doğurabilir. Bir ülkenin ekonomik izolasyonu, gıda, ilaç ve enerji gibi temel ihtiyaçlarda kıtlığa yol açabilir; aşırı durumlarda ise sağlık koşullarının kötüleşmesi, ölüm oranlarının artması ve yönetim sistemlerinin istikrarsızlaşması gibi olumsuz etkiler ortaya çıkabilir. Örneğin, İran, Venezuela ve Küba'ya uygulanan yaptırımlar, bu ülkelerde sivil nüfusun yaşam koşullarını ağırlaştırmış ve halkın rejimlere karşı tepkisini artırmak yerine, rejimlere desteğin pekişmesine neden olmuştur. Bu tür durumlarda, hükümetler yaptırımları halkına karşı yabancı güçlerin bir zulmü olarak sunarak iktidarlarını güçlendirme yoluna gidebilir.

Günümüzde yaptırımların etkisi, ekonomik alanın ötesinde, teknolojik ve stratejik rekabet alanlarında da kendini göstermektedir. Örneğin, ABD'nin Çin'in yarı iletken teknolojisine erişimini kısıtlaması, Çin'in askeri ve ekonomik alandaki gelişimini yavaşlatmayı amaçlamaktadır. Ancak bu tür kısıtlamalar, hedef ülkeyi kendi üretim kapasitelerini geliştirmeye veya alternatif tedarik kaynakları bulmaya zorlayarak istenmeyen sonuçlar doğurabilir. Nitekim, Rusya ve Çin'in stratejik sektörlerde kendi kendine yeterliliğini artırmaya yönelik çabaları, bu sürecin dikkat çekici örneklerindendir.

Yaptırımların etkisi yalnızca ekonomik sonuçlarla sınırlı kalmaz; küresel ittifakları ve ticaret modellerini de köklü şekilde değiştirebilir. Rusya-Ukrayna gerilimi sonrası uygulanan yaptırımlar, Avrupa'nın Rus enerji kaynaklarına olan bağımlılığını hızla azaltmıştır. Savaş öncesinde doğal gaz ihtiyacının %40'ını Rusya'dan karşılayan Avrupa, yaptırımlar sonrasında enerji kaynaklarını çeşitlendirerek yenilenebilir enerji ve sıvılaştırılmış doğal gaz (LNG) gibi alternatif kaynaklara yönelmiştir. Bu değişimin, küresel enerji piyasaları üzerinde uzun vadeli etkiler yaratması ve Rusya'nın enerji piyasasındaki payını azaltarak alternatif enerji kaynaklarına yatırımları artırması beklenmektedir.

Öte yandan, yaptırımlar uygulandıkları ülkelerde hedeflerine ulaşsalar dahi uzun vadeli hale gelebilir. Bu süreçte, yaptırımları uygulayan ülkelerdeki yerel çıkar gruplarının etkisi büyüktür. Örneğin, ABD'nin Küba'ya yönelik ambargosu, ABD'li şeker üreticilerinin Küba şekeriyle rekabetten kaçınma isteği nedeniyle yıllardır devam etmektedir. Bu tür yerel çıkarlar, değişen jeopolitik hedeflere rağmen yaptırımların devam etmesi için siyasi desteğin sürmesine yol açmaktadır.

Geleceğe baktığımızda, yaptırımların uluslararası krizlerde dış politikanın önemli bir aracı olmaya devam etmesi muhtemeldir. Özellikle bölgesel saldırganlık, insan hakları ihlalleri ve nükleer silahların yayılması gibi küresel tehditlerin ele alınmasında yaptırımlar ön plana çıkacaktır. Rusya'ya uygulanan yaptırımlar, bu stratejinin hem etkili olma potansiyelini hem de sınırlarını açıkça göstermiştir. Yaptırımlar Rusya'nın ekonomisine ciddi zararlar vermiş ve kritik kaynaklara erişimini kısıtlamıştır. Ancak istenilen siyasi değişim sağlanamamış ve komşu ülkeler ile küresel piyasalarda istenmeyen sonuçlar ortaya çıkmıştır.

Yaptırımların gelecekteki kullanımı, politika yapıcıların yalnızca kısa vadeli etkilerini değil, küresel ticaret, ekonomik istikrar ve insani koşullar üzerindeki uzun vadeli sonuçlarını da titizlikle değerlendirmelerini gerektirecektir. Yaptırımlar daha fazla tercih edilen bir jeopolitik baskı aracı haline geldikçe, yaptırımların delinmesini engellemek ve istenmeyen etkileri hafifletmek için daha gelişmiş uygulama mekanizmalarına ihtiyaç olacaktır. Ayrıca, yaptırımların geniş çaplı ekonomik ve insani etkilerinin farkında olunması, stratejik hedeflere ulaşırken ikincil zararları en aza indiren daha hedefe yönelik politikaların oluşturulmasına yardımcı olabilir. Bu yaklaşımlar, yaptırımların uluslararası krizlerde daha etkili bir araç olmasını sağlayabilir.

> 2024’te Rusya-Ukrayna anlaşmazlığı ve Orta Doğu’daki çatışmalar gibi jeopolitik gerilimler, finansal suç trendlerini etkilemiştir. Yaptırımlar, suçluları kripto paralar, DeFi ve paravan şirketlerle kara para aklamada yeni yöntemler geliştirmeye itmiştir. Ticaret yoluyla kara para aklama, yaptırımları aşmak için daha karmaşık sınır ötesi işlemlerle yapılmaktadır. Terörizmin finansmanı da artmış, küresel finans sistemleri çatışma bölgelerindeki faaliyetlerin desteklenmesinde kullanılmaktadır. Bu trendlere karşı finansal kuruluşlar, PEP'ler, sınır ötesi ödemeler ve muhabir banka ilişkilerinde kontrollerini güçlendirmektedir.
>
> 
> **Vivek Mishra**
> AML/KYC Professional

Sınır Ötesi Suçlar

Mevcut jeopolitik ortamda sınır ötesi suç, uluslararası ilişkilerdeki gerginlikler ve ekonomik belirsizliklerle daha karmaşık bir hale gelmiştir. Jeopolitik gerilimler ve çatışmalar, sınır ötesi suçların yayılmasına elverişli bir zemin sunarken, bu suçlarla mücadele için ülkelerin daha sofistike ve iş birliğine dayalı stratejilere ihtiyaç duyduğu bir gerçek haline gelmiştir.

Siyasi istikrarsızlık, ekonomik yaptırımlar ve diplomatik kopukluklar, düzenleyici yapıları zayıflatabilir ve kolluk kuvvetlerinin etkinliğini azaltabilir. Bu durum suç şebekelerinin ortaya çıkan boşluklardan faydalanmasına olanak tanır. Örneğin, Ukrayna'daki savaş gibi çatışmalar, insan kaçakçılığı ve diğer yasa dışı faaliyetlerde belirgin bir artışa neden olmuştur. 2023 yılı itibarıyla sınır ötesi suç faaliyetlerinde **%35'lik bir artış** gözlemlenmiş ve özellikle Doğu Avrupa ile Orta Doğu gibi çatışma bölgeleri, suç örgütlerinin operasyonları için merkezler haline gelmiştir.

Rusya'ya uygulanan ekonomik yaptırımlar, geleneksel finansal sistemleri zayıflatmış ve bu boşluklar, suç örgütlerinin düzenlenmemiş alternatif finansal araçları kullanmasına neden olmuştur. Özellikle kripto para birimleri gibi düzenlemeye tabi olmayan finansal kanallar, yasa dışı finansal akışların artmasına katkı sağlamış, bu da küresel finans sistemlerine ek zorluklar yaratmıştır. Bu süreçte, yasa dışı finansal faaliyetlerde %25 oranında artış gözlemlenmiştir, bu da jeopolitik gerilimlerin ve ekonomik yaptırımların suç faaliyetleri üzerinde nasıl etkili olduğunu göstermektedir.

Sınır Ötesi Suçlarla Mücadelede Yeni Zorluklar

Jeopolitik çalkantıların ve sınır ötesi suçların bir araya gelmesi birkaç temel zorluk ortaya çıkarmaktadır:

Yetki Alanı ve Yasal Karmaşıklıklar

Ülkeler arasında farklı yasal çerçeveler ve uygulama pratikleri, suçluların tespit edilmekten kaçınması için fırsatlar yaratmaktadır. Veri gizliliği yasaları ve soruşturma tekniklerindeki farklılıklar siber suçlular tarafından istismar edilmekte ve sınır ötesi saldırılarla mücadeleyi zorlaştırmaktadır

Teknolojik Gelişmeler

Suç örgütleri, sınır ötesi suçları kolaylaştırmak için şifreleme ve blockchain gibi gelişmiş teknolojileri giderek daha fazla kullanmaktadır. 2021 yılındaki kripto para çöküşüne rağmen, kripto ile ilgili suçlar 2022 yılında sabit kalmıştır. Veriler, saadet zincirlerinde **7,8 milyar dolar**, darknet piyasalarında **1,5 milyar dolar** harcandığını ve hack'ler yoluyla **3,7 milyar dolar** çalındığını gösteriyor. Bitcoin hakimiyetinden çok zincirli bir gerçekliğe geçiş, suçluların yasa dışı fonları gizlemek için zincirler arası köprülerden ve zincir atlamadan yararlanmasına olanak sağlamıştır.

Uluslararası İş Birliği ve Kaynak Kısıtlamaları

Jeopolitik gerilimler uluslararası işbirliğini zorlayarak ortak soruşturmaları ve bilgi paylaşımını engelleyebilir. Çatışan ulusal çıkarlar ve diplomatik anlaşmazlıklar çoğu zaman müdahaleleri geciktirmekte ve koordineli suçla mücadele çabalarını baltalamaktadır.

Yenilikçi Çözümler ve Yanıtlar

Bu zorluklara yanıt olarak, çeşitli yenilikçi çözümler ve uluslararası girişimler ortaya çıkmaktadır:

> Kolluk Kuvvetlerinde Teknolojik Gelişmeler: Kolluk kuvvetleri, sınır ötesi suçları takip etmek ve engellemek için yapay zeka ve makine öğrenimi gibi ileri teknolojileri benimsemektedir. Europol tarafından yapay zeka odaklı araçların kullanılması, yasa dışı faaliyetlerin başarılı bir şekilde durdurulmasında artışa yol açmıştır.

> Gelişmiş Uluslararası İşbirliği: Sınır Ötesi Suçlara Karşı Küresel İttifak gibi yeni uluslararası koalisyonlar koordinasyon ve bilgi paylaşımını geliştirmektedir. Bu koalisyon, büyük kaçakçılık şebekelerinin çökertilmesi ve önde gelen suçluların tutuklanması da dahil olmak üzere birçok ortak operasyonu kolaylaştırmıştır.

> Düzenleyici Yenilikler: Dijital para birimlerinin yükselişini ele almak için düzenleyici kurumlar güncellenmiş çerçeveler uygulamaktadır. FATF, gelişmiş AML önlemlerini ve daha sıkı KYC gerekliliklerini vurgulayarak kripto para birimi işlemleri için yeni yönergeler getirmiştir.

> İnsani Yardım ve Destek Girişimleri: Uluslararası Göç Örgütü (IOM) gibi kuruluşlar sınır ötesi suçların insani etkilerine odaklanmaktadır. IOM, 2023 yılında mağdurlara yardım programlarını genişleterek dünya genelinde +18.000 mağdura destek sağlamıştır.

2024 ve sonrası için, sınır ötesi suç ortamı, başta siyaset olmak üzere beklenmedik küresel olaylara paralel olarak gelişmeye devam edecektir. Bu zorluklarla başa çıkabilmek için yeni teknoloji, gelişmiş uluslararası işbirliği ve sağlam düzenlemeleri bir araya getiren kapsamlı bir yaklaşım gerekmektedir.

Küresel Gerilimlerin Uyumluluk Üzerindeki Etkisi

Son 20 yılda insanların iletişim biçimleri büyük ölçüde değişmiş; bu dönüşüm, uluslararası ilişkilerde de etkisini göstermiştir. Ülkeler, sınır ötesi suçlarla ve giderek karmaşıklaşan finansal düzenlemelerle başa çıkma gerekliliğiyle karşı karşıya kalmıştır.

Bunlardan biri, giderek daha fazla ülkenin enternasyonal arenada ticaret yapmalarının yasaklanmasıdır. Bu tür ticari kısıtlamalar, uluslararası alanda faaliyet gösteren şirketler için ciddi zorluklar yaratmaktadır. Rusya başta olmak üzere bazı ülkeler, devam eden jeopolitik çatışmalar nedeniyle bu tür kısıtlamalarla karşı karşıya kalmış, bu da bu ülkelerle ticaret yapan şirketlerin işlemlerini yönetmelerini, para transferi yapmalarını ve varlıklarını kontrol etmelerini zorlaştırmıştır.

Bu ticaret kısıtlamalarının etkisi, yalnızca yaptırım uygulanan ülkelerle sınırlı kalmayıp küresel finans piyasalarını da etkilemektedir. Özellikle finans kuruluşları, bu yaptırımlara uyduklarından emin olmak için büyük bir baskı altındadır. Uyumsuzluk durumunda karşılaşacakları ciddi cezalar, kurumları uyumluluğa daha fazla odaklanmaya ve iç kontrollerini güçlendirmeye itmiştir. Düzenleyiciler de artan küresel gerilimlerin bir sonucu olarak mali suçlarla mücadele çabalarını yoğunlaştırmış, özellikle kara para aklama ve terörizmin finansmanı gibi konulara daha fazla dikkat çekmiştir. Yaptırım uygulanan bölgelerle yapılan sınır ötesi finansal akışlar, yoğun incelemeye tabi tutulmuş ve bu tür işlemler üzerindeki düzenleyici baskı artmıştır.

Alternatif finansal sistemlerin ve dijital para birimlerinin ortaya çıkması, bu uyumluluk zorluklarını daha da derinleştirmiştir. Kripto para gibi düzenlenmemiş finansal kanallar, suç örgütleri tarafından yasa dışı finansal faaliyetler için kullanılmış ve bu durum, kripto para işlemlerinin daha yakından izlenmesini zorunlu hale getirmiştir. Özellikle, yaptırım altındaki bölgelerden kaynaklanan yasa dışı finansal akışlarda **%25 oranında** bir artış görülmüş, bu da jeopolitik gerilimlerin küresel finansal sistem üzerindeki baskısını gözler önüne sermiştir.

Düzenleyiciler, dijital varlıkların kötüye kullanılmasını önlemek için daha kapsamlı raporlama yükümlülükleri içeren yeni yönergeler yayınlamıştır. Şirketler ve finansal kuruluşlar, özellikle sınır ötesi işlemlerle ilgili olarak artan bir uyumluluk baskısıyla karşı karşıyadır. Bu yeni düzenlemelere ayak uyduramamak, büyük para cezalarına, itibar kaybına ve iş süreçlerinde önemli aksamalara yol açabilir.

Jeopolitik çatışmaların neden olduğu düzenlemelerdeki ani değişikliklere hızla uyum sağlamak, şirketler için hayati önem taşımaktadır. Uyum ekipleri, yeni ihracat kontrollerine, finansal ambargolara ve ticaret kısıtlamalarına hızlı bir şekilde adapte olabilmelidir. Şirketlerin küresel tedarik zincirlerini derinlemesine anlaması, yaptırım kurallarına uyum sağlamak açısından kritik önemdedir. Kapsamlı durum tespiti süreçleri, sınır ötesi operasyonlarla ilişkili risklerin belirlenmesine ve bu risklerin en aza indirilmesine yardımcı olacaktır.

Artan uyum taleplerine yanıt olarak birçok kuruluş, teknolojiye yönelmektedir. Yapay zeka (AI) ve makine öğrenimi (ML) gibi teknolojiler, uyum ekiplerine karmaşık görevleri otomatikleştirme, işlem izleme ve risk değerlendirmesi gibi konularda önemli avantajlar sunmaktadır. Bu teknolojiler sayesinde kuruluşlar, şüpheli davranış kalıplarını daha hızlı tespit edebilir ve olası ihlallere gerçek zamanlı olarak yanıt verebilir. Blockchain teknolojisi de sınır ötesi işlemlerde şeffaflık ve izlenebilirliği artırarak, finansal akışların değişmez kayıtlarını sunmakta ve uyumluluk sistemlerinin bütünlüğünü güçlendirmektedir.

Sonuç olarak, jeopolitik gerilimlerin artmasıyla birlikte düzenleyici kurumlar şeffaflık ve hesap verebilirliğe daha fazla önem vermektedir. Şirketler, küresel ticaretin karmaşıklıklarıyla başa çıkmak için daha sofistike uyum süreçlerine ihtiyaç duymakta ve bu süreçleri desteklemek için teknolojiye yatırım yapmaktadır.

Yıkıcı Dolandırıcılık Planları

Yıkıcı Dolandırıcılık Planları

2024 yılının sonuna geldiğimiz şu günlerde, dolandırıcılıkla mücadele kritik bir eşiğe ulaşmıştır. Dolandırıcılık, doğrudan mali kayıpların yanı sıra, bu kayıpları önlemek için harcanan kaynaklarla da ciddi bir küresel maliyete yol açmaya devam etmektedir. Sadece 2023 yılında küresel dolandırıcılık kayıpları **485,6 milyar dolara** ulaşmış, bu da tüm sektörlerde ve bölgelerde dolandırıcılık planlarının keskin bir şekilde arttığını göstermektedir.

Finansal kurumlar, tüketiciler ve düzenleyici otoriteler, teknolojik gelişmelerle birlikte evrilen ve daha karmaşık hale gelen dolandırıcılık yöntemlerine karşı koymakta zorlanmaktadır. Dolandırıcılık, artık dünya genelinde en yaygın ve en zarar verici ekonomik suçlardan biri haline gelmiştir ve toplumun hemen her kesimini etkilemektedir. Birleşik Krallık'ta dolandırıcılık, suçların **%40'ından fazlasını** oluşturarak en yaygın suç türü olurken, ABD'de kredi kartı sahiplerinin **%60'ı** dolandırıcılık mağduru olmuştur.

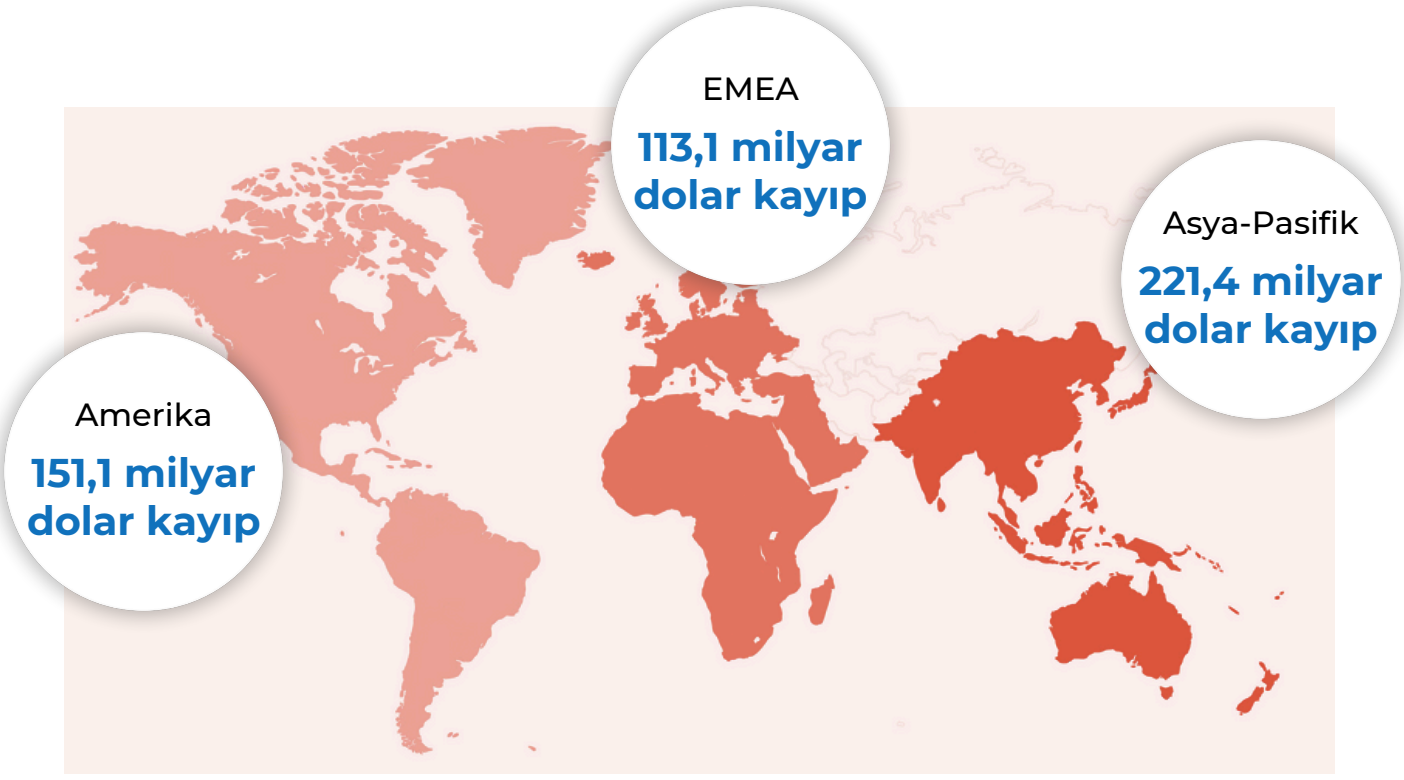
AI ve Hizmet Olarak Dolandırıcılık (Fraud-as-a-Service, FaaS) modellerinin ortaya çıkışıyla birlikte dolandırıcılar, operasyonlarını büyütme fırsatı yakalamış ve finansal sistemlerde daha önce görülmemiş seviyelerde yıkıcı etkiler yaratmıştır. Bu yeni nesil dolandırıcılık yöntemleri, geleneksel dolandırıcılık önleme tekniklerini yetersiz bırakmakta ve kurumların güvenlik açıklarını kapatma konusunda yeni stratejiler geliştirmelerini zorunlu kılmaktadır.

