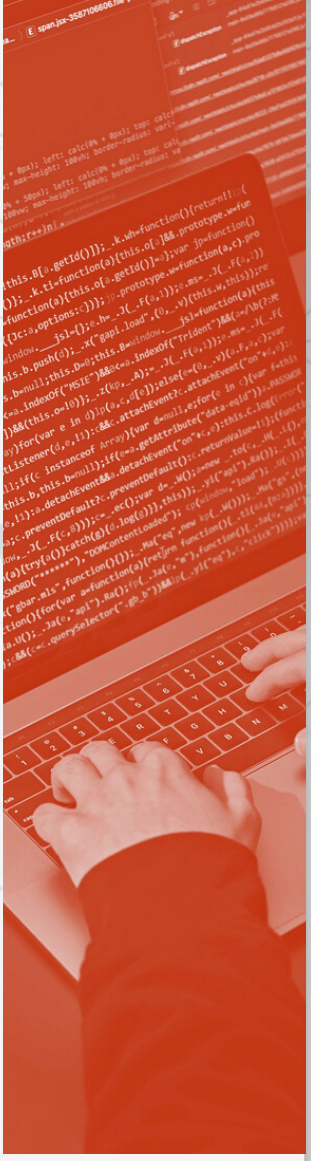
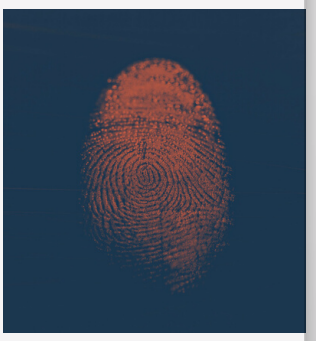




SANCTION SCANNER

2023 AML Endüstrisi:

Gelişen Trendler ve Geleceğe Yönelik Tahminler

2023

İçindekiler

ŞİRKET HAKKINDA

Sanction Scanner, Regülasyon Teknolojileri (RegTech) alanında suç gelirlerinin aklanması ve terörün finansmanını önlemeye yönelik yapay zeka destekli çözümler sağlayan bir teknoloji şirketidir. 220'den fazla ülke ve bölgenin 3000'den fazla yaptırım, izleme listesi ve PEP verisine karşı müşteriler ve işlemler için AML taraması sağlar. Aynı zamanda gerçek zamanlı bir işlem izleme çözümü sunar ve bununla her işlem izlenebilir ve hangisinin şüpheli olduğu tespit edilebilir. Ayrıca bu verileri anlık olarak analiz eder ve kullanıcılarına rapor halinde sunarak 360° risk değerlendirmesi ile hepsi bir arada uyum yaklaşımı sunar.

Bugün, 40'tan fazla ülkede 300'den fazla şirketin mali suçlarla mücadelesinde aktif rol oynuyor ve AML yazılım ürünleri sağlıyoruz. Kullanımı kolay vaka yönetimi arayüzleri, hızlı entegrasyon yaklaşımı ve üst düzey müşteri memnuniyeti ilkemiz ile uyum ve risk ihtiyaçlarını destekliyoruz.

Yönetici Özeti

Suç gelirlerinin aklanması ile mücadelede (AML) finansal sektörlerin 2023 yılında önemli gelişmeler yaşaması bekleniyor. Bu rapor, ilgili alanlarda faaliyet gösteren işletmelerin önümüzdeki yıl dikkat etmesi gereken çeşitli konulara genel bir bakış sağlamak için tasarlanmıştır.

Geçtiğimiz birkaç yıl içinde son yüzyılın en hızlı dijitalleşmesinin yaşanmasının ardından, bugün sektör için en kritik endişe alanları dolandırıcılık ve siber suçlar olarak görülüyor. Bu sorunlar giderek yaygınlaşırken işletmeler için de önemli bir risk oluşturuyor. "e-Ticaretten kazanılan her on dolardan birinin dolandırıcılık yönetimine harcandığı" anketlerle biliniyor. Rapor, işletmelerin bu tehditlere karşı uyanık kalmasının önemini vurguluyor ve 2023'te dikkat edilmesi gereken en yaygın dolandırıcılık ve siber suç türlerinden bazılarına genel bir bakış sunuyor. Burada, sosyal medya dolandırıcılığı, Google Voice dolandırıcılığı, sentetik kimlik dolandırıcılığı, e-ticaret dolandırıcılığı ve vergi dolandırıcılığına dair bir inceleme bulabilirsiniz. Vergi kaçakçılığı sektör için yeni bir konu olmasa da son yıllarda özellikle pandeminin etkisiyle daha yaygın hale geldi. Buna karşın, Kimlik Hırsızlığı Kaynak Merkezi (ITRC) tarafından alınan dolandırıcılık raporlarına göre, 2022'nin ilk yarısında bildirilen etkinliğin %37'sinden fazlası Google Voice tarafında gerçekleştiriliyor.

Orta ölçekli finans kurumlarının, Covid-19'un getirdiği hızlı dijital dönüşüm nedeniyle dolandırıcılık saldırılarına karşı en savunmasız firmalar olduğu uzmanların önemli çıkarımlarından biri olarak raporda yer alıyor. Pandemiden önce, bankalar ve sigorta şirketleri gibi kurumsal firmalar dolandırıcıların birincil hedefiydi. Ancak bu kurumlar yeterli deneyime ve güvenlik sistemlerine sahip. Orta ölçekli firmalar ise dijitale doğru acil bir geçiş ve deneyim eksikliği nedeniyle yeni hedefler haline geldi ve bu durum finansal ve müşteri kayıplarına ve itibar zedelenmesine yol açtı. Dolandırıcılık saldırılarının sayısı ve hacmi, son üç yılda orta ölçekli firmaların daha fazla suç faaliyetiyle karşılaşmasıyla birlikte önemli ölçüde arttı. Kurumsal şirketler hala tehditlerle karşı karşıya, ancak dolandırıcılar için hedefler çoğaldı ve yöntemler daha sofistike hale geldi.

AML endüstrisindeki bir diğer önemli trend olarak rapor, Regtech'lerin mali suçlarla mücadeledeki kritik rolünü vurgulamaktadır. Bu şirketlerin kuruluşların AML gerekliliklerine bağlı kalmalarına yardımcı olan çözümler sunması onları her zamankinden daha önemli endüstri oyuncuları haline getiriyor. Rapor ayrıca, regülasyonlara uyum için işlem izleme (TM) konusunun altını çiziyor. AML sektöründe faaliyet gösteren işletmeler için işlem izlemeye yönelik yazılım çözümleri bir zorunluluk haline geldi. Yine de, uygun olan yazılımı bulma, doğruluk ve maliyet etkinliği gibi belirli zorlukları da beraberinde getiriyor. Bu rapor işlem izlemenin önemini ve yazılım çözümlerinin, düzenlemelere işlemlerin izlenmesi için nasıl verimli ve uygun maliyetli bir yol sağlayabileceğine ışık tutuyor.