2023 yılında küresel dolandırıcılık kayıpları **485,6 milyar dolara** ulaşmıştır.

Dolandırıcılık Trendleri

Dolandırıcılık, küresel finansal sistemler üzerinde yıkıcı bir etki yaratmaya devam etmekte ve kilit bölgelerdeki kayıplar endişe verici seviyelere ulaşmaktadır. 2023 yılında, toplamda 485,6 milyar dolarlık bir kayıpla karşılaşılmış ve bu durumun 2024 yılında da devam ettiği gözlemlenmiştir. Asya-Pasifik bölgesi, 190,2 milyar dolarlık dolandırıcılık kaybıyla dolandırıcılıktan en çok etkilenen bölge olarak öne çıkmıştır; bu rakam, küresel dolandırıcılık kayıplarının neredeyse yarısını temsil etmektedir.

Amerika kıtasında dolandırıcılık kayıpları, 102,6 milyar dolarlık ödeme dolandırıcılığı, 21 milyar dolarlık çek dolandırıcılığı ve 13,6 milyar dolarlık kredi kartı dolandırıcılığından kaynaklanarak toplamda 151,1 milyar dolara ulaşmıştır. Avrupa, Orta Doğu ve Afrika (EMEA) bölgesinde de önemli dolandırıcılık kayıpları yaşanmış; 94 milyar dolarlık ödeme dolandırıcılığı ve 8,2 milyar dolarlık avans ücreti dolandırıcılığı ile toplam kayıp 113,1 milyar dolara ulaşmıştır.



Mevzubahis dolandırıcılık faaliyetlerindeki artış, siber destekli dolandırıcılık planları, deepfake teknolojisi ve kimlik doğrulama boşluklarından yararlanma gibi gelişen dolandırıcılık taktikleriyle beslenmektedir. Artık işletmeleri, tüketicileri ve hükümetleri hedef alan dolandırıcılık planları, en gelişmiş dolandırıcılık tespit sistemlerini dahi zorlayacak bir ölçekte faaliyet göstermektedir. Bu durum, finansal güvenliği sağlamak için daha güçlü ve etkili önlemlerin alınmasını zorunlu kılmaktadır.

Kimlik Hırsızlığı ve Sentetik Dolandırıcılık

Kimlik hırsızlığı, suçluların çalıntı kişisel bilgileri kullanarak bir dizi dolandırıcılık faaliyeti gerçekleştirmesiyle dünya genelinde en yaygın dolandırıcılık türlerinden biri haline gelmiştir. Sadece ABD'de, 2023 yılında **52 milyon Amerikalı** kredi veya banka kartlarında hileli harcamalarla karşılaşmış ve toplam yasa dışı satın alımlar **5 milyar doları** aşmıştır. Medyan dolandırıcılık ücreti, 2021 yılına göre %26'lık bir artışla **100 dolara** yükselmiştir.

Bununla birlikte, sentetik kimlik dolandırıcılığı olarak adlandırılan bir diğer dolandırıcılık türü giderek daha sinsi bir hal alıyor. The Aite Group'a göre, suçlular gerçek ve uydurma verileri birleştirerek sahte kimlikler oluşturmakta ve bu dolandırıcılık türü, teminatsız kredi portföylerindeki tahsilatların %10-15'ini temsil etmektedir. Sentetik kimlik dolandırıcılığını tespit etmek ve önlemek, özellikle zorlayıcıdır; çünkü bu planların arkasındaki suçlular, çeşitli sektörlerdeki kimlik doğrulama sistemlerindeki zayıflıklardan yararlanmaktadır.

2030'a kadar sentetik kimlik dolandırıcılığının
23 milyar dolara
ulaşacağı tahmin edilmektedir.

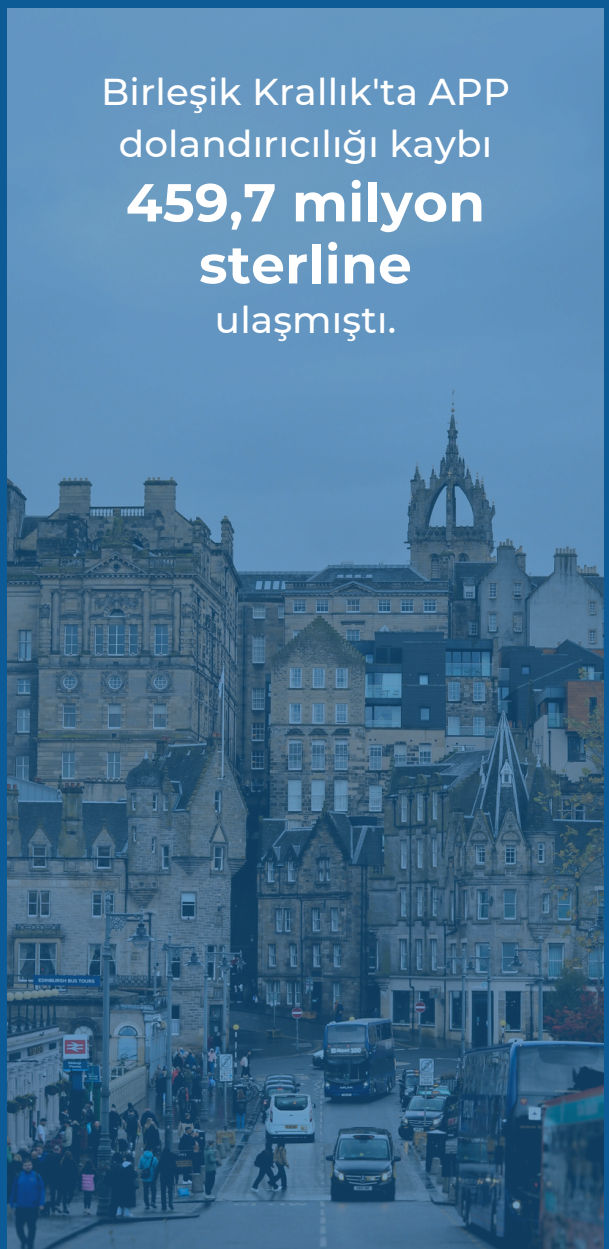
ABD, 2022 yılında **8,8 milyar dolara** ulaşan sentetik kimlik dolandırıcılığından kaynaklanan dolandırıcılık kayıplarında önemli bir artış gözlemlenmiştir. Giderek büyüyen bir endişe kaynağı olan bu durumun, potansiyel kayıpların 2030 yılına kadar **23 milyar dolara** ulaşabileceği tahmin edilmektedir. Finans kuruluşları, FinTech şirketleri ve müşteri doğrulamasına dayanan diğer sektörler, bu gelişen tehditlerle mücadele etmek için yapay zeka odaklı araçlara ve dinamik dolandırıcılık tespit sistemlerine büyük yatırımlar yapmak zorunda kalmıştır. Bu durum, finansal güvenliği sağlamak için daha kapsamlı önlemlerin gerekliliğini ortaya koymaktadır.

Sahtekarlık ve APP Dolandırıcılığı

Sahtekarlık, en yıkıcı ve yaygın dolandırıcılık trendlerinden biri haline gelmiş ve 2023 yılında yalnızca ABD'de **2,7 milyar dolarlık** zarara yol açmıştır. Bu dolandırıcılıklar, dolandırıcıların tanınmış işletmeleri, devlet kurumlarını ve hatta iş arkadaşlarını taklit ederek bireyleri para transferi yapmaya veya hassas bilgileri ifşa etmeye kandırmalarını içermektedir. Ticari sahtekarlıklar, **752 milyon dolarlık** kayba yol açarken, devlet sahtekarlıkları da toplam kayba önemli ölçüde katkıda bulunmuştur. Bu tür dolandırıcılıklar, suçluların kurbanları manipüle etmek için sosyal mühendislik tekniklerinden yararlandığı, birbirine bağlı dijital dünyada giderek daha yaygın hale gelmektedir.

Authorized Push Payment (APP) dolandırıcılığı, özellikle 2023 yılında kayıpların **459,7 milyon sterline** ulaştığı Birleşik Krallık'ta özellikle yıkıcı bir dolandırıcılık türü olarak öne çıkmıştır. APP dolandırıcılığı, mağdurların genellikle banka personeli veya polis memurlarının kimliğine bürünme gibi ikna edici planlarla doğrudan suçlulara para göndermeleri için kandırılmasıyla ortaya çıkmaktadır. Bu kayıpların önemli bir kısmı, APP dolandırıcılığı vakalarının %67'sini oluşturan satın alma dolandırıcılığından kaynaklanmaktadır. Başta Facebook, WhatsApp ve Instagram olmak üzere sosyal medya ve mesajlaşma platformlarının yükselişi, APP dolandırıcılıklarını körüklemiştir; 2023 yılında dolandırıcılıkların %60'ı bu üzerinden yürütülmüştür.

2023'te toplam kayıpların %62'sine tekabül eden **287,3 milyon sterlinlik** APP kaybı mağdurlara iade edilmiş olsa da, APP dolandırıcılığının sürekliliği, tüketicileri ve işletmeleri bu planlardan korumanın süregelen zorluğunu vurgulamaktadır. Düzenleyicilerin ve bankaların gerçek zamanlı dolandırıcılık tespitini geliştirme ve müşteri farkındalığını artırma çabaları bir miktar başarı göstermiştir; ancak dolandırıcılar, yeni güvenlik açıklarından yararlanmak için tekniklerini uyarlamaya devam etmektedir. Bu durum, dolandırıcılık önlemlerinin güçlendirilmesi ve kullanıcıların bilinçlendirilmesi gerekliliğini daha da ön plana çıkarmaktadır.



Sahtekarlık ve APP Dolandırıcılığı

Dolandırıcılık tespitindeki ilerlemelere rağmen, suçlular tedarik süreçlerini manipüle etmekte, maliyetleri şişirmekte ve sahte faturalar, komisyonlar ile satıcılar ve iç personel arasındaki gizli anlaşmalar gibi hileli planlar aracılığıyla fonları hortumlamaktadır. PwC tarafından yapılan bir anket, şirketlerin **%59'unun** geçtiğimiz yıl dolandırıcılık riski değerlendirmesi yaptığını, ancak **yaklaşık %20'sinin** satın alma dolandırıcılığını tespit etmek için veri analitiği kullanmadığını ortaya koymuştur. Bu boşluk, dolandırıcıların kurumsal kaynak planlama (ERP) sistemlerindeki ve tedarikten ödemeye süreçlerindeki zayıflıklardan yararlandıkça, birçok kuruluşu sofistike dolandırıcılık planlarına karşı savunmasız bırakmaktadır.

Küçük ve orta büyüklükteki işletmeler (KOBİ'ler), büyük şirketlerin gelişmiş sahtekarlık tespit sistemlerine sahip olmaması nedeniyle, her yıl milyonlarca dolara mal olan satın alma sahtekarlığı için birincil hedef haline gelmektedir. 2024 yılı itibarıyla, paravan şirketlerin ve sahte üçüncü taraf tedarikçilerin kullanımı artış göstermiş, bu durum dolandırıcıların var olmayan hizmetler veya mallar için işletmelere fatura kesen sahte tedarikçiler oluşturmasına olanak tanımıştır. Şirket içindeki bazı çalışanlar da, fonları yönlendirmek amacıyla bu paravan şirketleri kurarak suç ortağı olmuştur.

Satın alma dolandırıcılığıyla mücadele etmek için daha fazla şirket, gerçek zamanlı izleme ve şüpheli işlemlerin tespitine olanak tanıyan makine öğrenimi ve veri analitiği yöntemlerine yönelmektedir.

Ayrıca, ihbar programları ve iç denetimlerin hileli faaliyetlerin ortaya çıkarılmasında büyük önem taşıdığı kanıtlanmıştır. Bu stratejiler, dolandırıcılık riskini azaltma ve organizasyonların finansal güvenliğini sağlama açısından kritik bir rol oynamaktadır.

Temassız ve Anında Ödeme Dolandırıcılığı

2024 yılı itibarıyla temassız ve anında ödemelerin benimsenmesi hızla artarken, dolandırıcılar bu yeni ödeme yöntemlerinden büyük ölçüde yararlanma fırsatı bulmuştur. 2022 yılında **782 milyon** olan temassız mobil ödeme kullanan kişi sayısının, 2024 yılı sonunda **1 milyarı aşması** bekleniyor. NFC teknolojisinin akıllı telefonlar, dijital cüzdanlar ve Apple Pay ile Google Pay gibi giyilebilir cihazlarda yaygınlaşması, kullanıcıların sorunsuz işlemler gerçekleştirmesine olanak tanırken, dolandırıcılık için de cazip fırsatlar yaratmıştır.

Temassız dolandırıcılık kaynaklı kayıp **100,2 milyon sterline** ulaşmıştır.

Birleşik Krallık'ta temassız dolandırıcılık, 2023 yılında **%82 oranında bir artış** göstererek, çalınan veya kaybolan kartlarla ilgili kayıpların **100,2 milyon sterline** ulaşmasına neden olmuştur. Ayrıca, ACH transferleri, kripto ödemeleri ve dijital cüzdanlar gibi anlık ödemelerin yaygınlaşmasıyla birlikte dolandırıcılık riski de artmaktadır. SEPA bölgesindeki toplam kredi transferi hacminin %45'ini oluşturan anlık ödemeler, finansal ekosistemdeki artan önemlerini vurgulamaktadır. Ancak bu işlemlerin hızları, bankalara ve finans kuruluşlarına dolandırıcılık işlemlerini engellemek veya tersine çevirmek için çok az zaman tanımakta, bu durum da dolandırıcılar için cazip bir fırsat oluşturmaktadır.

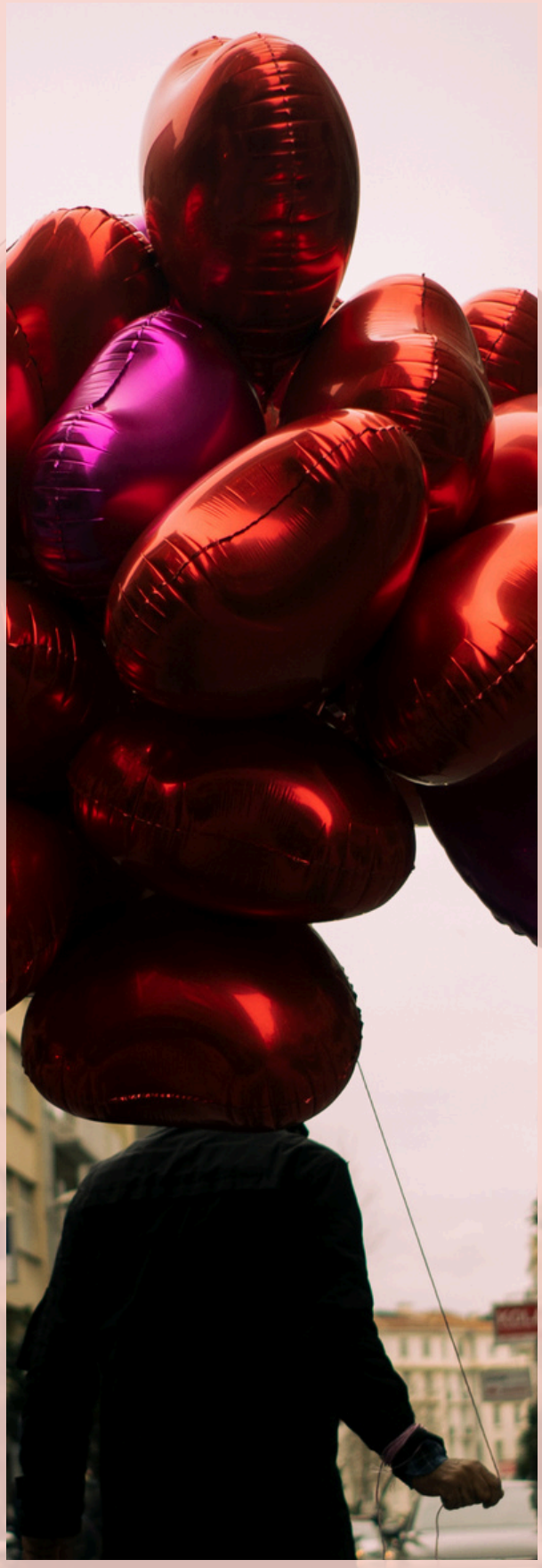
Suçlular, APP dolandırıcılığı gibi çeşitli taktiklerle bu sistemleri istismar etmekte; kurbanların dolandırıcılar tarafından kontrol edilen hesaplara para göndermeleri için kandırılmalarını sağlamaktadır. Gerçek zamanlı ödemelerin daha yaygın hale gelmesiyle birlikte, bankalar işlem kalıplarını analiz edebilen ve anormallikleri gerçek zamanlı olarak işaretleyebilen gelişmiş dolandırıcılık tespit sistemlerine yatırım yapmaktadır. Ancak, bu yeni ödeme yöntemlerinin hızlı yükselişi, finansal kuruluşlar için önemli zorluklar yaratmaya devam etmektedir. Dolandırıcılığın önlenmesi için sürekli olarak yenilikçi çözümlerin geliştirilmesi ve kullanıcıların bilinçlendirilmesi gerekmektedir.

Romantik Dolandırıcılık ve Güven Şemaları

Romantik ve güven temelli dolandırıcılık faaliyetleri, geçtiğimiz yıl önemli bir artış göstererek, dünya genelinde birçok kişiyi mağdur etmiştir. 2023 yılında romantik dolandırıcılık nedeniyle küresel çapta **3,8 milyar dolar** kaybedilmiş olup, bu durum bahsedilen dolandırıcılık türünün en hızlı büyüyen suçlardan biri olduğunu göstermektedir. Güvene dayanan dolandırıcılık türleri, özellikle yalnız veya arkadaşlık arayan bireyleri avlayarak, onların duygusal zayıflıklarını istismar etmektedir.

Bu dolandırıcılıklar sadece duygusal olarak yıkıcı olmakla kalmayıp, aynı zamanda finansal olarak da ciddi zararlar vermektedir. Mağdurlar, inandıkları dolandırıcılara büyük miktarlarda para transferi yapmaya ikna edilmekte; bazı durumlarda ise farkında olmadan para katırı olarak kullanılmaktadırlar. Bu kişiler, dolandırıcıların suç faaliyetlerinin gelirlerini aklamak için kullanıldığına dair bir anlayışları olmaksızın, para taşımakta ve dolayısıyla daha büyük suçların bir parçası haline gelmektedirler. Romantik dolandırıcılık, kurbanların aldatıldıklarını kabul etmeyi reddetmeleri nedeniyle özellikle sinsidir ve bu durum, müdahale ve önlemeyi zorlaştırmaktadır.

Sosyal medya platformları ve çevrim içi arkadaşlık siteleri, dolandırıcıların anonimlikten faydalanarak kurbanlarını manipüle ettiği başlıca kanallar haline gelmiştir. Action Fraud ve diğer yetkililer, bu tür vakalarda keskin bir artış olduğunu ve birçok mağdurun birikimlerini, evlerini veya emekli maaşlarını kaybettiğini rapor etmektedir. Bu durumu önlemek amacıyla finansal kuruluşlar ve kolluk kuvvetleri, tüketicileri bu dolandırıcılıkların tehlikeleri hakkında eğitmek için iş birliği yapmakta ve şüpheli işlem davranışlarını izlemek için gelişmiş dolandırıcılık tespit sistemleri kullanmaktadır. Dolandırıcılıkların yaygınlığı, eğitim ve farkındalık oluşturma çabalarının ne denli önemli olduğunu bir kez daha vurgulamaktadır.



Yaşlının Finansal Sömürüsü ve Savunmasız Mağdur Dolandırıcılığı

Dolandırıcılar, modern teknoloji ve finansal sistemlere olan sınırlı aşinalıklarını istismar ederek yaşlı ve savunmasız bireyleri giderek daha fazla hedef almaktadır. Yaşlı finansal istismarı (EFE) 2023 yılında dramatik bir artış göstermiş ve toplam kayıp **77,7 milyar dolara** ulaşmıştır. Yaşlılar sıklıkla, bir dolandırıcının kurbanın torununu taklit ettiği ve sahte bir kriz için acil mali yardım talep ettiği büyükanne-büyükbaba şeması gibi taklit, korku taktikleri ve sosyal mühendislik içeren dolandırıcılıklarla hedef alınmaktadır.

Ulusal Suç Ajansı, 2023 yılında Birleşik Krallık'taki her 10 yaşlıdan 1'inin finansal istismar mağduru olduğunu, ancak bilinen her yaşlı istismarı vakasına karşılık 23 vakanın bildirilmediğini bildirmiştir. Bu durum, yaşlı mağdurların genellikle utanç, bağımsızlıklarını kaybetme korkusu veya travmatik deneyimlerini unutma isteği nedeniyle bu suçları bildirmekten kaçındıklarını göstermektedir. Bu eksik raporlama, yetkililerin sorunun boyutunu tam olarak kavramasını zorlaştırmaktadır.

Yaşlıların mali istismarı tek bir dolandırıcılık türüyle sınırlı değildir. Dolandırıcılar, yaşlı kurbanları kandırmak ve paralarını ele geçirmek için taklit dolandırıcılığı, kimlik hırsızlığı ve romantik dolandırıcılık gibi farklı yöntemler kullanarak çeşitli yaklaşımlar sergilemektedir. Finans kuruluşları, şüpheli faaliyetleri izleyerek, eğitim kaynakları sağlayarak ve önemli mali zararlar meydana gelmeden önce istismarı tespit etmek ve önlemek için kolluk kuvvetleriyle yakın bir şekilde çalışarak bu tür dolandırıcılıkları engellemede kritik bir rol oynamaktadır.

Her 10 yaşlıdan 1'i finansal istismar mağduru

Yüksek Teknolojili Dolandırıcılık: Yapay Zekadan Deepfake'e

2024 yılı, finansal dolandırıcılıkta deepfake kullanımının ciddi ve yaygın bir sorun haline geldiği bir dönem olarak kaydedildi. Artık bu fütüristik kavram, kurumlar ve bireyler için büyük riskler oluşturan bir gerçeklik. En çarpıcı örneklerden biri, bir finans çalışanının CFO'su ve iş arkadaşlarıyla gerçek bir video görüşmesi yaptığına inanarak 39 milyon dolar transfer ettiği Hong Kong'dan geliyor. Gerçekte tüm toplantı, güvenilen yöneticilerin kimliğine bürünmek için deepfake teknolojisini kullanan dolandırıcılar tarafından düzenlenmişti. Bu olay, deepfake dolandırıcılığının teorik tartışmaların ötesine geçerek gerçek dünyadaki operasyonlara nasıl dönüştüğünü ve finans sektöründe nasıl hasara yol açtığını açıkça sergilemekte.

Deepfake teknolojisinin etkileri sadece finansal kayıplarla sınırlı kalmıyor. Yapay zeka tarafından üretilen bu manipülasyonlar aynı zamanda yanlış bilgi yaymak, itibara zarar vermek ve dijital iletişime olan güveni sarsmak için de kullanılıyor. Dolandırıcılar, gelişmiş yapay zeka araçlarıyla inandırıcı ses taklitleri yapabiliyor, son derece gerçekçi sahte videolar üretebiliyor ve tamamen meşru görünen sahte e-postalar gönderebiliyor. Bu durum, alıcıların kötü niyetli faaliyetleri tespit etmesini son derece zorlaştırıyor.

Bu yeni dolandırıcılık dalgasına karşı en savunmasız sektörlerden biri, 2023 yılında tespit edilen deepfake ile ilgili tüm dolandırıcılık vakalarının **%88** gibi şaşırtıcı bir oranını oluşturan kripto para birimidir. Kripto sektörünün dijital ve merkezi olmayan yapısı, onu gelişmiş dolandırıcılık teknikleri için cazip bir hedef haline getirmekte ve suçlular büyük ölçekli dolandırıcılıklar gerçekleştirmek için yüksek finansal risklerden ve dijital anonimlikten yararlanmaktadır. Kripto işlemlerine yönelik Deepfake saldırıları genellikle son derece karmaşıktır ve ikna edici sahte kimlikler oluşturmak veya kuruluş içindeki güvenilir kişileri taklit etmek için yapay zeka kullanır.

Finansal Teknoloji (FinTech) sektörü de deepfake dolandırıcılığının yükselişiyle başa çıkmakta zorlanıyor. 2023 yılında FinTech'te deepfake içeren olaylar %700 oranında artış gösterdi; bu durum, dolandırıcılık faaliyetlerini kolaylaştırmak için siber suçluların üretken yapay zekayı hızla benimsemesini yansıtıyor. Yapay zeka destekli dolandırıcılıklar, genellikle geleneksel güvenlik önlemlerini aşarak daha büyük tehditler oluşturuyor. Örneğin, dolandırıcılar uzaktan doğrulama süreçlerini atlatmak için sanal kameralar ve yapay zeka tarafından üretilen "yüz takasları" kullanarak kimlik doğrulama sistemlerine yönelik saldırıları %704 oranında artırdı.

Ancak, bu yeni dolandırıcılık dalgasına karşı birçok yönetici hazırlıksız. 2024 yılının sonuna kadar neredeyse her dört yöneticiden biri deepfake teknolojisine ya çok az aşina olacak ya da hiç aşina olmayacak. Bu durum, kuruluşlarını potansiyel risklere maruz bırakıyor. Uzmanlar, yapay zeka odaklı dolandırıcılıkların karmaşıklığı ve sıklığının artmasıyla birlikte, 2023'te üretken yapay zeka teknolojileri tarafından kolaylaştırılan dolandırıcılık kayıplarının sadece ABD'de 12,3 milyar dolardan 2027 yılına kadar 40 milyar dolara yükseleceğini öngörüyor.

Deepfake dolandırıcılığının yükselişi, finans kurumlarının savunmalarını güçlendirmeleri için acil bir ihtiyaca işaret ediyor. Bu ortamda, finans liderlerinin güvenlik protokollerini düzenli olarak gözden geçirmesi, ekiplerini şüpheli talepleri fark edebilmeleri için eğitmesi ve dolandırıcılık faaliyetlerini ciddi bir zarar oluşmadan önce tespit edip etkisiz hale getirebilecek gelişmiş anti-deepfake teknolojilerine yatırım yapması kritik öneme sahiptir.

FinTech sektöründe deepfake içeren vakalar **%700 artış** gösterdi

Kurumlar, AI tabanlı dolandırıcılıkla mücadele edebilmek için sahtekarlık tespit sistemlerini, yapay zeka destekli anomali tespiti ve davranışsal biyometriyi entegre ederek yeniden kalibre etmelidir. Gerçek zamanlı işlem takibi ve gelişmiş makine öğrenimi modelleri, normal kullanıcı davranışından sapmaları tespit ederek şüpheli örüntüleri işaretleyebilir. Özellikle kritik durumlarda işaretlenen vakaları doğrulamak için insan denetimi büyük önem taşır ve derin sahtecilik gibi gelişen tehditlere karşı katmanlı bir savunma sağlar.

Baptiste Forestier
Head of Compliance

Sektöre Özel Dolandırıcılık Taktikleri

2024 yılında, çeşitli sektörler, her biri finansal suçları işlemek için benzersiz güvenlik açıklarından yararlanan özel dolandırıcılık taktikleriyle karşı karşıya kaldı. Finans ve bankacılıktan perakende ve gayrimenkule kadar, dolandırıcılar sektöre özgü süreçlerden ve zayıflıklardan yararlanan sektöre özgü teknikler geliştirdiler.

Finansal Hizmetler

Finansal hizmetler sektörü, günlük işlenen büyük miktardaki para nedeniyle dolandırıcılık için cazip bir hedef olmaya devam etmektedir. Bu alandaki en önemli tehditlerden biri, teminatsız kredi portföylerindeki tahsilatların %10-15'inden sorumlu olan sentetik kimlik dolandırıcılığıdır. Suçluların yeni kimlikler oluşturmak için gerçek ve sahte bilgileri birleştirdiği bu dolandırıcılık türü, bankaları ve kredi verenleri ciddi şekilde rahatsız etmektedir. 2022 yılında ABD'de kimlik hırsızlığı kayıplarının yaklaşık **8,8 milyar dolar** olduğu tahmin edilmektedir ve sentetik kimlik dolandırıcılığının yaygınlaşmasıyla bu rakamın önümüzdeki yıllarda önemli ölçüde artması beklenmektedir.

Bir diğer kritik sorun ise hesap ele geçirme (Account Takeover, ATO) dolandırıcılığıdır. 2023 yılında fintech ve bankacılık sektörlerinde tüketici hesaplarından kaynaklanan dolandırıcılık girişimlerinde **%61'lik** bir artış gözlemlenmiştir. Bu durum, kuruluşların müşteri hesaplarını koruma çabalarını daha da zorlaştırmaktadır.

Anında ödemelerin artan popülaritesi, finansal ortama karmaşıklık eklemekte ve dolandırıcılık için yeni fırsatlar yaratmaktadır. Daha hızlı işlem yöntemleri, örneğin ACH, dijital cüzdanlar ve gerçek zamanlı ödemeler, kullanıcılar için kolaylık sağlarken dolandırıcılar için yeni hedefler oluşturmaktadır. Gerçek zamanlı ödemeler, hileli işlemlerin başlatıldıktan sonra geri döndürülmesini son derece zorlaştırarak finans kuruluşlarını kayıp fonları önlemeye veya kurtarmaya çalışırken zor bir duruma sokmaktadır.

Bu bağlamda, dikkat çekici bir örnek, 2023 yılında APP dolandırıcılığı vakalarında %12'lik bir artış yaşanması ve toplam kaybın **459,7 milyon sterline** ulaşmasıdır. APP dolandırıcılığı, dolandırıcıların meşru kişiler veya şirketler gibi davranarak mağdurları doğrudan kendilerine para göndermeye ikna etmesini içermekte ve bireyler ile küçük işletmeleri orantısız şekilde etkilemektedir.

Perakende ve E-Ticaret

Perakende sektöründe, özellikle e-ticaret alanında online alışverişin sürekli büyümesi, dolandırıcılığı da beraberinde getirmiştir. Mart 2023'te Birleşik Krallık'taki perakende satışların dörtte birinden fazlasının online olarak gerçekleşmesi beklenirken, dolandırıcılar bu artıştan faydalanmak için online işlemlerdeki zayıflıkları hedef almaya başladılar. Bu bağlamda, Card-not-present (CNP) dolandırıcılığı, suçluların çalıntı kredi kartı bilgilerini kullanarak çevrim içi alışveriş yapması için en yaygın yöntemlerden biri olarak dikkat çekiyor.

Black Friday ve tatil alışveriş sezonları gibi dönemlerde dijital işlemlerin yüksek hacmi, dolandırıcıların faaliyetlerini milyonlarca yasal işlem arasında gizlemelerine olanak tanıyarak durumu daha da kötüleştiriyor. Bu durum, hem tüketiciler hem de perakendeciler için ciddi riskler oluşturuyor.

Bir diğer önemli endişe ise dolandırıcıların teslimat şirketi gibi davranarak müşterilerden ek ücret talep etmesi ya da teslimatları yeniden planlamasını istemesidir. Bu tür paket teslimat dolandırıcılığı, yalnızca 2023'ün ilk çeyreğinde **yaklaşık 40 milyon** Birleşik Krallık vatandaşını mağdur etmiştir. Online alışverişin artmasıyla birlikte bu sorunun daha da kötüleşmesi bekleniyor.
Bilet dolandırıcılığı da özellikle konserler ve spor karşılaşmaları gibi yüksek talep gören etkinliklerle ilgili olarak yaygınlaşmaktadır. Geçtiğimiz yıl, sahte Premier Lig bilet satışları sadece Birleşik Krallık'taki kurbanlara **40.000 sterline** mal olmuştur. Suçlular, şüphelenmeyen taraftarları hedef almak için Facebook Marketplace gibi sosyal medya platformlarını kullanarak dolandırıcılık faaliyetlerini artırmışlardır.

Sonuç olarak, e-ticaretin büyümesiyle birlikte dolandırıcılık vakalarının artması, hem tüketicileri hem de perakendecileri daha dikkatli olmaya zorlamaktadır. Bu nedenle, güvenli online alışveriş için tüketicilerin dolandırıcılık belirtilerine karşı dikkatli olmaları, güçlü şifreler kullanmaları ve sadece güvenilir sitelerden alışveriş yapmaları önemlidir. Perakendeciler ise, müşteri bilgilerini koruma, dolandırıcılığı tespit etme ve güvenli ödeme yöntemlerini teşvik etme konusunda daha proaktif olmalıdır.

> 2024 yılında bankalar ve ödeme kuruluşlarında en sık rastlanan dolandırıcılık türlerinin başında, düşük finansal ve teknolojik okuryazarlığı istismar eden yöntemler geliyor. Özellikle sosyal medya kullanımının artmasıyla, sosyal mühendislik dolandırıcılıkları öne çıkıyor. E-ticaretin gelişmesiyle birlikte, savcılık veya kamu kurumlarının adı kullanılarak sosyal medya ve internet üzerinden çalıntı hesap ve kartlarla yapılan IBAN dolandırıcılıkları da yaygınlaştı.
>
> Kolay yoldan para kazanmak isteyen, ancak hukuki sonuçlarını tam kestiremeyen bilinçsiz gerçek veya tüzel kişiler, dolandırıcıların hesaplarını kullanmalarına izin veriyor. Bu kişiler, POS dolandırıcılığı gibi yöntemlerle ya doğrudan kartlarını kullanıyor ya da kumar ve bahis aracıları aracılığıyla POS cihazlarından yapılan düzensiz işlemlerle nitelikli dolandırıcılara ve kara para aklayıcılara araç oluyor.

Tuba Erdem
Director of Compliance & Internal Control

Emlak ve Mülk Yönetimi

2023 yılında, **her 8 kiralama başvurusundan 1'inin** bir tür sahtekarlık içerdiği tespit edilmiştir. Bu durum, mülk yöneticileri için daha yüksek tahliye ve alacak riski doğurmakta.

Gayrimenkul sektöründe, kira başvurusu dolandırıcılığı son yıllarda keskin bir artış göstermektedir. Dolandırıcılar, belgeleri taklit etmek için dijital sistemlerden faydalanarak daha sofistike yöntemler geliştirmekte; değiştirilmiş banka hesap özetleri ve maaş koçanları hazırlamaktadır.

Kira dolandırıcılığı, özellikle sahte belgelerin tespit edilmeden geçebildiği lüks emlak piyasasında daha yaygın hale gelmiştir. Mülk sahipleri, bu tür dolandırıcılıklara maruz kaldıklarında önemli mali kayıplar yaşayabilmektedir. Bu nedenle, kiralama sürecinde daha dikkatli ve titiz olunması gerekmektedir.

Daha geniş emlak piyasasında ise tapu dolandırıcılığı yeni bir tehdit olarak öne çıkmaktadır. Suçlular, çalıntı kimlikleri kullanarak mülk sahipliği kayıtlarını değiştirebilmekte, kredi almakta veya sahip olmadıkları mülkleri satabilmektedir. Pandemi döneminde uzaktan yapılan işlemlerin artması, bu sorunu daha da büyütmüştür. Tapu dolandırıcılığından kurtulmak, mağdurlar için maliyetli ve zaman alıcı olabilmekte, bu da sektördeki güveni zedelemektedir.

Sağlık Hizmetleri ve Sigorta

Sağlık sektörü, artan tıbbi maliyetler ve karmaşık faturalama süreçleri nedeniyle sigorta dolandırıcılığı ile mücadelede ciddi zorluklar yaşamaktadır. 2022 yılında, en yaygın türü trafik sigortası dolandırıcılığı olmak üzere, hileli sigorta taleplerinin toplamı **1,1 milyar £** olarak kaydedilmiştir. Dolandırıcılar, sigorta şirketlerini hedef alarak talepleri abartmakta veya tamamen hayali olaylar sunarak tüketicilerin primlerini artırmaktadır. Bu durum, hem sigorta şirketlerinin mali durumunu tehdit etmekte hem de dürüst tüketicilerin mali yüklerini artırmaktadır.

Ayrıca, tıbbi kimlik hırsızlığı, dolandırıcıların tıbbi hizmetlere erişmek veya reçeteli ilaçları almak için çalıntı kimlikler kullanarak gerçekleştirdiği bir diğer sorun haline gelmiştir. Bu tür dolandırıcılığın finansal etkilerinin yanı sıra, yanlış tıbbi kayıtlara yol açması ve hasta bakımının tehlikeye sokması oldukça ciddi sonuçlar doğurabilir. Yanlış teşhis ve tedavi uygulamaları, hastaların sağlıklarını ciddi şekilde tehdit edebilir. Sağlık hizmeti sağlayıcıları, hizmetlerini dijitalleştirmeye devam ettikçe, sağlam dolandırıcılık önleme sistemlerine duyulan ihtiyaç her zamankinden daha kritik hale gelmektedir.

1,1 milyar sterlin
hileli sigorta talebi kaydedildi

Teknoloji ve Telekomünikasyon

Telekomünikasyon sektörü, bulut iletişimin benimsenmesi ile ücretli arama dolandırıcılığında belirgin bir artışla karşı karşıya kalmaktadır. Dolandırıcılar, telefon sistemlerindeki açıklardan faydalanarak yüksek ücretli numaralara yetkisiz uluslararası aramalar gerçekleştiriyor ve bu yolla milyarlarca dolarlık yasa dışı kazanç elde ediyor. Ücret dolandırıcılığı, özellikle İnternet Protokolü Üzerinden Ses (VoIP) sistemlerini yoğun şekilde kullanan işletmelerde yaygındır. Bu tür teknolojiler, çoğu zaman gerekli güvenlik önlemlerinden yoksun oldukları için dolandırıcılığa karşı savunmasız hale gelmektedir. Geçiş ücreti dolandırıcılığı, telekomünikasyon sektöründeki en yaygın dolandırıcılık türlerinden biri olup, VoIP sistemlerinin küresel olarak benimsenmesi arttıkça kayıpların da artması beklenmektedir.

Ayrıca, teknoloji sektörü, Uygulamadan Kişiye (A2P) mesajlaşmada Yapay Trafik Enflasyonu (AIT) dolandırıcılığı ile de mücadele etmektedir. Dolandırıcılar, kurumsal maliyetleri şişirmek için büyük miktarlarda sahte trafik oluşturarak, İki Faktörlü Kimlik Doğrulama (2FA) gibi müşteri iletişim sistemlerine güvenen işletmeler üzerinde önemli mali baskılar yaratmaktadır. SMS tabanlı 2FA, popüler bir güvenlik önlemi olmaya devam ederken, AIT dolandırıcılığı birçok sektörde işletmeler için artan bir endişe kaynağı haline gelmektedir.

Finansal Suçların Önlenmesinde Öncü Teknoloji

Finansal Suçların Önlenmesinde Öncü Teknoloji

2024 yılı, finans dünyasında önemli bir teknolojik dönüşüm dönemini temsil ediyor. Bu dönemde, dolandırıcılık, kara para aklama, terör finansmanı ve diğer finansal suçların önlenmesinde teknolojik yeniliklerin rolü giderek daha kritik hale geldi. Suç örgütleri, yasa dışı amaçlar için yeni teknolojileri kullanma konusunda daha incelikli hale geldikçe, finansal kurumlar da operasyonlarını korumak için sürekli olarak gelişmek zorundalar. Yapay zeka, blockchain, robotik süreç otomasyonu (RPA) ve diğer teknolojilerin entegrasyonu, finans kuruluşlarının mali suçları tespit etme, önleme ve bunlara müdahale etme yöntemlerini temelden yeniden şekillendirmiştir.

Yapay zeka ve makine öğrenimi, modern finansal suçları önlemenin temel taşları haline geldi. Bu teknolojiler, dolandırıcılık, kara para aklama ve terör finansmanı ile mücadelede merkezi bir rol üstleniyor. AI'nın büyük miktarda veriyi gerçek zamanlı olarak analiz etme kapasitesi, finansal kurumların şüpheli faaliyetleri neredeyse anında tespit etmelerine olanak tanıyor. 2024 yılında, AI odaklı izleme sistemleri geçmiş verilerden öğrenerek, insanların gözden kaçırabileceği modelleri tespit ederek olağan dışı işlemleri tanımlamada daha da etkili hale geldi.

Yapay zeka, kapsamlı işlem verilerinin analizi yoluyla, müşteri davranışlarındaki potansiyel kara para aklama sinyallerini tespit etme yeteneğine sahiptir. Bu durum, beklenmedik önemli transferlerin yanı sıra uluslararası ödemelerdeki düzensizliklerin tanınmasını da içeriyor. Ayrıca, makine öğrenimi algoritmaları sürekli olarak gelişebilir, yeni suç taktiklerine uyum sağlayabilir ve finans kuruluşlarının suçlulardan bir adım önde olmasını güvence altına alabilir.