Raporda iklim değişikliği ve mali suçlarla ilişkisi de ele alınıyor. Burada konudan en çok etkilenen sektör olan sigortacılığın iklim değişikliği konusunda karşı karşıya olduğu riskler de yer alıyor. 2022 yılı boyunca kuraklık, sel, fırtına, orman yangını ve kasırga gibi çeşitli iklim anomalileri yaşandı. Buna cevaben Avrupa Birliği, sera gazı emisyonlarını 2030'dan önce en az %55 azaltmak amacıyla daha katı düzenlemeler uygulamaya koydu. Ancak bu düzenlemelerin hem AB üye devletlerinin ekonomileri hem de Avrupa ile ilişki kuran kuruluşlar üzerinde önemli etkileri var. İşletmelerin iklim değişikliğinin yarattığı zorluklarla başa çıkmak için proaktif bir yaklaşım benimsemesinin ve etkisini en aza indirmek için çalışmasının ilgili risklere hazırlık için zorunlu olduğu görülüyor. Bu sadece yasal bir yükümlülük değil, aynı zamanda gezegenimizi gelecek nesiller için korumanın ahlaki ve etik bir sorumluluğudur. Ek olarak, bu farkındalığı güçlendirmek ve aynı zamanda sektördeki artan odaklanmanın bir göstergesi olarak raporda çevresel, sosyal ve yönetişim (ESG) konuları inceleniyor.

Rapor, Merkeziyetsiz Finans (DeFi) ve Nitelikli Fikri Tapu'lara (NFT) odaklanarak kripto pazarındaki en son trendleri de inceliyor. DeFi'nin yükselişi, 2021'de yaklaşık %6.600'lük bir büyümeyle, 40 milyar dolarlık toplam kitlenmiş değere ulaşarak beklenmeyen bir gelişme oldu. NFT ise yıllık %27 büyüme oranıyla beklenen ciro ile değerini ve popülaritesini kanıtladı. Bu konu son yıllarda çok popüler olmasına rağmen etkisi azalmadan devam ediyor.

2023 yılının, geçen yıl olduğu gibi AML sektörü için yoğun bir yıl olması bekleniyor. Rus savaşı ve pandemi sonrasının küresel sonuçları sektörü oldukça büyük çapta etkiledi. Bu durumun sonucunda gördük ki işletmelerin sektördeki son gelişmelerden haberdar olması ve riskleri azaltmak için proaktif önlemler alması gerekiyor. Bu rapor, finansal hizmetlerde faaliyet gösteren işletmelerin 2023'te bilmesi gereken temel konulara ilişkin değerli bilgiler sunmak amacıyla okuyuculara sunuluyor.

Dolandırıcılık ve Siber Suç Tehditleri

Online ödeme sahtekarlığının 2020 yılında ABD Federal Ticaret Komisyonu'nun verilerine göre 5,8 milyar dolar olduğu bildirilirken, 2023 yılından 2027 yılına kadar dünya çapında 340 milyar dolar olacağı öngörülüyor.

İstatistiksel sayının resmin tamamı olmadığını hatırlamak önemlidir. Ne yazık ki, bildirilmeyen suç saldırıları nedeniyle gerçek faaliyet bunlardan çok daha fazlasıdır. 2021'de 95.000 kişinin 770 milyon dolar kaybettiğini biliyoruz; ancak bu, kayıplarını bildiren mağdurların yalnızca% 4,8'i.

10%

E-Ticaretten kazanılan her on dolardan biri dolandırıcılığı yönetmek için harcanıyor.

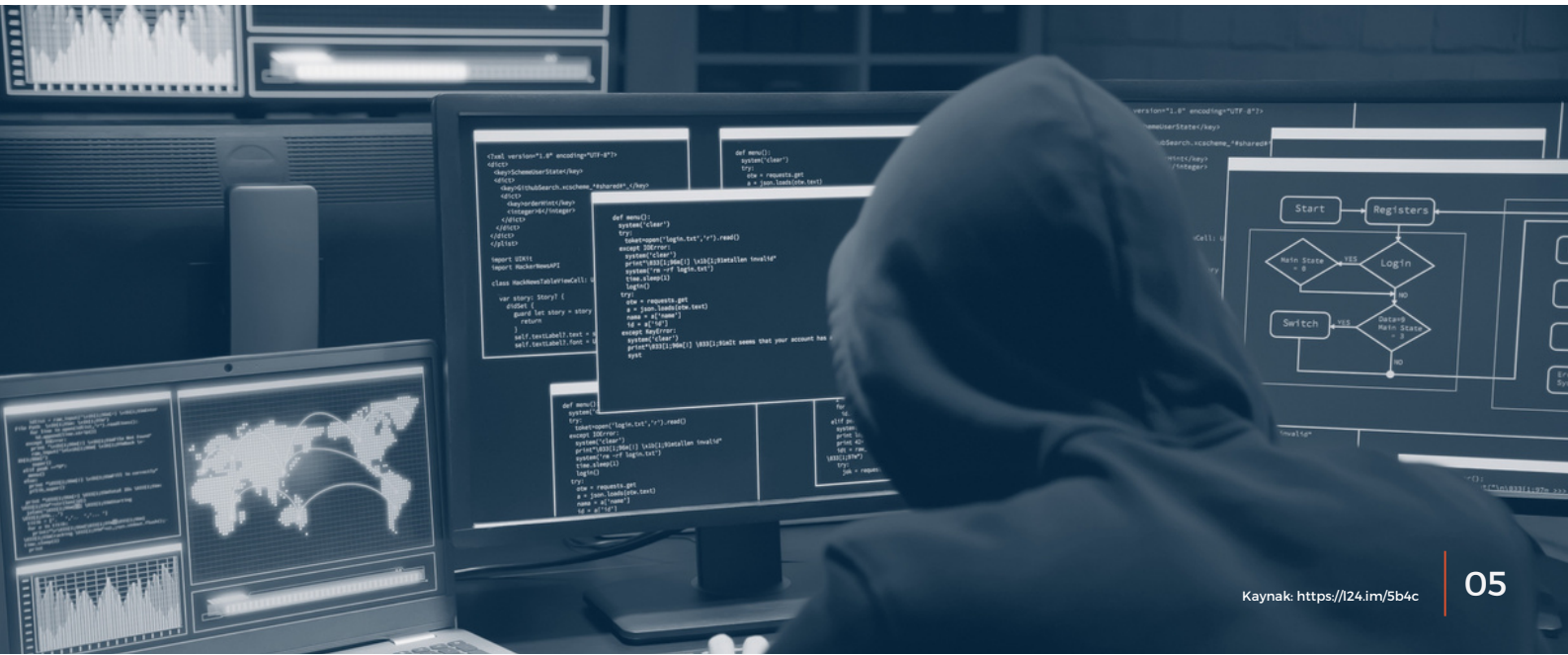
91%

Dolandırıcılık yönetimi, on tüccardan dokuzu tarafından zahmetli görülüyor.