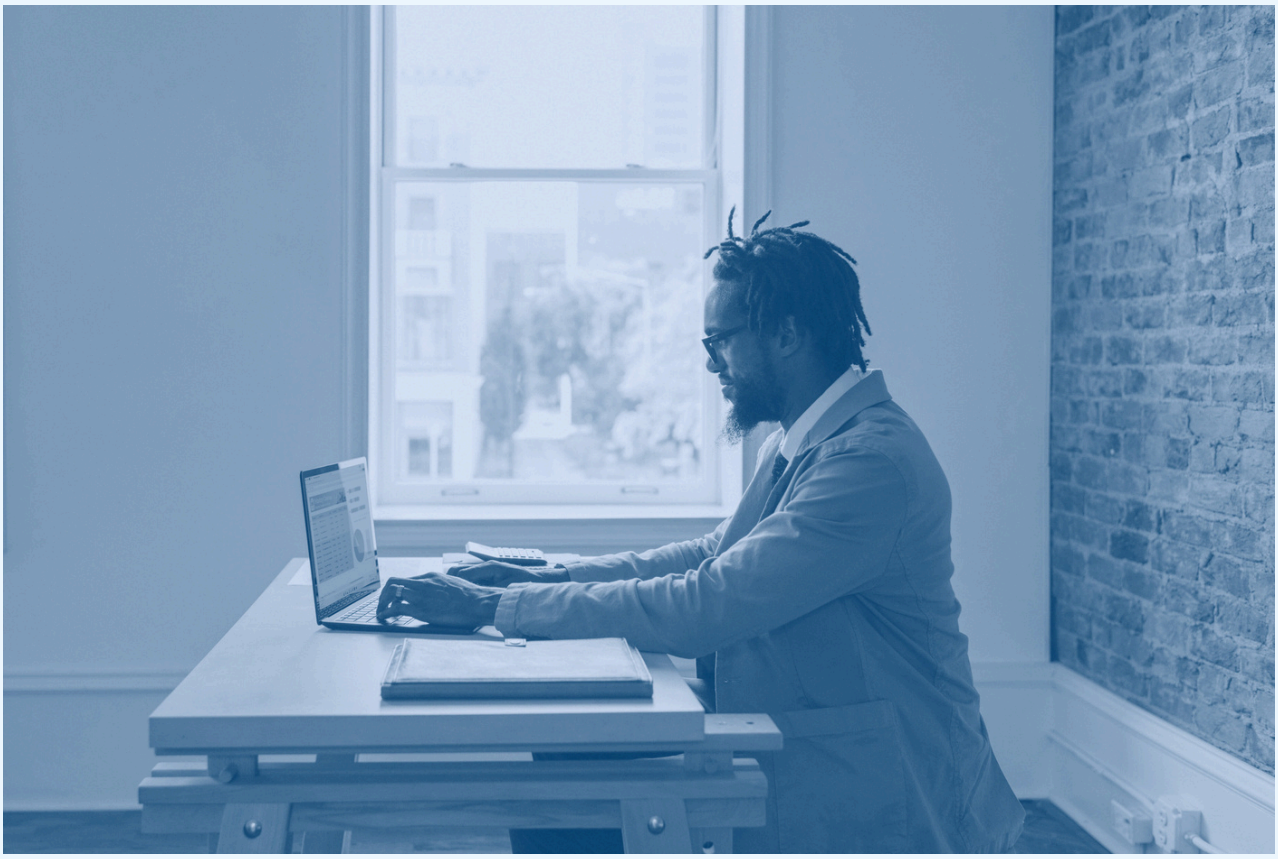
AI'nın rolü sadece AML ile sınırlı değildir; potansiyelinden yararlanılan bir diğer alan da CFT'dir. Jeopolitik veriler ve sosyal zeka ile entegre edilen yapay zeka modelleri, terörist ağlarla bağlantılı küçük ancak şüpheli finansal işlemlerin belirlenmesinde kritik bir öneme sahiptir. Bu tür verilerin analizi, güvenlik güçlerine ve finansal kurumlara, terörist aktiviteleri önceden tespit etme ve önleme fırsatı sunar.

> Blockchain analitik araçları, yapay zeka destekli KYC/AML sistemleri ve kuantum bilişim, mali suçlarla mücadelede en umut verici teknolojiler arasında yer almaktadır. Blockchain, işlemlerin şeffaflığını ve izlenebilirliğini artırırken, yapay zeka büyük veri işleyerek dolandırıcılık modellerini tespit edebilir. Henüz gelişme aşamasında olan kuantum bilişim ise şifreleme ve şifre çözme alanında devrim yaratarak finans sektöründe güvenlik çerçevelerini güçlendirme potansiyeline sahiptir. Bu teknolojileri benimsemek, mali suçlara karşı mücadelede bir adım önde olmanın anahtarı olacaktır.

Baptiste Forestier
Head of Compliance

Yapay zeka, finansal suçları tespit etmenin ötesinde, uyumluluk süreçlerini optimize etmek ve kurumlar üzerindeki operasyonel yükleri azaltmak için etkili bir araç haline geldi. Müşterileri gerçek zamanlı olarak taramak için biyometrik doğrulama ve AI destekli kimlik kontrollerinin kullanılması, KYC prosedürlerinin uygulanmasında önemli bir rol oynamaktadır. Bu AI güdümlü otomasyon, risksiz kullanıcılar için daha hızlı ve sorunsuz bir geçiş sağlarken, sağlayıcının da yasal yükümlülükler konusunda uyumlu kalmasına olanak tanımaktadır. Başlangıçta kripto para birimleri ile anılan blockchain teknolojisi, finansal suçların önlenmesinde güçlü bir araca dönüşmüştür. 2024 yılında, blockchain'in merkezi olmayan ve değişmez doğası, özellikle KYC ve AML düzenlemelerine uyumu sağlamak amacıyla finansal sistemlerde şeffaflığı artırmak için kullanılmaktadır. Finansal kurumlar, doğrulanmış KYC verilerini sınırlar arasında güvenli bir şekilde paylaşmak için blockchain teknolojisini kullanarak, yalnızca uyumluluğu kolaylaştırmakla kalmayıp aynı zamanda suçluların farklı yetki alanlarındaki parçalanmış düzenleyici çerçevelerden yararlanamamasını sağlıyor.

Blockchain teknolojisi, işlemlerin gerçek zamanlı olarak izlenmesine olanak tanıyarak suçluların kara para aklamasını veya finansal faaliyetlerini gizlemesini önemli ölçüde zorlaştırmaktadır. Akıllı sözleşmeler, uluslararası ticarette kullanılmakta ve belirli finansal eşiklere ulaşıldığında AML kontrollerini otomatik olarak gerçekleştirerek insan müdahalesini ve hata olasılığını azaltmaktadır. Blockchain'in potansiyeli, AML ve KYC'nin ötesine geçerek, şeffaflığı artırmak ve dolandırıcılık riskini azaltmak için sınır ötesi ödeme sistemlerinde de değerlendirilmeye başlanmıştır.



Açık Kaynak İstihbaratı (OSINT), finansal suçların önlenmesinde giderek artan bir rol üstlenmektedir. OSINT, kamuya açık bilgilerden yararlanarak finans kuruluşlarının durum tespiti süreçlerini geliştirmelerine ve küresel suç ağlarına dair anlayışlarını zenginleştirmelerine olanak tanır. Daha fazla kurum, yasa dışı faaliyetleri izlemek amacıyla karanlık web ve sosyal medyayı analiz etmek için OSINT'e yönelmekte; bu sayede dolandırıcılık planları, terör finansmanı ve kara para aklama gibi potansiyel tehditler hakkında kritik istihbarat elde etmektedir. OSINT'in dış kaynaklardan gelen erken uyarı işaretlerini tespit etme yeteneği, kurumların hızlı hareket etmesini sağlayarak kayıpları gerçekleşmeden önce önlemelerine yardımcı olur.

Robotik Süreç Otomasyonu (RPA), yapay zeka veya blockchain kadar dikkat çekici olmasa da, uyumluluk görevlerini kolaylaştırmada kritik bir rol oynamaktadır. RPA'nın işlem izleme, risk değerlendirmesi ve müşteri durum tespiti gibi tekrarlayan görevleri otomatikleştirme yeteneği, finans kuruluşlarının uyumluluk gereksinimlerinin artan karmaşıklığını daha verimli bir şekilde yönetmelerine olanak tanır. Finans kuruluşları, süreçleri hızlandırmak ve uyum maliyetini azaltmak için RPA'yı benimseyerek şüpheli faaliyet raporlarının hızlı ve doğru bir şekilde dosyalanmasını sağlamaktadır. Bu otomasyon, yalnızca insan hatalarını azaltmakla kalmayıp, uyum ekiplerinin daha stratejik ve yüksek öncelikli soruşturmalara odaklanmalarına da olanak tanır.

Kuantum bilişim mali suçların önlenmesinde potansiyel bir oyun değiştirici olarak ortaya çıkmaktadır.

Ayrıca, RPA ve yapay zekanın birleşimi olan Akıllı Otomasyon (IA), uyum süreçlerini kolaylaştırmaya devam etmektedir. 2024 yılında IA, işlem izleme, KYC prosedürleri ve müşteri durum tespiti gibi rutin görevleri otomatikleştirmek için kullanılmaktadır. Dolandırıcılık girişimleri daha karmaşık hale geldikçe, IA, artan uyumluluk verisi hacimlerinin yönetilmesine yardımcı olarak kurumlar üzerindeki operasyonel yükü azaltmakta ve daha stratejik, yüksek öncelikli soruşturmalar için insan kaynaklarını serbest bırakmaktadır.

Bulut bilişim, uzun zamandır dijital dönüşümün itici gücü olsa da, finansal suçların önlenmesindeki rolü de giderek artmaktadır. 2024 yılında finans kurumları, küresel varlıklar arasında gerçek zamanlı iş birliği ve veri paylaşımını mümkün kılmak için bulut tabanlı platformları daha fazla kullanmaktadır. Bu düzeyde bir bağlılık, kurumların ortaya çıkan tehditlere hızlı bir şekilde yanıt vermesine ve istihbaratı daha verimli bir şekilde paylaşmasına olanak tanır. Bulut platformları ayrıca uçtan uca şifreleme ve gelişmiş tehdit algılama gibi özellikler sunarak hassas finansal verilerin korunmasını sağlar; bu da finansal suçların dijital alana taşınmasıyla giderek yaygınlaşan siber saldırılara karşı bir güvenlik katmanı oluşturur. Gerçek zamanlı veri paylaşımı, finansal suçların önlenmesi konusunda kurumların sorunsuz bir şekilde iş birliği yapma gücünü artırırken, gizliliği artıran teknolojiler (PET'ler) aracılığıyla veri gizliliğini de korur.

Geleceği düşündüğümüzde, kuantum bilişim mali suçların önlenmesinde potansiyel bir oyun değiştirici olarak ortaya çıkmaktadır. Henüz emekleme aşamasında olmasına rağmen, 2024'teki pilot programlar, büyük veri kümelerini benzeri görülmemiş hızlarda işlemek ve analiz etmek için kuantum algoritmalarının kullanımını araştırmaktadır. Teorik olarak, kuantum bilişim, kurumların en karmaşık küresel finans ağlarında bile şüpheli faaliyetleri gerçek zamanlı olarak tespit etmelerini sağlayarak işlem izleme süreçlerinde devrim yaratabilir. Ayrıca, kuantuma dayanıklı kriptografi, gelecekteki siber tehditlere karşı gerekli bir savunma olarak ön plana çıkmaya başlamış ve kuantum bilişimin olgunlaşmasıyla finans kurumlarının güvenliğini artırmayı hedeflemektedir.

Mali suçlarla mücadelede, üretken yapay zekanın iki ucu keskin bir kılıç olduğu kanıtlanmıştır. Bir yandan suçlular, şirket yöneticilerini taklit etmek ve hileli işlemlerde milyonlarca dolar çalmak için kullanılan deepfake'ler oluşturmak gibi amaçlarla üretken yapay zekayı giderek daha fazla kullanıyor. Öte yandan, finans sektörü artık milyonlarca veri noktasını analiz edebilen ve dolandırıcılık faaliyetlerini büyümeden önce belirleyip durdurabilen yapay zeka odaklı dolandırıcılık tespit araçları kullanıyor. Yapay zeka ve makine öğreniminin tahmine dayalı analitikle entegrasyonu, kurumların potansiyel tehditleri ortaya çıkmadan önce tespit etmesini sağlayarak suçluların güvenlik açıklarından yararlanma fırsat penceresini azaltıyor.

Ayrıca, yüz tanıma ve parmak izi tarama gibi biyometrik kimlik doğrulama teknolojileri, hassas finansal sistemlere yetkisiz erişimi önlemek için 2024 yılında yaygın olarak benimsenmektedir. Bu teknolojiler, son yıllarda artış gösteren kimlik hırsızlığı ve hesap ele geçirmeleri gibi yaygın finansal suç türlerinin önlenmesinde özellikle değerlidir. Finans kuruluşları, biyometrik verileri müşteri doğrulama süreçlerine entegre ederek, bir işlemi başlatan kişinin gerçek hesap sahibi olduğundan emin olabilirler.

2025'e baktığımızda, mali suçları önleme ortamının teknoloji tarafından şekillendirilmeye devam edeceği açıktır. Ancak dijital platformlara olan güvenin artması, siber suç riskini de artırmakta ve kurumların daha da gelişmiş güvenlik önlemleri almasını gerektirmektedir. Yapay zeka odaklı dolandırıcılık tespitinden blockchain destekli şeffaflığa kadar bu teknolojilerin evrimi, uyumluluğun geleceğini şekillendirmede etkili olacaktır. Bu yeniliklerden yararlanan finansal kurumlar, mali suçların artan karmaşıklığını karşılamak ve küresel finansal sistemin bütünlüğünü sağlamak için daha donanımlı hale gelecektir.

Sonuç olarak, teknoloji artık isteğe bağlı bir araç değil, mali suçlara karşı devam eden savaşta bir gereklilik haline gelmiştir. 2024'ün yenilikleri, yapay zeka, blockchain, RPA ve diğer gelişmekte olan teknolojilerin dolandırıcılık, kara para aklama ve terör finansmanını önlemede değil, aynı zamanda tüm uyum çerçevesini dönüştürmede de etkili olduğunu göstermiştir.

Kripto Para Birimi ve Ötesi: Mali Suçların Yeni Sınırı

Kripto Para Birimi ve Ötesi: Mali Suçların Yeni Sınırı

Kripto para ve mali suçların kesişimi hızla gelişiyor ve dijital varlık alanı hem inovasyon hem de istismar için dinamik bir sınır olmaya devam ediyor. Kripto para birimleri, merkeziyetsiz finans (DeFi), NFT'ler ve sınır ötesi işlemlerde önemli ilerlemeler vaat ederken, bu yenilikler aynı zamanda önemli düzenleme ve uyum zorluklarını da beraberinde getiriyor. Nisan 2024 itibarıyla, **13.656 adet** kripto para birimi bulunuyor. Özellikle Bitcoin, **1,7 trilyon doların üzerinde** bir piyasa değeri ve **154,61 milyar dolarlık** 24 saatlik işlem hacmi ile dikkat çekiyor.

Dijital para birimlerinin sağladığı faydalar önemli olsa da bu ekosistemdeki yasa dışı faaliyetlerin kapsamı da aynı derecede geniş. Yüksek profilli skandallar, gelişen düzenleyici çerçeveler ve dolandırıcılık taktiklerinin sürekli artan karmaşıklığı, dijital varlık ekosisteminde mali suçlarla mücadelenin ileri görüşlü ve çok yönlü çözümler gerektirdiğini ortaya koyuyor.

2024 yılı itibarıyla **13.656 adet** kripto para birimi bulunuyor

Kripto Suçları

2024 yılında kripto suçları, suçluların blockchainnin merkezi olmayan ve sahte doğasından yararlanarak tespit edilmekten kaçınmalarıyla daha da karmaşık hale gelmiştir. Bitcoin, Ethereum ve diğer dijital varlıklar halka açık defterler aracılığıyla bir şeffaflık sağlasa da, suçlular bu platformları kara para aklama, dolandırıcılık, fidye yazılımı saldırıları ve yasa dışı ticaret gibi çeşitli mali suçlar işlemek için kullanmaktadır.

Yükselen Kripto Suç Trendleri

En son yayımlanan Kripto Suç Raporu, kripto alanındaki suç faaliyetlerinin artan ölçeğini vurgulamakta ve 2023 yılında bir önceki yıla göre %40'lık bir artışla **20 milyar dolarlık** yasa dışı işlem gerçekleştiğini ortaya koymaktadır. Suçlular, DeFi platformları ve diğer blockchain tabanlı sistemlerdeki güvenlik açıklarından yararlanma konusunda ustalaşmıştır. Özellikle DeFi hack'leri ve istismarları, yalnızca 2023'te merkezi olmayan borsalar aracılığıyla aklanan **9 milyar dolardan fazla** para ile bu artışın başlıca itici gücü olmuştur. Bu platformlar, anonimlik sunduğundan ve aracılar olmadan çalıştığından, kara para aklama ve diğer yasa dışı faaliyetler için verimli bir zemin oluşturmaktadır.

2024'te en hızlı büyüyen kripto suç alanlarından biri de fidye yazılımı kullanımıdır. Suç grupları, tespit ve kovuşturmadan kaçınmak amacıyla Bitcoin ve diğer kripto para birimlerinde giderek daha fazla fidye ödemesi talep etmektedir. Son raporlara göre, bilgisayar korsanları sağlık, finans ve devlet altyapısı gibi kritik sektörleri hedef alarak kripto cinsinden fidye ödemelerini küresel olarak 1,4 milyar dolara yükseltmiştir. Ayrıca, suçlular işlem geçmişlerini gizleyen ve düzenleyicilerin yasa dışı fonların izini sürmesini zorlaştıran Monero ve Zcash gibi gizlilik paralarından yararlanmaktadır.

Ek olarak, kripto ATM'leri de AML çerçevelerinde önemli bir zayıf nokta olarak ortaya çıkmıştır. Suçlular, uygun kimlik kontrolleri olmaksızın fiat para birimlerini kripto paralara dönüştürmek için bu ATM'leri kullanmaktadır. 2024 yılı itibarıyla dünya genelinde **40.000'den fazla** kripto ATM'si faaliyet göstermektedir ve bunların çoğu şüpheli faaliyetler ile ilişkilendirilmiştir. Kolluk kuvvetleri, bu ATM'lerdeki işlemlerin **%70'ine** kadarının uyuşturucu kaçakçılığı ve kara para aklama gibi suç faaliyetleriyle bağlantılı olduğunu bildirmektedir.

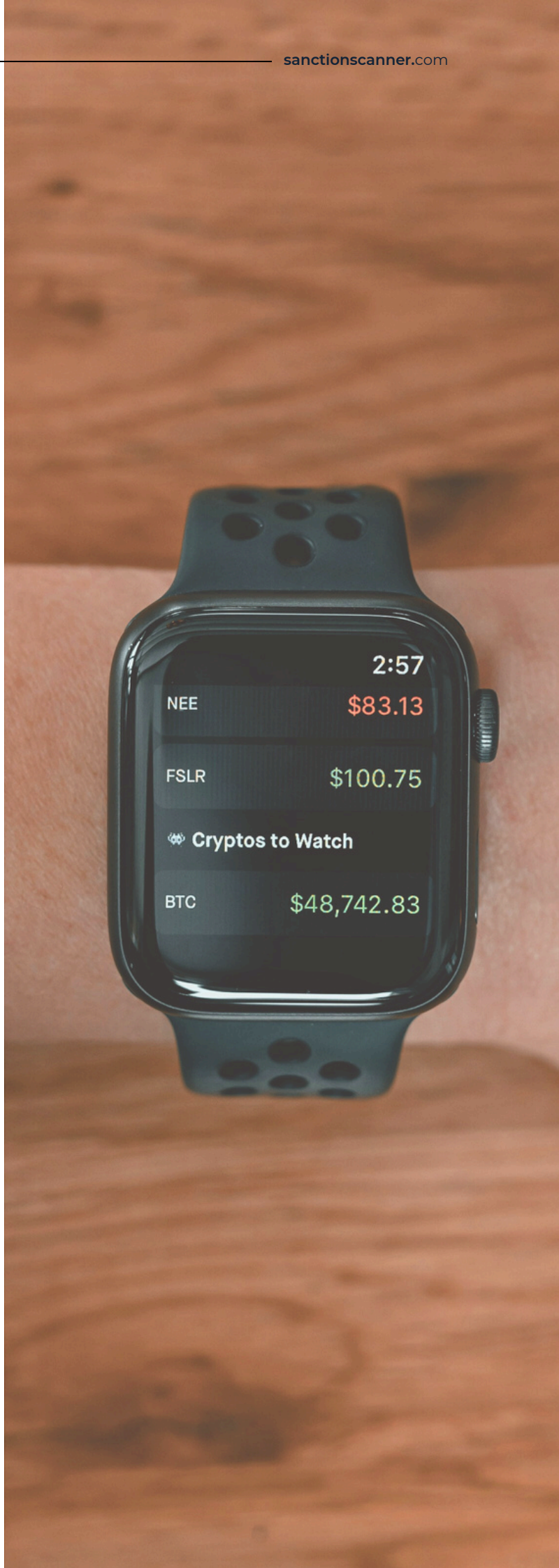
Kripto sektöründe
2023 yılında
20 milyar dolarlık
yasa dışı işlem
gerçekleşmiştir.

Kripto Alanında Dolandırıcılık

Kripto para piyasasındaki dolandırıcılık, 2024 yılı itibarıyla endişe verici seviyelere ulaşmış durumdadır. Yapılan araştırmalara göre, kripto yatırımcılarının %57'si para kazanırken, %14'ü kayıplarını bildirmiş ve yalnızca %7'si önemli ölçüde kâr elde ettiğini düşünmektedir. Bu eşitsizlik, hem yeni hem de deneyimli yatırımcıları hedef alan dolandırıcılıkların artışına zemin hazırlamıştır.

Kripto dünyasında dolandırıcılar tarafından en çok kullanılan taktikler arasında Ponzi planları, kimlik avı saldırıları ve halı çekme (geliştiricilerin fon topladıktan sonra ortadan kaybolması) bulunmaktadır. 2023 yılında bu dolandırıcılık türlerinin kurbanları yaklaşık **3,6 milyar dolar** kaybetmiştir. Bu rakamın, sahte video ve ses taklitleri yoluyla yatırımcıları hedef alan sofistike deepfake saldırılarının da artmasıyla 2024'te daha da yükselebileceği öngörülmektedir.

Kripto ekosisteminde büyüyen bir başka tehdit ise, APP dolandırıcılığıdır. Bu dolandırıcılık türünde, suçlular kurbanları kandırarak, genellikle iş e-postası kimlik avı (BEC) saldırıları yoluyla kontrolleri altındaki hesaplara büyük miktarlarda kripto para aktarmalarını sağlamaktadır. Aldatma süreci basit ancak son derece etkilidir; dolandırıcı, meşru bir işletme veya alacaklı gibi davranarak kurbanı, blockchain işlemlerinin değişmez doğasını koz olarak kullanarak tersine çevrilmesi zor olan ödemeler yapmaya ikna eder. 2023 yılında APP dolandırıcılığından kaynaklanan kayıplar küresel olarak **6,7 milyar dolara** ulaşmış olup, suçlular bu tekniklerde daha da usta hale geldikçe bu rakamın artması beklenmektedir.



Terörizmin Finansmanı ve Dark Web Piyasaları

Terör örgütleri, dijital para birimlerinin sınır tanımayan doğasından faydalanarak operasyonlarını finanse etmek için giderek daha fazla kripto para birimlerine yöneliyor. İstihbarat raporlarına göre, 2024 yılında **100 milyon doların üzerinde** kripto işlemi terör finansmanıyla ilişkilendirildi. Bu işlemler genellikle blockchain analitik araçları tarafından tespit edilmekten kaçınmak amacıyla tasarlanmış daha küçük, artan ödemeleri içeriyor.

Dark web piyasalarının yükselişi, kripto para karşılığında silah, uyuşturucu ve yasa dışı hizmetlerin satışını kolaylaştırarak bu faaliyetleri engelleme çabalarını daha da karmaşık hale getirmiştir. Yalnızca 2023 yılında, dark web işlemleri yasa dışı kripto işlemlerinin toplamında **1,2 milyar doların üzerinde** bir paya sahipti.

Blockchain Analitiğinin Rolü

Kripto suçlarının artan karmaşıklığına rağmen, kolluk kuvvetleri ve finans kurumları, çalınan fonların izini sürmek ve kurtarmak için blockchain analitiği ve OSINT kullanma konusunda önemli adımlar attı. Bu araçlar, araştırmacıların birden fazla cüzdan ve platformdaki kripto para akışını takip etmelerine ve suç operasyonlarındaki kilit oyuncuları belirlemelerine olanak tanır. 2024 yılında, bu teknolojilerin kullanımı çalınan varlıkların **1,2 milyar dolardan fazlasının** kurtarılmasına yardımcı olarak sektör için kritik bir kazanç sağladı. Sanction Scanner gibi şirketler, yasa dışı işlemlerin gerçek zamanlı takibini sağlayan sofistike araçlar geliştirerek bu çabaların ön saflarında yer alıyor.

Ancak, blockchain analitiği şüpheli faaliyetleri belirleyebilse de, mevzuat boşlukları önemli bir zorluk olmaya devam etmektedir. Kripto paranın küresel benimsenme oranı %4,2'dir ve dünya genelinde **420 milyondan fazla** kullanıcı bulunmaktadır. Benimsenme artmaya devam ettikçe, dijital varlıkların yarattığı benzersiz riskleri ele almak için kapsamlı düzenleyici çerçevelere duyulan ihtiyaç da artmaktadır. Birçok ülke henüz merkezi olmayan platformlar için sağlam KYC ve AML düzenlemelerini uygulamaya koymamıştır. Bu durum, suçlulara nispeten cezasız bir şekilde faaliyet gösterebilecekleri yeni fırsatlar sunmaktadır.

Dijital Varlıklara Yönelik Düzenleyici Yaklaşımlar

Kripto para piyasası, 2024 itibariyle **%4,2'lik** küresel benimsenme oranıyla hızlı büyümesini sürdürürken, dünyanın dört bir yanındaki düzenleyiciler dijital varlıkların ortaya çıkardığı yeni zorluklara ayak uydurmaya çalışıyor. Bitcoin, 2024 yılında **1,3 trilyon dolarlık** şaşırtıcı piyasa değeriyle baskın oyuncu olmaya devam ederken, DeFi ve NFT'ler de önemli ölçüde büyümeyi sürdürüyor. Ancak, bu dijital yeniliklerin yükselişi, küresel finansal sistemlerin bütünlüğünü tehdit eden güvenlik açıklarını da ortaya çıkarmış ve düzenleyicilerin daha kapsamlı düzenlemeler geliştirmesine yol açmıştır.

ABD ve Küresel Çerçeveler

ABD hükümeti, kripto para biriminin yükselişine yanıt vermede öncü bir rol üstlendi. 2024 yılının başlarında, ABD Menkul Kıymetler ve Borsa Komisyonu (SEC), dijital varlık piyasalarında şeffaflığı artırmayı ve dolandırıcılığı azaltmayı amaçlayan güncellenmiş yönergeleri uygulamaya koydu. SEC, özellikle ilk madeni para arzlarında (ICO'lar) kullanılan tokenlar olmak üzere çeşitli kripto para birimlerini menkul kıymet olarak sınıflandırarak bunları geleneksel finansal araçlarla aynı düzenlemelere tabi tutma kararı aldı. Bu hamle, kripto sektöründe giderek artan saadet zinciri ve hileli yatırım projelerini engellemeyi hedefliyor.

Buna paralel olarak, Emtia Vadeli İşlemler Ticaret Komisyonu (CFTC), kripto türevleri ticaret platformları üzerindeki denetimini artırarak borsaların mevcut finansal düzenlemelere uymasını sağladı.

FinCEN ise, kripto borsalarına ve cüzdan sağlayıcılarına daha sıkı AML gereklilikleri getirerek daha titiz KYC prosedürlerini zorunlu kıldı. FinCEN'in kuralları, 2024'ten itibaren borsaların 10.000 doların üzerindeki tüm işlemleri rapor etmesini ve uyumsuzluk için ağır para cezaları uygulamasını gerektirmektedir.

Küresel ölçekte, FATF, sanal varlık hizmet sağlayıcılarının (VASP'ler) belirli bir eşiğin üzerindeki kripto işlemlerinde katılımcıların kimlikleri hakkında bilgi toplamasını ve paylaşmasını gerektiren "Seyahat Kuralı" yetkisini şekillendirmeye devam ediyor. 2024 yılı itibarıyla, 50'den fazla ülke, yasa dışı kripto para akışlarının izlenmesinde küresel iş birliğini güçlendirmek amacıyla bu kuralı ya uygulamış ya da uygulama sürecindedir.

AB'de 2023'te **500 milyar dolarlık** stabilcoin işlemi gerçekleşti.

AB'nin MiCA ve Diğer Küresel Girişimleri

Avrupa'da, Kripto Varlık Piyasaları (MiCA) düzenlemesi, dijital varlıklar için en kapsamlı düzenleyici çerçevelerden biri olarak öne çıkıyor. 2023 yılında onaylanan ve 2024 ortasına kadar tam olarak uygulanması planlanan MiCA, Avrupa Birliği genelinde kripto varlıkları için birleşik bir yasal çerçeve oluşturmayı hedefliyor. Bu düzenlemenin hükümleri arasında kripto ihraççıları için şeffaflık gereklilikleri, sabit paralar için sermaye gereklilikleri ve tüketici koruma önlemleri yer alıyor. Ayrıca, MiCA'nın farklı kripto varlık türlerine ilişkin net tanımlar sunması, sektörde faaliyet gösteren işletmeler için düzenleyici belirsizliği azaltıyor.

MiCA'nın önemli etkilerinden biri, sınır ötesi ödemeler ve havaleler için artan kullanımları göz önüne alındığında, stabilcoinlere odaklanması olacaktır. Bu düzenleme, stabilcoin ihraç edenlerin yeterli rezerv tutmasını ve sıkı operasyonel ile şeffaflık standartlarına uymasını sağlamayı amaçlıyor. Sadece AB'de 2023 yılında 500 milyar dolarlık stabilcoin işlemi gerçekleştiği ve bu rakamın 2024'te keskin bir şekilde artacağı tahmin edildiğinde, bu önlem tam zamanında alınmış bir adım olarak değerlendiriliyor.

Diğer taraftan, Singapur, dijital varlıklar için ileriye dönük bir düzenleyici ortamın nasıl oluşturulacağına dair öncü bir örnek haline geldi. Singapur Para Otoritesi (MAS), 2024 yılında yalnızca AML ve CFT önlemlerini geliştirmekle kalmayıp aynı zamanda blockchain ve kripto sektörlerinde inovasyonu teşvik eden yeni kurallar getirdi. Bu hassas denge, çok sayıda kripto girişimini Singapur'a çekerek, ülkenin blockchain teknolojisi için küresel bir merkez olma rolünü daha da pekiştirdi.

DeFi Alanında Düzenleme

2024'te 26,1 milyar dolarlık bir TVL ile büyümesi öngörülen DeFi, benzersiz düzenleyici zorluklar ortaya koyuyor. Tasarım gereği, DeFi platformları aracılara ihtiyaç duymadan çalışmakta ve işlemleri kolaylaştırmak için otomatik akıllı sözleşmelere güvenmektedir. Bu durum, düzenleyici makamların kendilerini sorumlu tutacak merkezi bir otorite olmadığında uyumluluğu nasıl sağlayabileceklerine dair soruları gündeme getiriyor.

Bu endişeleri gidermek amacıyla, Avrupa Bankacılık Otoritesi (EBA) gibi çeşitli düzenleyici kurumlar, DeFi'yi mevcut düzenleyici çerçevelere dahil etmenin yollarını araştırıyor. Öneriler arasında, DeFi platformlarının programlanabilir uyumluluğu uygulamasını zorunlu kılmak bulunuyor. Bu sayede akıllı sözleşmeler, işlemleri gerçekleştirmeden önce KYC ve AML kurallarını otomatik olarak uygulayabilecektir. Henüz erken aşamalarda olmasına rağmen, bu tür önlemler DeFi platformlarının kara para aklama ve terör finansmanı gibi yasa dışı faaliyetler için kullanılma riskini azaltmaya yardımcı olabilir.

DeFi'nin
26,1 milyar dolarlık
bir TVL ile büyümesi
öngörülüyor

Küresel Koordinasyon ve Kripto Düzenlemesi

Kripto paraların küresel niteliği, farklı yetki alanlarındaki düzenleyicilerin eşgüdümlü çabalarını gerektirmektedir. 2024 yılında Uluslararası Para Fonu (IMF) ve Dünya Bankası, özellikle gelişmekte olan piyasalara odaklanarak dijital varlıklar için standartlaştırılmış bir düzenleyici çerçeve oluşturmak üzere ortak bir girişim başlattı. Nijerya ve El Salvador gibi ülkelerin Bitcoin'i yasal bir ödeme aracı veya finansal sistemlerinin önemli bir parçası olarak benimsemesi, bu bölgelerde kripto para kullanımının hızla yaygınlaşmasına katkı sağlamıştır. Ancak, bu bölgelerde uyum regülasyonu eksikliği, onları kripto suçlarına karşı daha duyarlı hale getirdi.

Şeffaflığı teşvik etmek amacıyla hem IMF hem de Dünya Bankası, sınır ötesi büyük kripto işlemlerini takip edebilen ve izleyebilen gerçek zamanlı işlem izleme sistemlerinin uygulanmasını savunuyor. Bu çabalar, büyük ölçekli kara para aklama planlarını önlemeyi ve kripto para birimleri aracılığıyla yasa dışı fon akışını engellemeyi amaçlamaktadır.

Sektöre Özgü Mali Suçlar Mercek Altında

Sektöre Özgü Mali Suçlar Mercek Altında

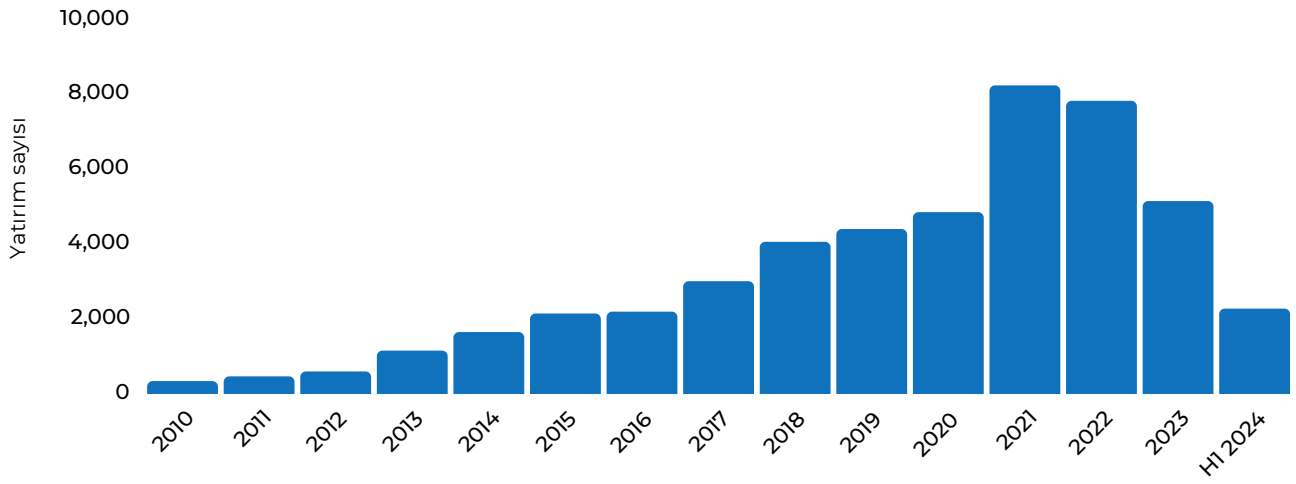
Sektöre özgü mali suçlar küresel piyasaları zorlamaya devam etmekte, her sektör kendi kırılganlıkları ve gelişen tehditleriyle karşı karşıya kalmaktadır. Bazı sektörler finansal suçluların artan karmaşıklığına adapte olurken, diğerleri finansal ekosistemlerini korumak için gerekli sağlam önlemleri almakta hala gecikiyor.

Finansal Hizmetler ve Bankacılık

2024 itibariyle dünya genelinde **30.000'den fazla** FinTech'in faaliyet gösterdiği finansal hizmetler sektörü, hem geleneksel dolandırıcılık hem de dijital bankacılık alanında ortaya çıkan tehditler nedeniyle artan zorluklarla karşı karşıya. Çevrim içi bankaların, özellikle Avrupa'daki rekabetçi ortamda popülaritesi artarken, Afrika gibi bölgeler bu gelişmenin gerisinde kalmaktadır. Dijital bankacılığa geçiş, müşterilerin mobil bankacılık ve dijital cüzdanlara olan güvenlerinin artmasıyla birlikte, yeni dolandırıcılık risklerini de beraberinde getirmiştir.

Endişe verici trendlerden biri, dolandırıcıların çalıntı ve yanlış bilgilerin bir karışımını kullanarak sahte kimlikler oluşturduğu sentetik kimlik dolandırıcılığının yükselişidir. 2024 yılı itibarıyla ABD'deki teminatsız kredi portföylerindeki tahsilatların %10-15'ini temsil eden bu tür dolandırıcılıklar, kimlik avı saldırıları ve veri ihlalleri ile beslenen hesap ele geçirme dolandırıcılığının da artmasına yol açmıştır; bu dolandırıcılıklar sonucunda küresel kayıpların bu yıl **25 milyar doları aşması** beklenmektedir.

2010'dan 2024'ün ilk yarısına kadar dünya genelinde fintech alanında yapılan yatırımların sayısı.



Kaynak: statista.com

Bir diğer önemli tehdit, özellikle İngiltere gibi bölgelerde **%82** oranında artış gösteren temassız ödeme dolandırıcılığıdır. Dijital ödemelerin artışıyla dolandırıcılar, NFC teknolojisindeki açıklardan faydalanarak yetkisiz işlemler gerçekleştirmektedir.

Bu teknolojilerin dolandırıcılık tespitini önemli ölçüde geliştirmesiyle birlikte, düzenleyiciler de mali suçlarla mücadele çabalarını artırmıştır. Avrupa Birliği'nin AMLD düzenlemesi, bankaların CDD uygulamalarını daha fazla incelemeye alarak, daha sıkı KYC protokolleri ve finansal işlemlerde daha fazla şeffaflık gerektirmiştir. ABD'de, 2024 yılında yürürlüğe giren FinCEN Gerçek Sahiplik Kuralı, suçluların yasa dışı fonları gizlemek için paravan şirketler kullanmasını önlemek amacıyla finansal kurumların şirketlerin gerçek sahipleri hakkında bilgi toplamasını ve doğrulamasını zorunlu kılmaktadır.

Teknolojik gelişmeler ve sıkı düzenlemelerle desteklenen finansal hizmetlerin evrimi, sektörde dolandırıcılıkla mücadele yaklaşımını yeniden şekillendiriyor.

Fintech'lerin ve çevrim içi bankaların yükselişiyle birlikte, finans kuruluşları, faaliyetlerini tehdit eden ve giderek karmaşıklaşan dolandırıcılık planlarının önüne geçmek için tetikte olmalı ve yenilik yapmaya devam etmelidir.

> Finans kurumları, şüpheli faaliyetleri daha iyi tespit etmek ve yanlış pozitifleri azaltmak için yapay zeka destekli izleme sistemlerini benimsiyor. Mevzuat değişikliklerine ayak uydurmak için yüksek riskli müşteriler için gelişmiş durum tespiti ve çevik uyum çerçeveleri uygulanmaktadır. Bu önlemler, işlem izlemenin doğruluğunu, risk tabanlı müşteri kabulünü ve yeni küresel yaptırımlara daha hızlı adaptasyonu iyileştirmeyi amaçlamaktadır.

Vivek Mishra
AML/KYC Professional

Sigortacılık

Sigorta sektörü, küresel operasyonların artan karmaşıklığı ve dijital dönüşüm sürecinin hızlanması nedeniyle dolandırıcılıktan kara para aklamaya kadar birçok mali suç riskiyle karşı karşıya kalmaktadır. Sigorta dolandırıcılığı, yıllık 80 milyar doları aşan küresel kayıplarla en önemli endişe kaynağı olmayı sürdürürken, kara para aklama gibi diğer suçlar, uyum çerçevelerindeki zayıflıklar ve dijitalleşmeden faydalanarak bu sektöre giderek daha fazla sızmaktadır.

Sigorta dolandırıcılığı, sahte talepler, düzenlenmiş kazalar ve prim saptırması gibi çeşitli biçimlerde uzun süredir var olan bir sorundur. 2023 yılında motor sigortası dolandırıcılığı, küresel dolandırıcılık taleplerinin %59'unu oluştururken, ortalama dolandırıcılık talebinin değeri 15.000 dolar olarak kaydedilmiştir. Sektör, poliçe sahibinin yanlış beyanı ve sağlık hizmet sağlayıcılarının sahte faturalar göndererek veya hizmet maliyetlerini şişirerek gerçekleştirdiği sağlayıcı dolandırıcılığı gibi sorunlarla da başa çıkmaktadır. Sigortacılıkta dolandırıcılık tespiti gelişim gösterse de, dolandırıcılar dijital platformlardan ve çevrim içi uygulamaların sağladığı görece anonimlikten yararlanmaya devam etmektedir.

Sigorta dolandırıcılığından kaynaklı kayıplar yıllık **80 milyar doları** aşıyor.