47%

Tüccarlar, işletmelerin dolandırıcılık faaliyetlerini sıklıkla yanlış raporladığını düşünüyor.

Bu durum nedeniyle, 2023'ün gündem başlıklarından biri haline geldi ve diğer benzer konuların uzun süre gündem başlıkları kalmasını öngörüyoruz. Teknoloji, pandemi ve dijitalleşme gibi birçok faktör bu sorunu hızlandırıyor. Bu raporda, olayların başlangıcını, mevcut durumu ve bizim için sırada ne olduğunu ele alacağız.



Kaynak: https://l24.im/5b4c

Son deneyimlere ve uzmanlara göre orta boyutlu finans kurumları en fazla tehdit altındadır. Covid-19 pandemisi ve birçok finansal işlemin hızlı dijital dönüşümünden önce, bankalar ve sigorta şirketleri gibi şirketler hileciler için en cazip olanlar idi. Finansal şirketler uzun zamandır müşteri ve iç süreçlerdeki finansal aktiviteler için online kanalları kullanıyorlar. Bu da, onları daha açık bir kaynak ve dolandırıcılık saldırılarına daha açık hale getiriyor. Dolayısıyla, personel ve güvenlik sistemleri ile daha az veya daha fazla hazırlıklıydılar. Covid-19'un dijital dönüşüm üzerindeki hızlandırılmış etkisi nedeniyle orta ve küçük boylu şirketler ve start-up'lar dolandırıcılar için yeni bir alan haline geldi. Daha az deneyime sahip veya hiç deneyime sahip olmayan bu kurumlar, saldırılar karşısında şok oldular ve finansal varlıklarını, müşterilerini ve itibarlarını kaybettiler.

İstatistikler son üç yıl içinde dolandırıcı saldırıların hacmi ve sayısı dramatik bir şekilde artmıştır. Yukarıda belirtildiği gibi, orta büyüklükteki şirketler daha fazla suç faaliyetine maruz kaldı. Küçük şirketler daha kolay hedeflerdir, ancak kaynakları, müşterileri ve varlıkları sınırlıdır. Bu nedenle kötü niyetli kişiler orta büyüklükteki şirketleri dolandırmayı tercih eder. Öte yandan kurumsal şirketlere yönelik tehdit, sofistike ve karmaşık yöntemlerle devam ediyor.

Ne yazık ki, ekonomi teknolojik gelişmelerin avantajlarıyla birlikte dezavantajlarını da taşır. Bir yandan kötü niyetli kişiler, kimlikleri veya kartları kopyalamak, hesaplara ulaşmak ve güvenlik sistemlerini bozmak için teknolojiyi kullanırlar. Diğer yandan, işletmeler finansal suçlarının önlenmesi ve şirketlerinin korunması için teknolojiyi kullanırlar.

Sosyal mühendisler, yemleme (baiting), oltalama (phishing) veya hedefli oltalama (spear phishing), balina saldırıları (whaling attack), korkutma yazılımı (scareware) ve bahane saldırıları (pretexting) gibi farklı metodlar kullanıyor. Bunlar farklı yöntemler ancak, tümü bireylerin psikolojik zayıflıklarından faydalanıyor.

Tamamlanan bir dolandırıcılık saldırısından sonra kayıplar finansal olmakla kalmıyor, aynı zamanda işletmeler kurumsal itibarlarını, müşteri sadakatlerini veya müşterilerin kendilerini de kaybedebiliyor. Etkileri ele almak ve tamir etmek kolay değil, bu nedenle bu tür kayıplar yaşanmadan önce hazırlıklı olunmalı. Bu yılın beklenen dolandırıcılık eğilimlerini titizlikle derledik ve bununla mücadele etmek ve önlemek için bazı önerileri de listeledik.

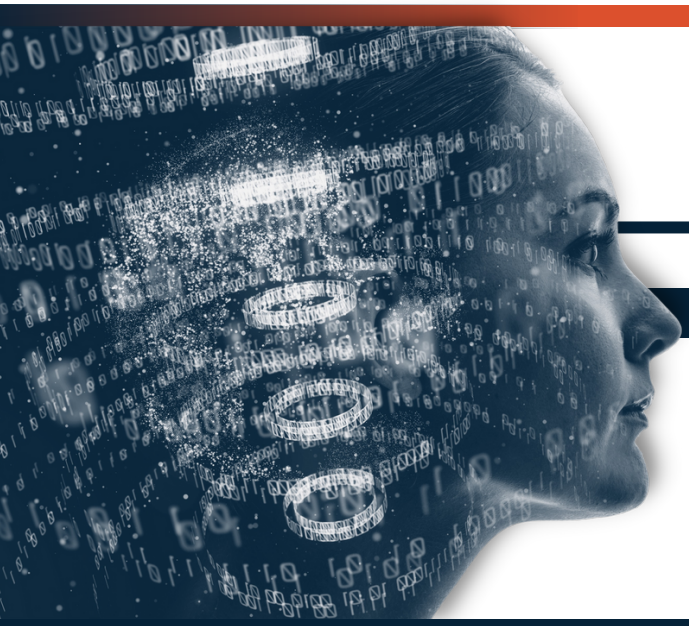
DEV-0537 veya LAPSUS$'ı duydunuz mu?

DEV-0537, şirketlere en kolay erişim noktası sağlamak için bir personel istihdam eden bir suç organizasyonudur. Verilere veya müşterilere erişmek için mevcut kimlik bilgilerini kullandıklarından, aktivitenin algılanması ve izlenmesi azordur. Bu yüzden işletmeler için daha tehlikeli bir suç grubu olabilirler.