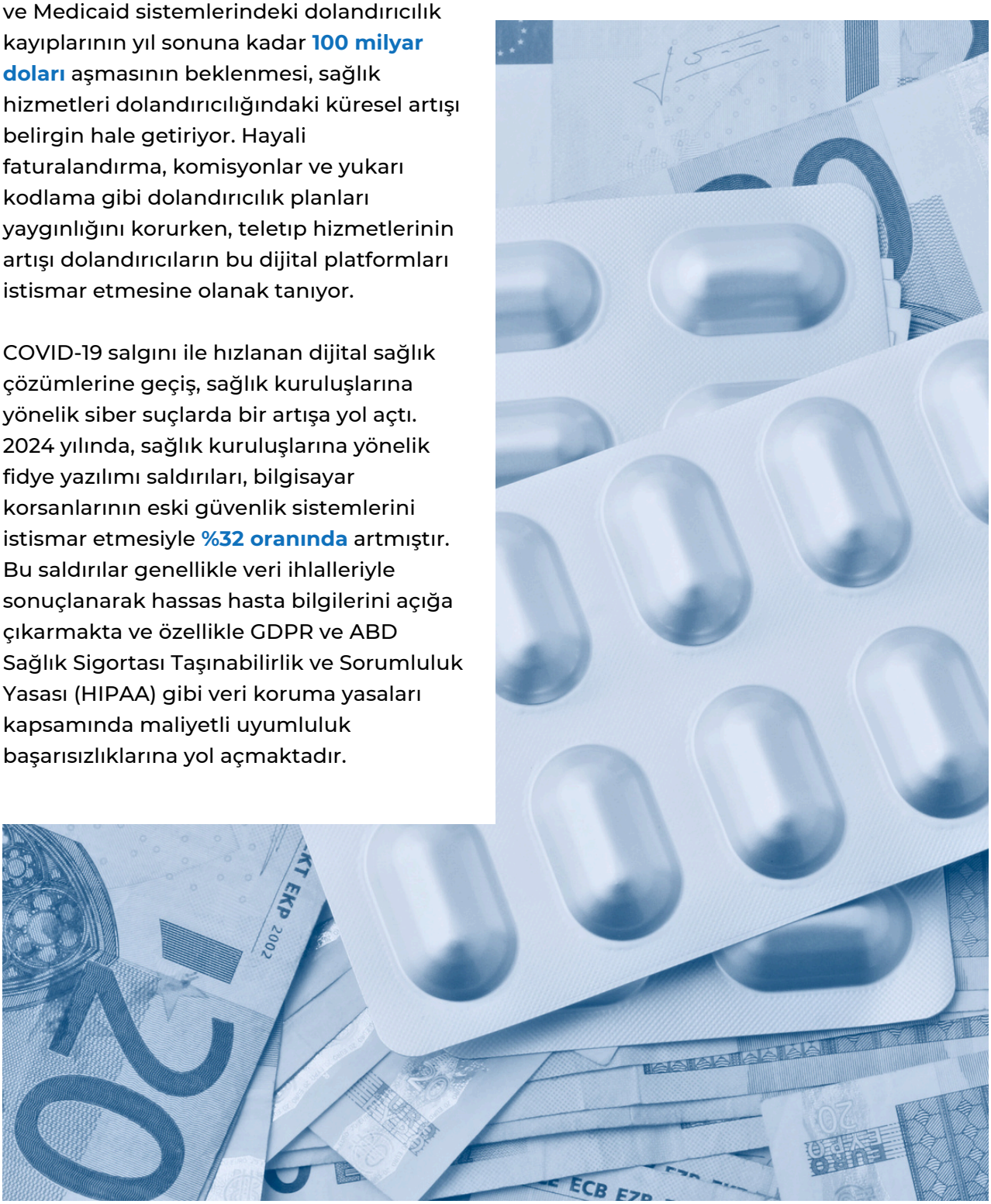
Kara para aklama, özellikle yasa dışı mali faaliyetler için daha az incelenen yollar olarak görülen hayat sigortası poliçeleri ve reasürans düzenlemeleri aracılığıyla sigorta şirketleri için önemli bir sorun haline gelmiştir. Suçlular, yüksek değerli sigorta ürünleri satın alarak, bunları zamanından önce iptal edebilir ve ardından meşru fonlar gibi görünen geri ödemeler alabilirler. Sigorta sektörü, işlemlerin büyüklüğü ve yasa dışı fonların kaynaklarını gizleme kabiliyeti nedeniyle bu tür dolandırıcılık planları için cazip bir hedef haline gelmektedir.

Sağlık Hizmetleri

2024 yılında sağlık sektörü, tıbbi kuruluşların yönettiği büyük miktarda hassas veri nedeniyle dolandırıcılık ve siber saldırılar açısından birincil hedef olmaya devam ediyor. Özellikle ABD'de Medicare ve Medicaid sistemlerindeki dolandırıcılık kayıplarının yıl sonuna kadar **100 milyar doları** aşmasının beklenmesi, sağlık hizmetleri dolandırıcılığındaki küresel artışı belirgin hale getiriyor. Hayali faturalandırma, komisyonlar ve yukarı kodlama gibi dolandırıcılık planları yaygınlığını korurken, teletıp hizmetlerinin artışı dolandırıcıların bu dijital platformları istismar etmesine olanak tanıyor.

COVID-19 salgını ile hızlanan dijital sağlık çözümlerine geçiş, sağlık kuruluşlarına yönelik siber suçlarda bir artışa yol açtı. 2024 yılında, sağlık kuruluşlarına yönelik fidye yazılımı saldırıları, bilgisayar korsanlarının eski güvenlik sistemlerini istismar etmesiyle **%32 oranında** artmıştır. Bu saldırılar genellikle veri ihlalleriyle sonuçlanarak hassas hasta bilgilerini açığa çıkarmakta ve özellikle GDPR ve ABD Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) gibi veri koruma yasaları kapsamında maliyetli uyumluluk başarısızlıklarına yol açmaktadır.

Sonuç olarak, düzenleyici kurumlar, sağlık hizmeti sağlayıcıları üzerinde zorunlu şifreleme, çok faktörlü kimlik doğrulama ve dijital altyapıların sürekli izlenmesi gibi siber güvenlik savunmalarını güçlendirmek için baskıyı artırmaktadır.



Gayrimenkul

Gayrimenkul sektörü, kara para aklama faaliyetleri için en cazip yollardan biri olmaya devam etmektedir. Suçlular, özellikle emlak piyasalarının şeffaf olmadığı ve düzenleyici gözetimin sınırlı olduğu bölgelerde, yasa dışı fonları aklamak amacıyla gayrimenkul alımlarını bir araç olarak kullanmaya devam ediyor. FinCEN'in 2024 yılında bildirdiğine göre, şüpheli gayrimenkul işlemlerinde kayda değer bir artış gözlemlenmiş; yalnızca ABD'de lüks emlak yatırımlarıyla ilgili kara para aklama faaliyetlerinde **%15'lik bir artış** yaşanmıştır. Sorun, özellikle Miami, Los Angeles ve New York gibi yüksek değerli gayrimenkul işlemlerinin genellikle anonim paravan şirketler aracılığıyla gerçekleştirildiği pazarlarda daha ciddi boyutlara ulaşmaktadır.

Küresel düzeyde, FATF, emlak işlemlerinde şeffaflığı artırmak için tavsiyelerini sıkılaştırarak hükümetleri emlakçılardan ve tapu şirketlerinden daha titiz raporlama talep etmeye zorlamaktadır.

Avrupa Birliği ise AMLD6 kapsamında, 10.000 Avro üzerindeki gayrimenkul işlemleri için daha sıkı KYC gereklilikleri getirerek, yüksek değerli mülk transferlerinde yer alan tarafların daha sıkı bir incelemeye tabi tutulmasını sağlamıştır.

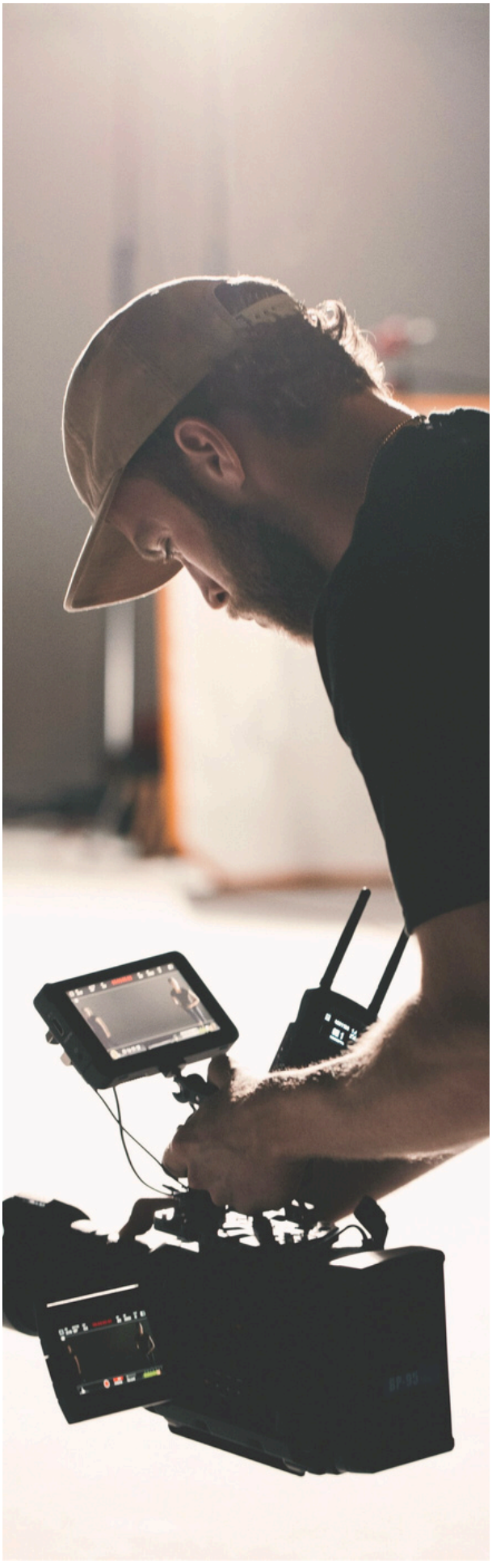
Kara para aklama faaliyetlerinin yanı sıra, gayrimenkul yatırım dolandırıcılığı da 2024 yılında, özellikle hızlı büyüme gösteren pazarlarda artış göstermiştir. Dolandırıcılar, sahte yatırım fırsatları yaratarak veya mülk değerlemelerini manipüle ederek konut patlamasını istismar etmiş ve yatırımcılar için önemli mali kayıplara yol açmıştır. Bu yıl, hileli gayrimenkul yatırım planları nedeniyle küresel olarak tahmini **6,4 milyar dolar** kaybedildiği belirtiliyor; bu durum, sektörde daha güçlü gözetim ihtiyacını bir kez daha gözler önüne sermektedir.

Enerji Sektörü

Enerji sektörü, özellikle petrol ve gaz alanında, yolsuzluk, rüşvet ve kara para aklama gibi risklerin ön planda olduğu mali suçlar için uzun zamandır önemli bir merkez olmuştur. 2024 yılı itibarıyla, yeşil enerji yatırımlarının yükselişi, sektörün daha sürdürülebilir enerji çözümlerine geçişiyle birlikte yeni mali suç risklerini de beraberinde getirmiştir. Suçlular, hileli yeşil tahviller oluşturarak ve karbon kredi piyasalarını manipüle ederek, yenilenebilir enerji projelerine yapılan yatırım akışından yararlanmaktadır.

Ayrıca, ABD Adalet Bakanlığı (DOJ) ve İngiltere'deki Serious Fraud Office (SFO) gibi düzenleyici kurumlar, enerji sektöründeki yolsuzluk ve rüşvetle daha fazla odaklanmaya başlamıştır. 2024'te dikkat çeken bir dava, Batı Afrika'daki sözleşmelerin güvence altına alınmasıyla ilgili rüşvet suçlamaları nedeniyle 1,2 milyar dolar para cezasına çarptırılan çok uluslu bir enerji şirketini içermektedir. Bu tür yüksek profilli davalar, sektördeki devam eden riskleri ve mali suçların kovuşturulmasında uluslararası iş birliğinin artan rolünü vurgulamaktadır.

Yenilenebilir enerjiye geçiş, aynı zamanda yeşil enerji projelerine bağlı yatırım dolandırıcılığında da bir artışa neden olmuştur. Dolandırıcılar, sürdürülebilir yatırımlara yönelik artan talebi istismar ederek yatırımcıları çekmek için hayali yeşil enerji girişimleri oluşturmuşlardır. Hükümetler karbon nötrlüğü için baskı yapmaya devam ettikçe, düzenleyici kurumların dolandırıcılığı ve finansal kötü yönetimi önlemek için yeşil enerji projelerine yönelik yeni uyum gereklilikleri getirmesi beklenmektedir.



Eğlence Sektörü

Eğlence sektörü, çeşitli alanları etkileyen mali suç dalgasına karşı bağışıklık kazanamamıştır. 2024 yılı itibarıyla, sektör, özellikle film, müzik ve oyun alanlarında fikri mülkiyet (IP) hırsızlığında kayda değer bir artış yaşamıştır. Dolandırıcılar, içerik korsanlığı yapmak için sofistike yöntemler kullanarak sektöre yalnızca bu yıl tahmini **20 milyar dolar** gelir kaybına yol açmıştır. Dijital platformlar, özellikle yayın hizmetleri sunanlar, hacklenmeye karşı savunmasız kalmakta ve bu da premium içeriğe yetkisiz erişim ile abonelik dolandırıcılığına neden olmaktadır.

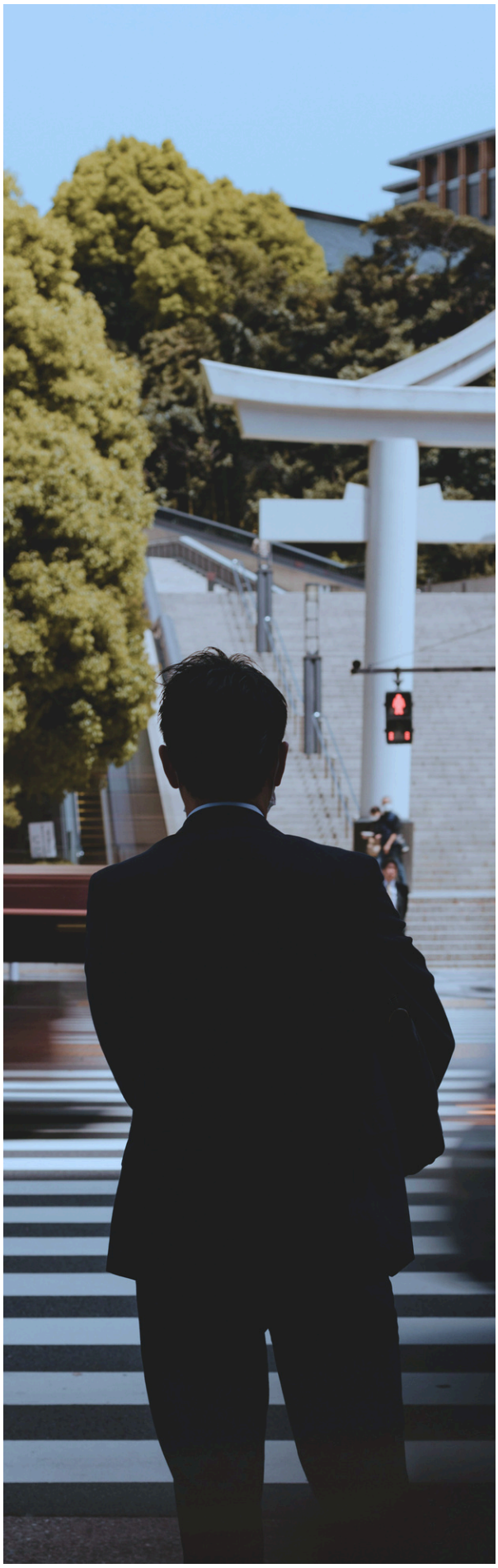
Ayrıca, 2024 yılında ünlülerin reklam dolandırıcılıkları da artış göstermiştir. Dolandırıcılar, tanınmış kişileri taklit ederek özellikle kripto para alanında sahte yatırım planlarını desteklemekte, bu dolandırıcılıklar sosyal medya aracılığıyla reklamı yapılan hileli planların kurbanı olan hayranlar ve yatırımcılar için önemli mali kayıplara yol açmaktadır.

Bu sorunlara karşılık olarak, Sinema Filmleri Derneği (MPA) ve diğer eğlence kuruluşları, daha etkili korsanlıkla mücadele önlemleri geliştirmek ve abonelik tabanlı hizmetlerde dolandırıcılığı önlemek için teknoloji firmalarıyla yakın iş birliği yapmaktadır. Dijital Haklar Yönetimi (DRM) sistemlerini güçlendirmek ve içerik sahipliğini takip etmek için blockchain teknolojisini kullanmak, fikri mülkiyet haklarının korunmasında öncelikli bir hedef haline gelmiştir.

İçerik korsanlığı sektöre bu yıl **20 milyar dolar** kaybettirdi.

2025 İçin Stratejik Yol Haritası

2025 İçin Stratejik Yol Haritası



Mali suçlar gelişmeye devam ettikçe, kurumların yalnızca mevcut zorluklarla başa çıkmakla kalmayıp, gelecekteki tehditleri de öngörerek ileri görüşlü stratejilerle donatılması gerekmektedir. 2025 yılına geldiğimizde, hızlı teknolojik gelişmeler, mevzuat değişiklikleri ve giderek daha sofistike hale gelen suç taktikleri bir araya gelerek mali suçların önlenmesine dair oluşacak senaryoyu şekillendirecektir.

Yapay zeka, blockchain inovasyonları ve diğer ileri teknolojilerin benimsenmesi, finansal sistemlerin korunmasında kritik bir öneme sahip olacak. Bu teknolojiler, dolandırıcılığı tespit etme ve önleme, veri analitiği sağlama ve uyum süreçlerini güçlendirme gibi alanlarda önemli katkılar sunacaktır. Ayrıca, sınır ötesi işbirliği ve mevzuat uyumu, hem geleneksel hem de yeni ortaya çıkan finansal suç türleriyle etkili bir şekilde mücadele etmede çok önemli roller üstlenecektir.

Dijital ekonominin genişlemesiyle birlikte, onu korumak için kullanılan araçlar ve yaklaşımlar da sürekli olarak gelişmelidir. Finansal kurumlar, uyum çerçevelerini adapte etmeli, teknolojik yeteneklerini geliştirmeli ve gelişen risklere karşı tetikte olmalıdır.
Bu yol haritası, finansal suçların önlenmesinin geleceğini şekillendirecek temel stratejileri ve yenilikleri özetlemekte ve kurumları önümüzdeki yıllarda daha dirençli ve güvenli operasyonlara yönlendirmektedir.

Gerçek Zamanlı Finansal Suç Tespiti için Yapay Zekanın Uyarlanması

2025 yılına gelindiğinde, yapay zeka ve makine öğreniminin mali suçlarla mücadeledeki etkinliği, finans kuruluşlarının bu teknolojileri daha spesifik ve etkili bir şekilde kullanma yeteneğine bağlı olacaktır. Dolandırıcılık tespiti için yapay zeka zaten yaygın bir şekilde kullanılmakta, ancak kara para aklama ve terör finansmanı konusundaki kalıpların belirlenmesindeki rolü daha da rafine hale gelecektir. Bu geçiş, yapay zeka sistemlerinin yalnızca şüpheli faaliyetleri işaretlemekle kalmayıp, aynı zamanda hangi işlemlerin mali suça yol açma olasılığının daha yüksek olduğunu tahmin eden gerçek zamanlı risk değerlendirmeleri sağlamasıyla, reaktif modellerden öngörücü modellere geçişin önemini artıracaktır.

Finans kuruluşlarının 2025 yılında karşılaşacağı en önemli zorluklardan biri, yapay zekanın eski sistemlere entegrasyonudur. Birçok kurum, gerçek zamanlı yapay zeka işlemlerini desteklemeyen eski altyapıya güvenmeye devam etmektedir. Ancak, önde gelen kuruluşların hibrit yapay zeka mimarilerine yatırım yaparak eski sistemlerle birlikte çalışabilen çözümler geliştirdiği ve aynı zamanda sorunsuz gerçek zamanlı uyumluluk izleme sağladığı tahmin edilmektedir. Uzmanlar, akıllı otomasyonun bu boşluğu doldurmakta önemli bir rol oynayacağını, rutin uyumluluk görevlerini otomatikleştirmek için yapay zeka odaklı iş akışlarını kullanarak soruşturma yeteneklerini de geliştireceğini öngörmektedir.

Buna ek olarak, 2025 yılına kadar yapay zeka tabanlı OSINT araçlarının, kripto ticaret platformları ve eşler arası finansal ağlar gibi merkezi olmayan ortamlarda ortaya çıkan suç ağlarını ve yasa dışı faaliyetleri belirlemede kritik bir araç olarak yaygın bir şekilde benimsenmesi beklenmektedir. OSINT araçları, sosyal medya platformlarını, dark web forumlarını ve şifreli iletişim kanallarını izlemek için özel olarak tasarlanacak ve finansal kurumlara ölçeklenebilir ve uyarlanabilir proaktif tehdit istihbaratı sağlayacaktır.

> Yapay zeka ve makine öğrenimi, veri modellerini analiz ederek ve dolandırıcılık tespitini güçlendirerek mali suçları önlemede kritik bir rol oynamaktadır. Blockchain analitiği, yasadışı fonların takibini kolaylaştıran izlenebilirlik sunarken, iris ve yüz tanıma gibi biyometrik kimlik doğrulama teknolojileri güvenliği artırarak dolandırıcılığı önlemeye katkıda bulunuyor. Henüz gelişme aşamasında olan kuantum bilişim ise, şifrelenmiş suç ağlarını çözme potansiyeline sahip. Bu teknolojiler, gelecekte mali suçlarla mücadelede kilit bir rol oynayacaktır.

Vivek Mishra
AML/KYC Professional

Blockchain'in Kurumsal Şeffaflık ve AML Uyumluluğundaki Rolü

2025 yılına gelindiğinde, blockchain teknolojisinin AML uyumluluğundaki rolü, yalnızca değişmez işlem kayıtları sunmaktan çok daha öteye geçecek. Gerçek yenilik, birden fazla finans kurumunun işlem verilerini güvenli bir şekilde ve gerçek zamanlı olarak paylaşmasına olanak tanıyan sınır ötesi blockchain ağları şeklinde ortaya çıkacak.

> Risk tabanlı yaklaşımı temel alan bir AML Programı, kripto sektöründeki değişimlere karşı hızlı ve dikkatli bir tepki verebilmelidir. Mevzuat değişikliklerini düzenli olarak takip etmek için bir KOBİ ekip üyeniz veya bir üçüncü taraf sağlayıcınız var mı? Bu tür bir proaktif izleme, yeni tehditleri ve gelişen riskleri önceden belirlemek açısından önemlidir. Tarama ve izleme hizmeti sağlayıcılarınızla iş birliği yaparak ihtiyaç duyduğunuz güncel verileri elde edebilir, böylece uyumluluk stratejinizi hızla uyarlayabilirsiniz. KOBİ'lerinizi de bu sürece dahil ederek verilerin analizine katkıda bulunmalarını sağlamak, savunma hattınızı güçlendirecektir.
>
> 
>
> **Mario M. Duron**
> Chief Compliance Officer

Bu merkezi olmayan ve şeffaf uyumluluk sistemlerine geçiş, kurumların kırmızı bayraklara daha hızlı yanıt vermesini ve kendilerine özgü kimlik doğrulama mekanizmalarını kullanarak KYC işlemlerini kolaylaştırmasını sağlayacak.

DeFi platformları, suçluların bu sistemleri kara para aklama ve terör finansmanı amacıyla kullanma çabalarıyla birlikte, 2025 yılında benzersiz zorluklar sunmaya devam edecek. DeFi'yi yöneten düzenleyici çerçevelerin, finans kuruluşlarının DeFi ekosistemlerinde TVL verilerini gerçek zamanlı olarak izleyebilen gelişmiş analitik araçları benimsemesini zorunlu kılması bekleniyor. Bu yetenek, şüpheli işlemlere yönelik daha ayrıntılı bir inceleme düzeyi sağlayacak ve eşler arası borsalar ile gözetim dışı cüzdanların artmasıyla yasa dışı fonların izini sürme çabalarını daha karmaşık hale getirecektir.

Ayrıca, 2025 yılına kadar AML uyumluluğu için akıllı sözleşmelerin uygulanmasında önemli bir büyüme öngörülmektedir. Bu durum, kurumların uyumluluk kurallarını doğrudan işlem akışına yerleştirmesine olanak tanıyacak.
Akıllı sözleşmeler, uyumluluk standartlarını karşılamayan herhangi bir işlemi otomatik olarak işaretleyerek veya durdurarak, işlem sonrası soruşturmalara olan ihtiyacı azaltacaktır. Böylece, hem güvenlik hem de verimlilik açısından büyük bir iyileşme sağlanacaktır.

Düzenleyici Değişiklikler ve Küresel Koordinasyon

Finansal suçların önlenmesine yönelik küresel düzenleyici çerçeveler 2025 yılında da gelişmeye devam edecek ve özellikle finansal suç risklerinin yüksek olduğu bölgelerde düzenleyiciler ile finansal kurumlar arasında daha fazla iş birliğine odaklanacaktır. RegTech çözümleri, uyum departmanlarına daha entegre hale gelecek ve kurumların değişen bölgesel düzenlemelerle uyumlu kalmasını sağlamak için otomatik araçlar sunacaktır. Özellikle, FATF ve diğer uluslararası kuruluşların, hem geleneksel bankacılık sistemlerini hem de hızla gelişen dijital varlık ekosistemlerini barındıran standartlaştırılmış çerçeveler için baskı yapması beklenmektedir.

Kripto para alanında, 2025 yılında kripto ile ilgili mali suçlarla mücadele etmek için sınır ötesi düzenleyici işbirliğinin daha fazla uygulandığını göreceğiz. Hükümetler, kripto borsalarından, özellikle yasa dışı faaliyetlerin tespit edilmesinin zor olabileceği merkezi olmayan özerk kuruluşlar ve merkezi olmayan finansal uygulamalar kolaylaştıranlardan daha fazla şeffaflık talep edecektir. Düzenleyici kum havuzları, özellikle gelişmekte olan dijital para birimlerinin bulunduğu bölgelerde, yenilikçi uyum teknolojilerini test etmek için yaygın hale gelecektir.

Ayrıca, neobankalar ve FinTech'ler para transferleri ve ACH (Automated Clearing House) ödemeleri sırasında dolandırıcılığı önlemede zorluklarla karşılaşmaya devam ettikçe, geçici kredi düzenlemeleri sıkılaştırılacaktır. Bu kurumlar, fonlar tamamen ödenmeden önce geçici kredi risklerini yönetmek için yapay zeka ve blockchain ile entegre edilmiş gerçek zamanlı dolandırıcılık tespit sistemlerini giderek daha fazla arayacaklardır.

Kripto Para Ekosisteminde Mali Suçlarla Mücadele

Dijital varlıklar gelişmeye devam ettikçe, kripto para sektöründeki mali suçlar, kurumların merkezi olmayan ağları izleyen ve takip eden özel araçlar benimsemesini zorunlu hale getirecektir. Kripto para istihbarat platformları, özellikle suçluların hareketlerini gizlemek amacıyla yasa dışı faaliyetleri birden fazla zincir arasında giderek daha fazla kaydırmasıyla, karmaşık zincirler boyunca para izlerini takip etmede etkili olacaktır. Bu platformlar, finansal kurumların, riskli işlemleri ve bağlantılı varlık akışlarını daha iyi tespit etmelerini sağlayacak.

2025 yılında, stablecoinlerin yükselişi, AML uyumluluğu için ek zorluklar yaratması beklenmektedir. Genellikle itibari para birimlerine sabitlenen stablecoinler, merkezi olmayan piyasalarda likidite sağlamakta ve sıklıkla sınır ötesi işlemlerde kullanılmaktadır. Ancak bu durum, kara para aklamada "smurfing" ve "katmanlama" teknikleri için güvenlik açıkları yaratmaktadır. Özellikle, küçük miktarlarda para akışlarının birden fazla işlemde dağılması, izlenmeyi zorlaştırmakta ve dolayısıyla düzenleyicilerin bu işlemleri tespit etmesini güçleştirmektedir.

Bu riskleri azaltmak için, finansal kurumların yalnızca bireysel stablecoin işlemlerini değil, aynı zamanda birden fazla varlık sınıfındaki fon akışını da izleyebilen ve en opak ortamlarda bile AML düzenlemelerine uyumu sağlayan yapay zeka sistemlerini kullanmaları gerekecektir.

2025'te Siber Dayanıklılığın Güçlendirilmesi

Finansal hizmetler sektörünün giderek dijitalleşmesiyle birlikte, siber suçlar en önemli tehditlerden biri olmaya devam edecektir. 2025 yılında, finans kuruluşlarının siber dayanıklılıklarını artırmak için zero-trust güvenlik modelleri ve çok katmanlı şifreleme protokolleri uygulamaları gerekecektir. Bu gelişmiş güvenlik çerçevelerinin, kullanıcı davranışlarındaki anormallikleri tespit edebilen ve kurumun saldırıları önleme yeteneğini daha da artıran davranışsal analitiklerle entegre edilmesi önemlidir.

Ayrıca, deepfake ve ses kopyalama teknolojisinin sürekli gelişimi, sosyal mühendislik saldırıları için artan riskler sunmaktadır. Bu tür saldırılara karşı koyabilmek için finans kurumları, dijital kanallarda kullanıcı kimliğini doğrulamak ve dolandırıcılık olasılığını azaltmak amacıyla biyometrik güvenlik sistemlerine ve ses tanıma teknolojilerine yatırım yapmalıdır. Biyometrik doğrulama, kullanıcıların kimliklerini doğrulamanın yanı sıra, kötü niyetli kişilerin bu sistemleri aşmasını da zorlaştıracaktır. Üretken yapay zeka sistemleri, bu saldırılara karşı gerçek zamanlı savunmalar oluşturabilme yeteneği sayesinde, siber suç ağlarının artan karmaşıklığına karşı koymada önemli bir rol oynayacaktır.

Finans kuruluşları, siber dayanıklılık için zero-trust güvenlik modelleri ve çok katmanlı şifreleme uygulamalıdır.

Gelişen Teknolojiler ve Finansal Suçlar Üzerindeki Etkileri

Bugünden bakıldığında, kuantum bilişimin işlem izleme ve kriptografik analizde sağladığı benzeri görülmemiş hız, finansal suçların önlenmesi ortamını temelden yeniden şekillendirme potansiyeline sahiptir. Henüz başlangıç aşamasında olsa da, kuantum bilişim finans kurumlarına mevcut yapay zeka ve blockchain sistemlerinin hızını ve ölçeğini aşan gerçek zamanlı yetenekler sunarak suçla mücadelede devrim yaratabilir.

> İyi düşünülmüş bir risk değerlendirmesi, sürdürülebilir bir AML programının temelidir. Bu değerlendirme, sektöre, şirkete, hizmetlere ve ürünlere göre uyarlanmalıdır; çünkü iki şirket birbirinin aynısı değildir. Karar verin. Bu basit ifade, bir departmanı başarıya ulaştırabilir ya da ürün ve hizmetlerin piyasaya çıkışını geciktirebilir. Karar verememe durumu oldukça yaygındır ve yüksek riskli sektörlerde bu durum daha da karmaşık hale gelebilir. Yavaş ilerlemek bazen faydalı olabilir, ancak odak ve dikkatin kaybolmasına yol açarak gözden kaçan risklere neden olabilir. Kararınıza sahip çıkmak, ekibinizin güvenini kazandırabilir ve düzenleyicilere sorumluluk almaya hazır olduğunuzu gösterebilir.
>
> 
>
> **Mario M. Duron**
> Chief Compliance Officer

Bunun yanı sıra, dijital ikiz teknolojisinin kullanımının uyumluluk testi için gelişmiş simülasyon ortamları sağlaması beklenmektedir. Kurumlar, finansal sistemlerin sanal modellerini oluşturarak, güvenlik açıklarını suçlular tarafından istismar edilmeden önce tespit edebilir ve bu sistemlerin gerçek dünyadaki benzerlerini saldırılara karşı güçlendirebilir.

Öte yandan, OSINT ve yapay zeka tabanlı tehdit istihbarat platformlarının entegrasyonu, 2025 yılında finansal suç tespitinde kritik bir rol oynamaya devam edecektir. Kurumlar, OSINT'ten faydalanarak sosyal medya, derin web forumları ve diğer açık platformlar gibi çeşitli kaynaklardan veri toplayabilecek ve ortaya çıkan tehditleri gerçekleşmeden çok önce tespit etmek için gerekli proaktif istihbaratı sağlayabileceklerdir.

Sonuç olarak, finansal kurumların mali suçlarla mücadele etmek için daha uzmanlaşmış ve proaktif yaklaşımlar benimsemesi kritik bir ihtiyaç haline gelmiştir. Gelişmiş yapay zeka ve blockchain inovasyonlarından, gelişmiş düzenleyici iş birliğine ve siber esneklik önlemlerinin yükselişine kadar, finansal suçların önlenmesinin geleceği, suçlular tarafından kullanılan sofistike yöntemlere karşı çeviklik, teknolojik yatırım ve küresel koordinasyon gerektirecektir. Bu yeni trendleri ve teknolojileri benimseyen kurumlar, karmaşık ve hızla gelişen finansal suç ortamında en iyi şekilde konumlanacaklardır.

Türkiye’de Finansal Suçlar ve Uyumluluk

Türkiye’de Finansal Suçlar ve Uyumluluk

Türkiye, jeopolitik konumu itibarıyla Asya, Avrupa ve Orta Doğu’nun kesişim noktasında yer alarak, küresel ticaret ve finansal hareketler açısından stratejik bir öneme sahiptir. Bu merkezi konum, Türkiye’yi hem fırsatların hem de risklerin merkezine yerleştiriyor. Son yıllarda, dijital dönüşüm ve kripto varlıkların yaygınlaşması gibi dinamiklerle birlikte, finansal suçlar ve AML ile CFT alanlarında artan zorluklar gözlemleniyor. Türkiye, bu zorluklarla mücadele ederken aynı zamanda uluslararası uyum standartlarına ayak uydurarak finansal sistemini daha şeffaf ve güvenilir hale getirme çabasında.

Türkiye’nin Gri Listeden Çıkması

Türkiye, Ekim 2021'de FATF tarafından kara para aklama ve terörizmin finansmanıyla mücadelede yetersizlikler nedeniyle gri listeye alınmıştı. Bu durum, Türkiye'nin uluslararası finansal piyasalar üzerindeki itibarını zedeleyerek, doğrudan yabancı yatırım girişlerinde azalma riskini ve uluslararası bankacılık ilişkilerinde ek denetim ve maliyetler yaratma olasılığını beraberinde getirdi. Gri listede olmak, ülkenin ekonomik büyümesi ve finansal sisteminin istikrarı açısından ciddi sonuçlar doğurabilecek bir risk olarak değerlendirildi.

Türkiye'nin gri listeden çıkma süreci, aynı zamanda ülke ekonomisinin birçok farklı sektörünü doğrudan etkilemiş durumda. Özellikle bankacılık, finans ve gayrimenkul gibi yabancı yatırımlara bağımlı olan sektörlerde olumlu yansımalar bekleniyor. Gri listeye alındığı dönemde, özellikle doğrudan yabancı yatırımlarda yaşanan yavaşlama ve uluslararası kredi değerlendirme kuruluşlarının Türkiye’nin kredi notu üzerinde yaptığı olumsuz değerlendirmeler, finansman maliyetlerini artırmıştı.

Bu durum, özellikle büyük altyapı projelerinde, enerji sektöründe ve diğer sermaye yoğun sektörlerde önemli bir zorluk yaratmıştı.

2024 yılı itibarıyla Türkiye, FATF'nin talep ettiği reformları tamamlamaya ve bu alandaki uluslararası normlara uyum sağlamaya devam ediyor. Bu süreçte Türkiye’nin önemli odak noktalarından biri de finansal sektördeki risk odaklı denetim mekanizmalarının daha da güçlendirilmesi oldu. Özellikle kara para aklama ve terörizmin finansmanıyla mücadelede yeni dijital teknolojilerin kullanılması ve finansal teknolojilere yönelik regülasyonların genişletilmesi, Türkiye’nin bu alanda attığı adımlar arasında yer alıyor. FinTech şirketlerinin artan sayısı ve dijital bankacılığın hızla gelişmesi, yeni risklerin ortaya çıkmasına neden olurken, Türkiye'nin bu alanlara odaklanarak denetim kapasitesini artırması ve MASAK gibi kurumların dijital suçlarla mücadelede daha etkin hale gelmesi önemli bir gelişme olarak değerlendiriliyor.

Kripto para birimleri gibi dijital varlıkların kullanımında yaşanan artış da Türkiye'nin FATF sürecindeki kritik unsurlardan biri oldu. Kripto varlıkların izlenmesi, kara para aklamanın bu yeni dijital platformlar üzerinden gerçekleşmesinin engellenmesi ve blockchain teknolojilerinin suç faaliyetlerinde kullanılmasına karşı alınan önlemler, Türkiye'nin AML/CFT stratejisinin önemli bir parçasını oluşturdu. Özellikle kripto varlık borsalarına yönelik düzenlemeler, bu platformların şeffaflığı ve kullanıcı kimlik doğrulama süreçlerinin sıkılaştırılması, Türkiye'nin uluslararası normlara uyumunu güçlendiren adımlar arasında sayılıyor.

Ayrıca, Türkiye’nin mali yapısının uluslararası piyasalarla daha uyumlu hale getirilmesi amacıyla yurt içindeki düzenleyici kurumlar arasında iş birliği artırıldı. Bu kapsamda, bankacılık düzenlemeleri ve MASAK ile Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) gibi kurumların finansal suçlarla mücadelede daha koordineli çalışması sağlandı. Uluslararası iş birliği de bu sürecin önemli bir parçası haline geldi. Türkiye, Avrupa Birliği, Birleşmiş Milletler ve diğer uluslararası kuruluşlarla bilgi paylaşımını artırarak sınır ötesi suçların engellenmesinde daha aktif bir rol oynamaya başladı.

Türkiye’nin gri listeden çıkma sürecindeki bir diğer önemli boyut da kamu ve özel sektör iş birliğinin güçlendirilmesiydi. Özellikle finansal hizmetler sektöründeki aktörlerin, kara para aklama ve terörizmin finansmanı konusunda farkındalıklarının artırılması ve şirket içi uyum süreçlerinin sıkılaştırılması, Türkiye’nin mali suçlarla mücadelesinde kilit bir rol oynadı. Şirketler, şüpheli işlem bildirimlerinde bulunma ve KYC prosedürlerini daha etkin bir şekilde uygulayarak, bu sürece katkıda bulundu.

Sonuç olarak, Türkiye’nin FATF gri listesinden çıkma süreci, sadece uluslararası finansal sistemdeki itibarını yeniden kazanmasını değil, aynı zamanda finansal suçlarla mücadeledeki kararlılığını da pekiştirdi. Türkiye, mali suçlar karşısında daha dayanıklı bir yapı inşa ederek, ekonomik büyüme ve yatırım çekme potansiyelini artırmayı hedefliyor. Gri listeden çıkış sürecinin ardından, Türkiye’nin finansal sektöründeki reformların derinleşmesi ve dijital teknolojilerle uyumlu daha güçlü bir regülasyon altyapısı inşa etmesi bekleniyor.

Türkiye'nin Yeni Kripto Varlık Kanunu

2024 yılı, Türkiye’de kripto varlık piyasası açısından önemli bir dönüm noktası oldu. Kripto varlıkların hızlı yükselişi, hükümetin bu alandaki düzenlemeleri sıkılaştırma ihtiyacı hissetmesine neden oldu. Yeni kripto varlık kanunu, Türkiye'nin finansal piyasalarındaki dijital varlık hareketlerini daha güvenli hale getirmeyi ve uluslararası standartlara uygun bir düzenleyici çerçeve oluşturmayı hedefliyor. Bu yasa, hem bireysel yatırımcıları hem de kripto varlık hizmet sağlayıcılarını kapsayacak şekilde geniş bir düzenleme yelpazesine sahip.

Yeni kanun, özellikle kripto borsalarının faaliyetlerini denetlemek, kara para aklama ve terörizmin finansmanı risklerine karşı mücadele etmek amacıyla tasarlandı. Türkiye'de faaliyet gösteren kripto borsalarının ve dijital varlık hizmet sağlayıcılarının lisanslanması zorunlu hale getirildi. Bu düzenleme, sektörde şeffaflık sağlarken, yatırımcıların da daha güvenli bir ortamda işlem yapmasına olanak tanıyor. Borsaların KYC süreçlerini sıkılaştırmaları ve tüm işlemleri detaylı bir şekilde rapor etmeleri gerekiyor. Aynı zamanda, şüpheli işlem bildirimleri konusunda MASAK ile yakın iş birliği içinde çalışmaları zorunlu kılınıyor.

Yeni kanun kapsamında, kripto varlıkların vergilendirilmesi konusu da ele alındı. Yatırımcıların kazançlarının belirli bir eşiği aşması durumunda, elde ettikleri gelirlerin vergilendirilmesi öngörülüyor. Bu durum, dijital varlıkların geleneksel finansal araçlarla aynı muameleye tabi tutulmasını sağlarken, kayıt dışı ekonomiyi engellemeyi ve devlete vergi geliri sağlamayı amaçlıyor.

Kripto varlıkların kara para aklama ve terörizmin finansmanında kullanılma potansiyeli, Türkiye'nin uluslararası düzenleyici standartlara uyum sürecinde önemli bir tehdit olarak görülüyor. Yeni kanun, bu riskleri minimize etmek için borsaların ve diğer kripto varlık hizmet sağlayıcılarının daha katı denetimlere tabi tutulmasını öngörüyor. Özellikle yüksek hacimli işlemler ve sınır ötesi para transferleri, daha detaylı inceleme süreçlerine tabi olacak. Bu çerçevede, kripto varlık işlemlerinin izlenmesi ve şüpheli aktivitelerin raporlanması gibi önlemler, MASAK'ın ve diğer düzenleyici kurumların denetiminde daha etkin bir şekilde uygulanacak.

2024 itibarıyla, kripto varlık kanunu ile birlikte Türkiye'nin finansal sistemi, hem iç pazarda hem de uluslararası arenada güven kazanmayı hedefliyor. Türkiye'nin, bu kanunla birlikte FATF'nin belirlediği uluslararası standartlara daha uyumlu hale gelmesi ve gri liste riskinden uzaklaşması amaçlanıyor. Ayrıca, bu düzenlemeler, Türkiye'nin fintech ekosistemine de olumlu katkılar sağlayarak, kripto varlık hizmet sağlayıcılarının ve dijital finans şirketlerinin daha güvenli ve şeffaf bir ortamda faaliyet göstermesine olanak tanıyor.

Son olarak, yeni kanun, tüketiciyi koruma önlemlerini de artırmayı amaçlıyor. Yatırımcıların bilinçlendirilmesi ve dolandırıcılıklara karşı korunması için eğitim ve bilgilendirme kampanyaları başlatıldı. Türkiye'nin kripto varlık kanunu, sektördeki belirsizlikleri gidermeyi ve bu yeni finansal araçların düzenlenmiş, güvenilir bir çerçevede işlem görmesini sağlamayı hedefliyor.