DEV-0537, geçen yıl Microsoft'u hackledikten sonra dünya çapında yayılmış ve en olağanüstü tehdit gruplarından biri olarak tanınmıştır. Saldırılarını sosyal medyada paylaşıyorlar ve personele kimlikleri için ödeme yapıyorlar. Microsoft, DEV-0537 saldırılarına karşı aşağıdaki altı öneriyi açıkladı:

Çok Faktörlü Kimlik Doğrulama (MFA) uygulamasını güçlendirin: Kuruluş, çok faktörlü kimlik doğrulamasındaki boşlukları hedefler. Personelin e-postaları, hesap bilgileri veya kimlik bilgileri siber tehditlere karşı iyi korunmalıdır. Microsoft, riskleri azaltmak için bazı korumalar öneriyor:

- Tüm kullanıcılar için, tüm çalışma ortamlarında, tüm sistemler için MFA gereksinimi
- Azure AD Parola Koruması
- Parolasız kimlik doğrulama yöntemleri olarak İş İçin Windows Hello, Microsoft Authenticator veya FIDO belirteçleri
- Telefon tabanlı MFA yöntemleri yerine FIDO Tokens veya Microsoft ile eşleşen doğrulayıcı numarası
- Ara verme hesapları için çevrimdışı depolama
- Riskler için detaylı analizli raporlar için Azure Monitor çalışma defterleri
- Çalışanların eğitimi
- Metin mesajları, ses onayları ve hücresel telefon itmeleri gibi zayıf MFA yöntemlerinden kaçıma



Güvenli uç noktaları zorunlu tutun: Güvenilir, uygun ve sağlıklı cihazlar veri çalınmasına karşı mücadele etmek için esastır. Ayrıca, Microsoft Defender Antivirus'ın bulut tabanlı koruma özelliği ekstra güvenlik sağlayabilir.

VPN'ler için modern kimlik doğrulama seçenekleri: Riske dayalı oturum açma ve uyumlu cihazlar, daha katı erişim koşulları kullanarak VPN kimlik doğrulamasından yararlanır.

Bulut güvenliğinizi güçlendirin ve takip edin: Yukarıda belirtildiği gibi, geçerli kimlik kullanımı saldırılarının tespit edilmesini engeller. Faaliyet sistemi ihlal etmelerine rağmen, normal erişim gibi görünür. Güçlendirilmiş bir bulut güvenliği pozisyonu koruma için yardımcı olabilir. Microsoft, koşullu erişim kullanıcı ve oturum risk yapılandırmalarını gözden geçirmesini, yüksek riskli değişikliklere yönelik bir inceleme yapmayı teşvik eden uyarıların yapılandırılmasını ve Azure AD Identity Protection'daki risk algılamalarının incelenmesini öneriyor.

Operasyonel güvenlik süreçlerini kurun: Sisteminize saldırmaya çalıştıklarında saldırıya cevap vermek için çalışan bir aksiyon planına sahip olmalısınız. Microsoft, şüpheli aktiviteler için sıkı araştırma süreçlerini öneriyor.

Sosyal mühendislik saldırılarına karşı farkındalığı arttırın: DEV-0537 ile mücadele etmek için çalışanları eğitmek şarttır. Özellikle BT departmanları, grubun kullandığı risk ve yöntemlerin farkında olmak zorundadır. Şüpheli faaliyetleri tespit edip yakalamaları ve derhal rapor etmeleri gerekir.

Microsoft, DEV-0537 tehdidi için bu önerileri vermiş olsa da, şirketlerin güvenlik sistemleri bunlardan yararlanabilir. Bunlar genel olarak siber güvenliği iyileştirme yöntemleridir.

Şirket Büyüklüğüne Göre En Çok Karşılaşılan Sahtecilik Türleri

Küçük İşletme	KOBİ	Kurumsal
Dostça Yaklaşma	Dostça Yaklaşma	Dostça Yaklaşma
Kart testi	Kart testi	Kart testi
Oltalama-Yönlendirme	Oltalama-Yönlendirme	Oltalama-Yönlendirme
Kimlik hırsızlığı	Kimlik hırsızlığı	Sadakat Dolandırıcılığı
Kupon/İndirim/İade sahtekarlığı	Kupon/İndirim/İade sahtekarlığı	Kupon/İndirim/İade sahtekarlığı

Kaynak: https://www.shopify.com/uk/enterprise/ecommerce-fraud-prevention

2023'de İzlenmesi Gereken 6 Dolandırıcılık Tehdidi

01 Sosyal Medya Dolandırıcılıkları

Dünya her gün birçok türde dolandırıcılıkla karşı karşıya kalıyor, ancak büyük bir miktarının, hangi tür olduğu önemli değil, sosyal medyada başladığı söylenebilir. Örneğin, gençler arasında, pandemi sonrası karantina süresinde sosyal medyadan romantik ilişki dolandırıcılığı arttı. Dolandırıcılar, yalnız bireyleri kolay hedef olarak görüyor ve bu durumdan faydalanıyor.

Suçlular, Facebook, Twitter, Instagram, Snapchat gibi sosyal medya platformlarını kullanarak kişisel tanımlanabilir bilgilerinizi (PII) çalmaya veya hesaplarınıza erişim vermenize yol açmaya çalışması, sosyal medya kimlik dolandırıcılığı olarak bilinir.

Dolandırıcılar, hesaplarınızın kontrolünü ele geçirebilir, sosyal medyada sizmiş gibi görünebilir, takipçilerinize oltalama saldırıları düzenleyebilir ve hatta yeterli PII'niz varsa mali tablolarınıza da erişebilir.

Sosyal medyada başlayan dolandırıcılıklar genellikle kredi kartı dolandırıcılığı, APP dolandırıcılığı (authorized push payment fraud), para karıştırma veya hesap ele geçirme gibi farklı türde hırsızlık veya kimlik hırsızlığına neden olur. Tipik olarak, dolandırıcılar sahte sosyal medya hesapları aracılığıyla arkadaşlık istekleri gönderir. Bunun ardından, spam mesajlarını ve URL'lerini oltalama ile veya "güvenilir" bir hikaye olarak ve "arkadaşları" kendilerine doğrudan ve isteyerek para göndermelerini sağlamak için kullanırlar.

Dolandırıcıların kullandığı diğer yaygın yöntemler;

- Polis, avukat, banka memuru gibi sahte kimlikler kullanarak mağduru "güçlü" bir nedenle para göndermesi gerektiğine ikna ederler.
- Kötü amaçlı yazılım bağlantıları gönderirler.
- Kartınızı veya kişisel bilgilerinizi kopyalamak için sahte mağazalara bağlantılar gönderirler.
- Bilgi toplamak vb. için anketler kullanırlar.
- Başkalarına onlarla yaptığınız konuşmaları anlatmanızı engellemek için konuşmanızın özel ve gizli olduğuna inanmanızı sağlamaya çalışırlar.
- Anlattıkları hikayelerde borsa, ekonomi ve teknolojinin anlaşılması zor olan ve günlük hayatta karşılaşmadığımız teknik terimlerini kullanarak sizi etkilemeye çalışırlar.

Buraya kadar korkutucuydu ama bir dolandırıcılık girişimini fark etmenin ve kendinizi korumanın yolları var. Sosyal medyada bir dolandırıcıyı tespit etmek için bazı yöntemler:

- Sahte bir hesapsa, birbirleriyle bağlantısı olmayan daha az arkadaşları vardır ve hiç veya az gönderileri vardır.
- Gerçek arkadaşınızın adına sahip bir hesapsa, bu klonlanmış bir hesap olabilir.
- Birisi size yatırım fırsatı sunarsa, fiyatları düşürürse veya para göndermenizi isterse, bu bir arkadaşınızdan olsa bile %99 dolandırıcılıktır. Yatırım önerileri, risksiz yüksek getirilere sahiptir. Ayrıca son zamanlarda kripto para birimleri kullanmaya başladılar.
- Sizin çok faktörlü kimlik doğrulama kodlarınıza ulaşmak isterler. Bir arkadaş olarak yardım isteyerek, kısa mesaj veya e-posta olarak sahip olduğunuz ve kırılması zor olan kodları öğrenmeye çalışırlar.
- Sosyal medya kısıtlamalarını ortadan kaldırmak için başka iletişim kanallarını kullanmak isterler.
- Bağlantılar içeren rastgele mesajlar gönderirler ve bilinmeyen web sitelerine yönlendirirler.
- Doğal olmayan bir dil kullanırlar. Bunun nedeni robotlar/otomatik mesajlar veya anadili İngilizce olmaması veya yerel dili konuşan kişi olmamasıdır.

02 Google Voice Dolandırıcılıkları

Identity Theft Resource Center tarafından alınan dolandırıcılık raporlarına göre, 2022 yılının ilk yarısında bildirilen faaliyetlerin yaklaşık %37'si Google Voice ile gerçekleştirildi.

Google Voice, Google tarafından sunulan bir telekomünikasyon hizmetidir. Kullanıcılarına sanal bir telefon numarası aracılığıyla telefon görüşmeleri yapma, metin mesajları gönderme ve yönetme, ve sesli mesajları yönetme imkanı sunar. Genellikle güvenli bir hizmet olsa da, Google Voice diğer telekomünikasyon araçları gibi dolandırıcılıklara da açıktır. Google Voice dolandırıcılıklarının çeşitli türleri vardır ve kullanımlarıyla birlikte riskler artmaktadır.

En yaygın türlerden biri, Google Voice'un kimlik avı dolandırıcılığıdır. Kimlik avı, dolandırıcıların meşru, güvenilir bir kuruluş veya kişi kılığına girerek kullanıcıları Google Voice hesap bilgileri gibi kişisel bilgiler sağlamalak için aldatma girişimidir. Bu dolandırıcılıklar bir e-posta, mesaj veya telefon görüşmesi şeklinde gelebilir ve genellikle kullanıcıyı sahte bir web sitesine veya çağrı merkezine yönlendiren bir bağlantı veya telefon numarası içerir. Bu dolandırıcılıklar bir e-posta, mesaj veya telefon görüşmesi şeklinde gelebilir ve genellikle kullanıcıyı sahte bir web sitesine veya çağrı merkezine yönlendiren bir bağlantı veya telefon numarası içerir. Kullanıcı bilgilerini sağladıktan sonra, dolandırıcılar bunu kullanıcının Google Voice hesabına erişmek ve hileli faaliyetler için kullanmak için kullanabilir.

Diğer bir yaygın Google Voice dolandırıcılığı türü, premium hizmet dolandırıcılığıdır. Bu aldatmaca, kullanıcıları bir burç veya psişik yardım hattı gibi bir Google Voice numarası kullanarak mükemmel bir hizmete abone olmaları için kandıran dolandırıcıları içerir. Dolandırıcılar, kullanıcıyı abone olmaya ikna etmek için ücretsiz deneme sürümü sunmak veya bir ünlünün hizmeti onayladığını iddia etmek gibi çeşitli taktikler kullanabilir. Ancak, kullanıcı abone olduktan sonra, hizmet için yinelenen bir ücret alınır, bu da iptal edilmesi zor veya imkansız olabilir.

Teknik destek dolandırıcılığı da en çok kullanılan yöntemlerden biridir. Bu dolandırıcılıkta, dolandırıcıların teknik destek temsilcileri olarak davranır ve kullanıcılarla Google Voice numaraları aracılığıyla iletişim kurar. Dolandırıcılar, kullanıcının cihazının veya hesabının bir sorunu olduğunu iddia edebilir ve yardım etmeyi teklif edebilir. Yine de, hedefleri kullanıcının kişisel bilgilerine erişmek veya gereksiz hizmetler için ücret talep etmektir.

Kendinizi Google Voice dolandırıcılıklarından korumak için yapacağınız ilk önemli şey, kişisel bilgilerinizi verirken veya her tür dolandırıcılık için hizmetlere abone olurken dikkatli olmaktır. Herhangi bir bilgi vermeden veya bir hizmete abone olmadan önce daima sizinle iletişim kuran kişi veya kuruluşun kimliğini doğrulayın. Ayrıca, şüpheli bir e-posta, kısa mesaj veya telefon aramasından aldığınız bir bağlantıya asla tıklamamalı veya bir telefon numarasını aramamalısınız. Bir Google Voice dolandırıcılığının kurbanı olduğunuzu düşünüyorsanız, hemen Google Voice desteğiyle iletişime geçmeli ve olayı Federal Ticaret Komisyonu'na (FTC) bildirmelisiniz.

Günümüzde, Google Voice dolandırıcılığı, önemli mali kayıplara ve kişisel bilgi hırsızlığına neden olabilecek yaygın bir sorundur. Bu nedenle, farklı dolandırıcılık türlerinin farkında olmak ve kendinizi korumak için adımlar atmak çok önemlidir. Tetikte ve temkinli kalarak, bir Google Voice dolandırıcılığının kurbanı olma riskini azaltabilirsiniz.

03 Vergi Kaçakçılığı

Vergiler tarih boyunca dünyanın her ülkesinde hep sorun olmuştur. Kimileri bunu doğru yapmak için çaba sarf ederken, kimileri de ek gelir kaynağı, kara para aklama yöntemi ve hatta dolandırıcılık yöntemi olarak kullanıyor. Her yıl, kimlik avı dolandırıcıları ve dürüst olmayan vergi hazırlayıcıları, sayısız vergi mükellefinin kişisel bilgilerini tehlikeye atıyor. Geçen yılki rakamlar, bunun 2023'teki en büyük endişelerden biri olacağını gösteriyor. Vergi beyannamesi belirsizliğinin dolandırıcıların çabalarını artırdığı tartışmalıdır çünkü dolandırıcılar bu korkuyu naif kurbanları dolandırmak için kullanırlar. Bazı örnekler, dolandırıcıların insanların şaşkınlığını ve endişelerini nasıl kullandıklarını gösteriyor.