Ne yazık ki, merkeziyetsiz platformlar aracılığıyla dolandırıcılıkları, suç gelirlerinin sisteme sokulmasını veya kullanıcıların vergi yükümlülüklerini gizlemesini tamamen önlemek mümkün değil.

Ancak, Türkiye'de kripto paralara yönelik yapılan son düzenlemelerin, özellikle bu platformların Sermaye Piyasası Kurulu'nun düzenlemelerine tabi tutulacak olması, Bilgi Sistemleri yükümlülüklerine uyum hedefinin getirilmesi ve KYC yükümlülüğünün devreye sokulması çok önemli ve kritik adımlar.

Bu platformlar daha önce böyle düzenlemelere tabi değilken, Türkiye'de sanki öyleymiş gibi hareket edenler de vardı. Ancak çoğu bilgi sistemlerindeki zayıflıklar ve suistimale açık hizmetleri nedeniyle suç gelirlerinin kaynağı haline geldi ve bu durum, onlarla ortak çalışan düzenlenmiş finansal kurumları da olumsuz etkiledi.

Bu anlamda, 2025 yılının kripto para dünyasında değişim ve dönüşüm yılı olacağını düşünüyorum. Önlerinde kat etmeleri gereken uzun bir yol ve uyum sağlayacakları düzenlemelere evrilmeleri gereken birçok süreç var.

Uyum süreçlerini destekleyecek şekilde eğitimli personel istihdamı, doğru dış destek seçimi ve bilgi sistemlerinin güçlü tasarımı kritik önemde olacak.

Tuba Erdem
Director of Compliance & Internal Control

2023 MASAK Faaliyet Raporu

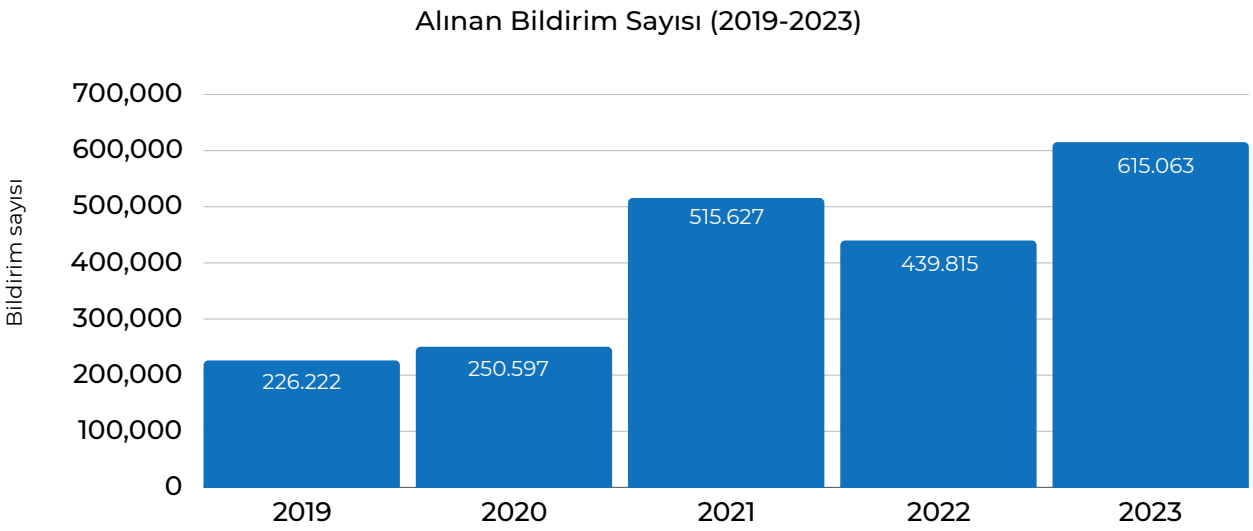
Türkiye'de finansal suçlar ve terörizmin finansmanına karşı mücadele çabalarının merkezinde yer alan Mali Suçları Araştırma Kurulu (MASAK), 2023 yılı boyunca kapsamlı faaliyetlerde bulunmuştur. MASAK, finansal suçlar ve yasa dışı mali hareketlerle mücadelede yürüttüğü analiz çalışmaları, alınan bildirimler, idari yaptırımlar ve şüpheli işlem bildirimleriyle Türkiye'nin mali güvenliğini sağlama misyonunu sürdürmektedir.

2023 yılı faaliyet raporu, MASAK’ın ulusal ve uluslararası düzeydeki finansal suç risklerine karşı aldığı önlemleri ve bu alanda kaydedilen gelişmeleri detaylı bir şekilde gözler önüne sermektedir. Bu yıl alınan tedbirler, risk bazlı denetim süreçlerinin geliştirilmesi, yüksek riskli alanlara yönelik artan odaklanma ve dijital teknolojilerin etkin kullanımını içeriyor.

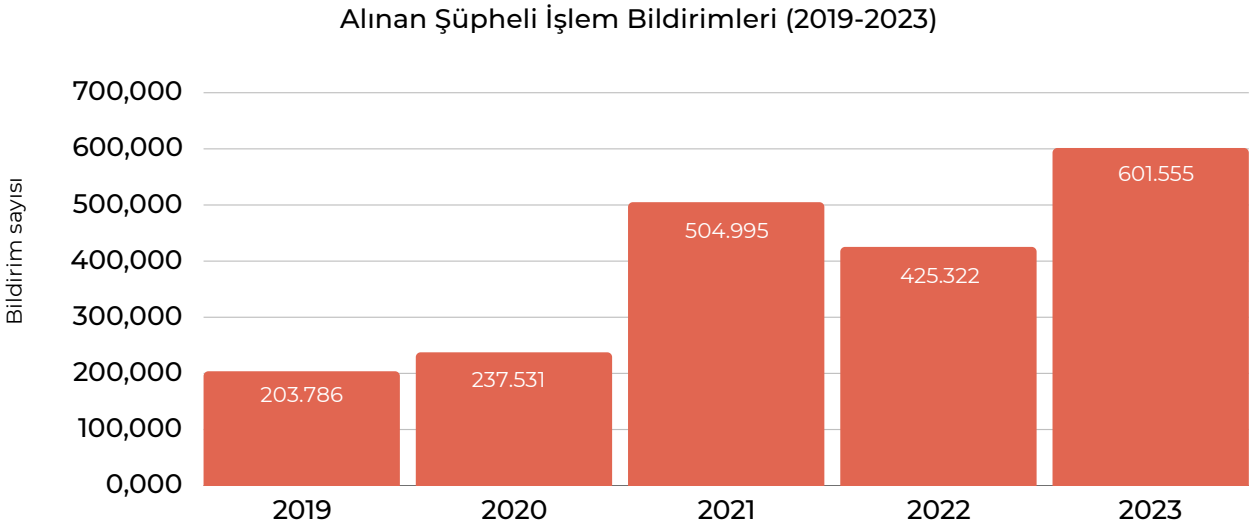
MASAK, 2023 yılında finansal suçlarla mücadele amacıyla kapsamlı bir iş yükünü yönetmiş ve etkin sonuçlar elde etmiştir. Başkanlık, şüpheli işlem bildirimlerinin yanı sıra suç gelirlerinin aklanması ve terörizmin finansmanına yönelik analiz, değerlendirme ve denetim faaliyetlerini artırmıştır. Toplamda 601.555 şüpheli işlem bildirimi alınmış, ayrıca kolluk kuvvetlerinden ve adli makamlardan gelen taleplerle MASAK’ın veri tabanı genişlemiştir. Bu bildirimler çerçevesinde 48.449 kişi hakkında inceleme yapılmış, elde edilen veriler doğrultusunda adli makamlara bilgi sunulmuştur.

Bununla birlikte, MASAK yükümlülüklerini yerine getirmeyen kurumlara yönelik yaptırımlar uygulamış, müşterinin tanınması ve şüpheli işlem bildirim yükümlülüklerine uymayan 415 yükümlü hakkında toplamda 350 milyon TL üzerinde idari para cezası vermiştir. MASAK’ın aldığı bu önlemler, finansal sektördeki suistimal riskini düşürmek ve yükümlülük uyumunu artırmak adına etkili olmuştur.

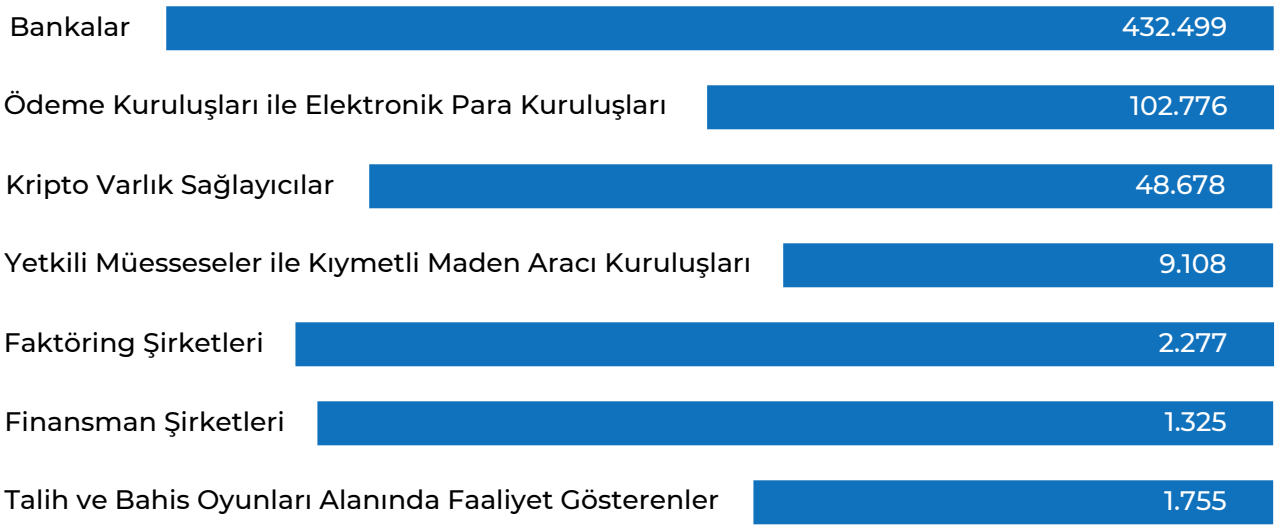
2023 yılında MASAK'a iletilen toplam bildirim sayısı, bir önceki yıla göre %35 oranında artarak 615.063 seviyesine ulaşmıştır. Bu artış, finansal kurumların finansal suçlara karşı giderek daha yüksek bir hassasiyet geliştirdiğini ve bildirim süreçlerinin daha düzenli hale geldiğini göstermektedir.



MASAK'a yapılan şüpheli işlem bildirimleri de 2023 yılında %41 oranında artış göstererek 601.555'e ulaştı. Bu yükseliş, finansal sistemde şüpheli işlemlere yönelik farkındalığın arttığına ve kurumların suç risklerini daha etkili bir şekilde izlediğine işaret etmektedir.

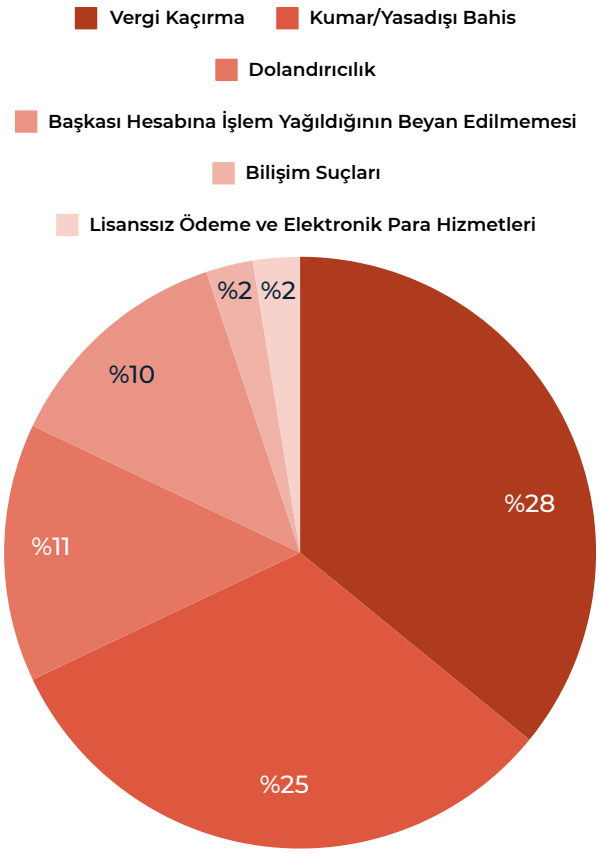


Şüpheli İşlem Bildirim Yapan Yükümlüler



2023 yılında MASAK'a şüpheli işlem bildiriminde bulunan yükümlü sayısı 395'e yükseldi. Farklı sektörlerden gelen yükümlü kuruluşların yaptığı şüpheli işlem bildirimleri, MASAK'ın geniş bir kapsama alanına sahip olduğunu ve çeşitli sektörlerin de bu sürece katkıda bulunduğunu göstermektedir.

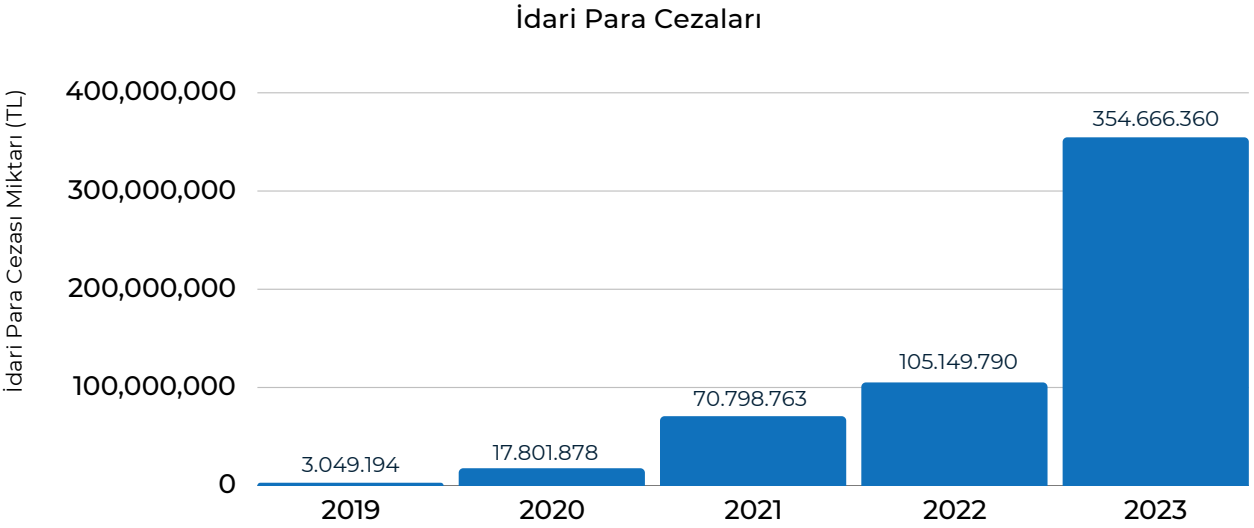
En Fazla Bildirilen Suçlar



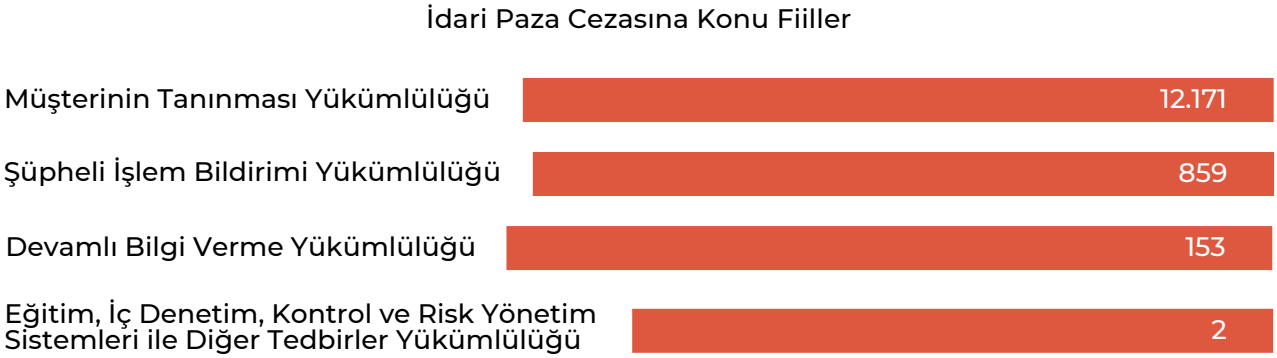
Özellikle ödeme ve elektronik para kuruluşları ile yetkili müesseselerdeki bildirimler dikkat çekiyor. Bu durum, finansal hizmet sağlayıcılarının uyum yükümlülüklerine verdikleri önemin arttığını ve MASAK ile etkili bir işbirliği kurduklarını göstermektedir.

Şüpheli işlem bildirimlerinde en çok rastlanan suç kategorileri, Türkiye'nin finansal suçlarla mücadelesinde hangi alanlara daha fazla odaklanılması gerektiğini gösteriyor. Bildirimler arasında en çok vergi kaçakçılığı, yasa dışı bahis faaliyetleri ve başkası adına işlem yapma gibi suçlara rastlanıyor. Bu suçların sıklıkla raporlanması, finansal sistemde özellikle bu alanlarda ciddi risklerin bulunduğunu ve MASAK'ın bu risklere karşı teyakkuzda olduğunu ortaya koyuyor.

Geçtiğimiz yıl boyunca uygulanan idari para cezaları, finansal kurumların yasal düzenlemelere uyum sağlamasını teşvik eden önemli bir unsur olarak öne çıkıyor. Bu cezalar, finansal kurumların sorumluluklarını yerine getirmesini sağlamak adına etkin bir şekilde kullanılıyor. MASAK, 2023 yılında yükümlülüklerini yerine getirmeyen kuruluşlara toplam 354,6 milyon TL idari para cezası uyguladı.



Bu cezaların büyük bir kısmı, şüpheli işlem bildiriminde bulunmama, kimlik doğrulama yükümlülüklerini ihlal etme ve kayıt tutma gerekliliklerine uymama gibi temel uyum eksikliklerinden kaynaklandı.



Türkiye'nin finansal suçlarla mücadelede attığı adımlar, hem iç hem de dış paydaşlarla iş birliğinin önemini ve uyum süreçlerindeki kararlılığını gözler önüne seriyor. MASAK'ın risk odaklı yaklaşımı, güncellenen düzenlemeler ve artan bildirim oranları, finansal sistemin güvenliğini sağlamada önemli bir ilerleme kaydetmiştir. Kripto varlıklar, kara para aklama ve diğer finansal suçlarla mücadelede Türkiye, küresel standartlara uyumunu güçlendirmekte ve toplumun tüm kesimlerini bilinçlendirme yolunda kararlı adımlar atmaktadır.

Önümüzdeki dönemde uyum süreçlerinin daha da güçlenmesi ve yenilikçi teknolojilerin bu mücadelede etkin bir şekilde kullanılması, Türkiye'nin finansal güvenlik alanında attığı adımları daha da ileriye taşıyacaktır. Bu bağlamda Türkiye, uluslararası finansal sistemde güvenli bir aktör olma yolunda sağlam adımlarla ilerlemeye devam etmektedir.

Geleceğe Hazır İş Ortaklarımız

papara · sipay · Unity · taxfix · NN

AirHelp · CHUBB · Togg · Qwist · APMEX

iyzico · Türk Telekom · OYAK · moldcell · GIG

مشربش للصرافة Musharbash Exchange · golden pay · mondu · GENERALI · my Fatoorah

United Payment · Koç · HangiKredi · NomuPay

payment · midas · bpn · luxaviation

SisalSans · ICRYPEX · EmbaFinans · hepsiburada

Dünya genelinde **60'tan fazla ülkede 500'ü aşkın** kuruluş
uyum süreçlerinde Sanction Scanner'a güveniyor

500 Technology Fast 500 2023 EMEA WINNER Deloitte.

50 Technology Fast 50 2022 TÜRKİYE WINNER Deloitte.

50 Technology Fast 50 2023 TÜRKİYE WINNER Deloitte.

2024 FINCRIMETECH 50

SANCTION SCANNER

Geleceğin çözümleri, bugün sizlerle

info@sanctionscanner.com

sanctionscanner.com

Finansal Suçlara
Karşı Güçlü Bir
Adım Atın,
Aramıza Katılın

SANCTION SCANNER

Yasal Uyarı: Bu belgenin içeriğinin yalnızca bilgilendirme amaçlı olduğunu lütfen unutmayın. Burada sunulan bilgiler hukuki tavsiye olarak yorumlanmamalıdır. Sanction Scanner, sağlanan bilgilerin doğruluğu, eksiksizliği veya güncelliği konusunda hiçbir sorumluluk kabul etmez ve bu bilgilere dayanarak yapılan herhangi bir işlem için tüm sorumluluğu reddeder.

Bu raporda kullanılan kaynak materyallere ilişkin ayrıntılı bilgi için www.sanctionscanner.com adresini ziyaret edebilirsiniz.

SANCTION SCANNER