Vergi kaçakçılığı yöntemlerini gösteren örnekler:

Sesli oltalama (vishing) dolandırıcılıkları: Dolandırıcılar, Vergi İdaresi'ndenmiş gibi davranarak kurbanları telefonla arar ve kurbanın vergi evraklarındaki sözde bir hatayı çözmek için kişisel bilgiler ister.

Oltalama/Kimlik avı dolandırıcılıkları: Vergi idaresinden bir devlet görevlisi gibi davranan dolandırıcılar, vatandaşlara e-postalar gönderir ve vergi beyannamelerinde eksik bilgi varmış gibi davranarak onları kişisel bilgilerini paylaşmaya teşvik eder.

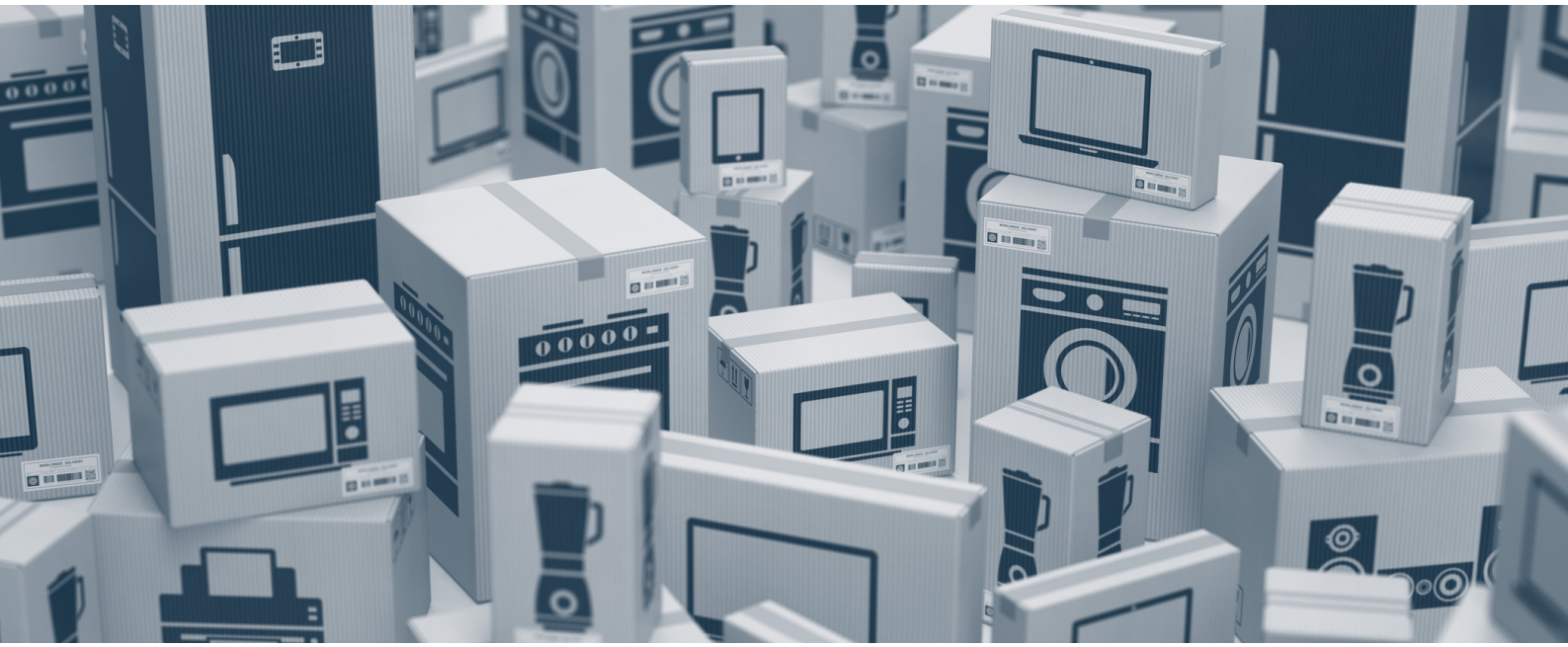
Farklı bir kişi adına vergi beyannamesi doldurma: Dolandırıcılar, meşru vergi mükellefine yönelik bir geri ödeme almak için doğru ve yanlış bilgileri bir arada kullanır ve farklı bir adres veya banka hesabı sunar.

Cömert bir vergi iadesi vaat eden dolandırıcılar: Dolandırıcılar, vergi hazırlama uzmanı kılığına girer ve kurbanlara hizmetlerini sunarak büyük bir geri ödeme sözü verir. Mağdurlar kişisel bilgilerini verir ve hizmetler için ödeme yapar ancak hiçbir zaman geri ödeme almaz.

Hileli telefon görüşmeleri: Dolandırıcılar, Vergi İdaresi görevlilerinin kimliğine bürünür ve vergiler ödenmezse kurbanları tutuklamakla veya sınır dışı edilmekle tehdit eder.

Kimlik hırsızlığı: Dolandırıcılar, Sosyal Güvenlik numarası, adres ve doğum tarihi gibi kişisel bilgileri çalar ve geri ödemelerini almak üzere kurbanın adına vergi beyannamesi vermek için kullanır.

04 E-Ticaret Dolandırıcılığı



Bu sektördeki öncelik, mali kayıpların artması ve hükümetlerin daha katı düzenlemeleri sonrasında değişti. Tüccarlar, pandemi sırasında Kuzey Amerika'daki dolandırıcılık girişimlerinde %68'lik bir artışla karşı karşıya kaldı. Şirketler, Müşterinizi Tanıyın (KYC) prosedürleri, kimlik kontrolleri ve uzun işe alım süreçleri yerine son birkaç yıla kadar müşteri deneyimini tercih ettiler. Günümüzde güvenlik programlarına daha fazla yatırım yapıyorlar ve kimlik doğrulama yöntemlerine ve çok faktörlü kimlik doğrulamaya güveniyorlar. Öte yandan, birçok e-ticaret web sitesi müşteriler için dijital cüzdan oluşturuyor. Bunun arkasında finansal stratejiler olsa da dijital cüzdanlarını tanıtmalarının nedenlerinden biri de daha güvenli bir ödeme avantajı olması.

%59'u mobil uygulamalara, %32'si mobil cüzdanlara ve %28'i ses tabanlı ürünlere yatırım yapıyor

E-ticaret satışları 2022'de küresel olarak 5,55 trilyon dolara ulaştı.

E-ticaret perakendecileri ayda ortalama 206.000 web saldırısıyla uğraşıyor

Kaynak: https://www.ravelin.com/blog/5-types-of-fraud-that-is-used-to-target-e-commerce-retailers

Aşağıda, bu sektördeki yaygın dolandırıcılık türleriyle ilgili yöntemler yer almakta;

- Kimlik hırsızlığı olarak da bilinen ödeme dolandırıcılığı, tüm saldırıların yarısından fazlasını içerir ve kredi kartı bilgileri, e-posta hesapları, kullanıcı hesapları, adlar, adresler, IP adresleri ve kişisel cihazlar gibi çalınan kişisel bilgilerin hileli satın alımlar yapmak, sahte hesaplar oluşturmak ve trafiği manipüle etmek için kullanılmasını içerir.

- Dostça dolandırıcılık, müşteriler satın aldıkları ürünün hiç gelmediğini veya belirtildiği gibi olmadığını iddia ederek bankalarıyla bir ücrete itiraz ettiğinde gerçekleşir. Bu dolandırıcılık Avustralya ve Kanada'da yaygındır ve küresel dolandırıcılık saldırılarının% 39'unu oluşturur.

- Kart testi sahtekarlığı, dolandırıcıların, çalınan bir kredi kartının küçük, düşük değerli bir satın alma işlemi yaparak çalışıp çalışmadığını test etmek ve belirlemek için kartları kullandığı yöntemdir. Kartın çalıştığı onaylandığında, kartı kullanarak daha maliyetli işlemler yaparlar.

- İade kötüye kullanımı, müşterilerin geri ödeme karşılığında kırılmış, hasar görmüş veya çalınan ürünleri bir perakendeciye iade ettiği yerdir. Bu maliyetli bir sorundur ve perakendeciler bu dolandırıcılık nedeniyle iade edilen her 100 ABD Doları için 5,90 ABD Doları kaybeder.

- Çevrimiçi ödeme dolandırıcılığı, dolandırıcıların başka bir kişinin ödeme ayrıntılarını çaldığı ve bunları bir e-ticaret mağazası aracılığıyla alışveriş yapmak için kullandığı yerdir. Dünya çapındaki perakendeciler bu sahtekarlıktan muzdariptir, ancak en yaygın olanı Meksika'dır.

- Hesap devralma dolandırıcılığı, dolandırıcıların bir müşterinin çevrimiçi hesabına girdiği ve sahte satın alımlar yapmak için kayıtlı ödeme kartlarını kullandığı yöntemdir. Markaların %23'ü geçen yıl hesap devralma dolandırıcılığı yaşadı.

- Kuruluş sahtekarlığı, sadakat sahtekarlığı ve promosyon sahtekarlığı; E-ticaret markalarının yeni müşteriler çekmek için promosyonlar, bağlı kuruluşlar ve sadakat programları kullandığı, ancak dolandırıcıların bu programlardan yararlanmak için taktikler kullandığı promosyon, bağlı kuruluş veya sadakat kötüye kullanımı ile e-ticaret şirketlerine gelir kaybı.

Kaynak: https://www.shopify.com/uk/enterprise/ecommerce-fraud-prevention

Temiz dolandırıcılık, meşru görünen ve işlemler kara listeye alınmış dolandırıcılık hesapları tarafından işaretlenmediği veya bloke edilmediği için perakendeciler için giderek daha fazla sorun oluşturan hileli işlemleri ifade eder. Bu dolandırıcılık, çalınan kredi kartı bilgileri kart sahibinin kimliğine bürünmek için kullanıldığında gerçekleşir.

Satış ortağı dolandırıcılığı, bağlantıların ve içeriğin paylaşılması yoluyla komisyon oluşturabilen bağlı kuruluş pazarlama programları aracılığıyla trafiğin ve kayıtların manipüle edilmesini içerir. Kötü niyetli aktörler, yanlış bir yüksek trafik algısı oluşturmak için bir web sayfasını birden çok kez yenileyebilir veya spam e-postalar ve açılır pencereler gönderebilir.

Nirengi dolandırıcılığı, çevrimiçi suçluların sahte veya kopya bir web sitesi kurması ve alıcıları var olmayan veya hiç gönderilmeyen ucuz mallarla kandırmasıdır. Bu tür dolandırıcılık ayrıca kişisel bilgilerin kaybolmasına ve meşru bir işletmenin itibarının zedelenmesine neden olabilir. 'Nirengi' adı, alıcıları cezbetme, ayrıntılarını çalma ve bunları daha geniş bir planın parçası olarak kullanma şeklindeki üç aşamalı süreçten gelir.

05 Sentetik Kimlik Dolandırıcılığı

Sentetik Kimlik Dolandırıcılığı (Synthetic Identity Fraud - SIF), gerçek ve sahte bilgilerin birleşimiyle yeni bir kimlik oluşturan dolandırıcılar tarafından yapılan dolandırıcılığı ifade eder. Belirli bir kişinin bilgilerini çalıp kullanan geleneksel kimlik dolandırıcılıklarının aksine, tek bir meşru bilgiye dayalı sahte bir kimlik oluştururlar. 2023 yılında özellikle finans sektöründe işletmelerin en büyük endişelerinden biri haline geldi.

SIF'in farklı tanımları ve tespitine yönelik çoklu yaklaşımlar, bu dolandırıcılığı tespit etmeyi ve hafifletmeyi zorlaştırıyor. Bu nedenle Federal Rezerv, belirli bir tanım geliştirmek için 12 dolandırıcılık uzmanından oluşan bir grup oluşturdu. Terimi şu şekilde tanımladılar: **"Sentetik kimlik dolandırıcılığı (SIF), kişisel veya mali kazanç için dürüst olmayan bir eylemde bulunmak üzere bir kişi veya kuruluşu uydurmak için kişisel olarak tanımlanabilir bilgilerin (PII) bir kombinasyonunu kullanıyor."** Buna ek olarak, Federal Rezerv endüstri büyümesini artırmak ve SIF risklerini azaltmak için üç teknik rapor yayınladı.

Sahte kimlik oluşturma

- Dolandırıcılar, çocuklar veya evsizler gibi kredi kullanmayan kişilerin sosyal güvenlik numarası gibi kişisel olarak tanımlanabilir bilgilerini çalar.
- Ayrıca kimlik numarası, banka hesap bilgileri ve e-posta gibi birden çok kişiden çalınan bilgileri kullanarak "Frankenstein Kimlikleri" oluştururlar.
- Bilgi, atılan belgeler, dark web veya veri ihlalleri yoluyla elde edilebilir.

Kredi başvurusu

- Dolandırıcılar, çevrimiçi kredi başvurusu yapmak için sentetik kimlikler kullanır.
- İlk başvurular, kimliğin daha önce kredi geçmişi olmadığı için genellikle reddedilir.
- Dolandırıcılar, genellikle yüksek riskli bir borç verenden küçük bir kredi limiti ile başlayarak, onaylanana kadar devam ederler.

Sentetik kimlik hırsızları, kişilerin sosyal güvenlik numaralarını, banka hesap numaralarını, kredi kartı bilgilerini, e-posta ve bakım kayıtlarını en kolay şekilde çalar. Teknolojinin gelişmesiyle birlikte çeşitli dolandırıcılık yöntemleri de ortaya çıkmıştır. Genel olarak, SIF bu adımlarla çalışır.

Olumlu bir kredi geçmişi oluşturmak

- Dolandırıcılar, kredi notlarını yükseltmek ve sağlam bir kredi sicili oluşturmak için kredi limitini kullanır ve düzenli ödemeler yapar.
- Zamanla, daha cömert kredi limitlerine ve diğer borç verenlere erişim sağlayabilirler.
- Gelişmiş suç çeteleri, kimliğin daha meşru görünmesini sağlamak ve daha yüksek ödemelere erişim elde etmek için sahte işletmeler oluşturabilir ve mevcut adresleri kullanabilir.

Ortadan kaybolma:

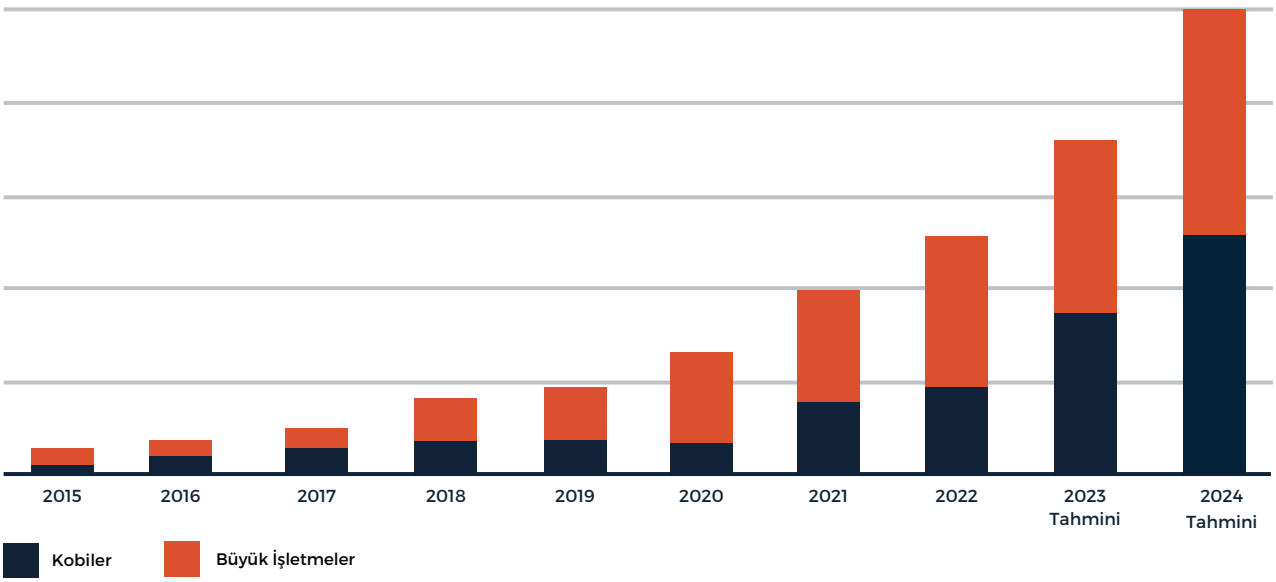
- Dolandırıcılar kredi limitlerini maksimuma çıkarır ve ortadan kaybolur.
- Bazıları yeni kimlikler oluşturabilir, bazıları ise birden fazla sahte kimlik kullanabilir.
- Dolandırıcıların izini sürmek, onlara ulaşacak kesin bir bilgi olmadığı için zor olabilir ve SSN'yi kullanan kişinin masum olduğunu kanıtlamak zor olabilir.

Sektörün Yenilikçi Oyuncuları: Regtech'ler

Regülasyon Teknolojisi (Regtech) şirketleri, son yıllarda kara para aklamayla mücadelede giderek daha önemli bir rol oynamaktadır. Bu şirketler, kara para aklama ve dolandırıcılığı tespit etmeye ve önlemeye yardımcı olabilecek benzersiz yeteneklere ve kaynaklara sahip. 2023'te onları daha fazla görmeyi umuyoruz ve bu nedenle Regtech'lerin sektör için önemi hakkında bir tartışmaya yer verdik ve bu şirketlerin kara para aklamayla ilişkili riskleri azaltmaya nasıl yardımcı olabileceğini bu raporda inceledik.

Regtech şirketleri, finansal kurumlara kara paranın aklanmasının önlenmesine yönelik yenilikçi çözümler sağlamaya odaklanır. Müşteri durum tespitini otomatikleştirerek, kara para aklamayı anında tespit etmelerini ve önlemelerini sağlayan işlemleri izleyerek ve uyumlulukla ilgili görevler için diğer hizmetleri otomatikleştirerek uyumluluk için uygun maliyetli bir çözüm sunarlar. Ayrıca şifreleme ve çok faktörlü kimlik doğrulama gibi gelişmiş güvenlik çözümleri aracılığıyla finansal sistemlerin güvenliğinin sağlanmasında çok önemli bir rol oynarlar. Sağladıkları teknolojinin en son düzenleyici gerekliliklere uygun olmasını sağlamak için düzenleyicilerle yakın işbirliği içinde çalışırlar. Yeni düzenlemelerin geliştirilmesi için bunların sağladığı girdiler de önemlidir.

ABD Regtech Pazar Büyüklüğü



Kaynak: https://linkisalt.com/9Z5km

Sağladıkları en önemli avantajlardan biri, kara para aklamayı tespit etmek ve önlemek için teknolojiden yararlanma yetenekleridir. Bu şirketler genellikle büyük miktarda veriye erişebilir, yapay zeka (AI) ve makine öğrenimi algoritmalarını kullanabilir; örneğin, şüpheli etkinlik modellerini belirlemek. Bu şirketlerin, kara para aklama ve terörün finansmanını zamanında önlemeye yardımcı olabilecek şüpheli etkinlikleri olduğu gibi tespit edip işaretlemelerine olanak tanıyan gelişmiş analizlerle gerçek zamanlı işlem izleme sağlarlar. Bu, aksi takdirde tespit edilemeyecek mali suçların belirlenmesine yardımcı olabilir ve ayrıca kurumların yüksek riskli müşterileri ve işlemleri tanımasına yardımcı olabilir.

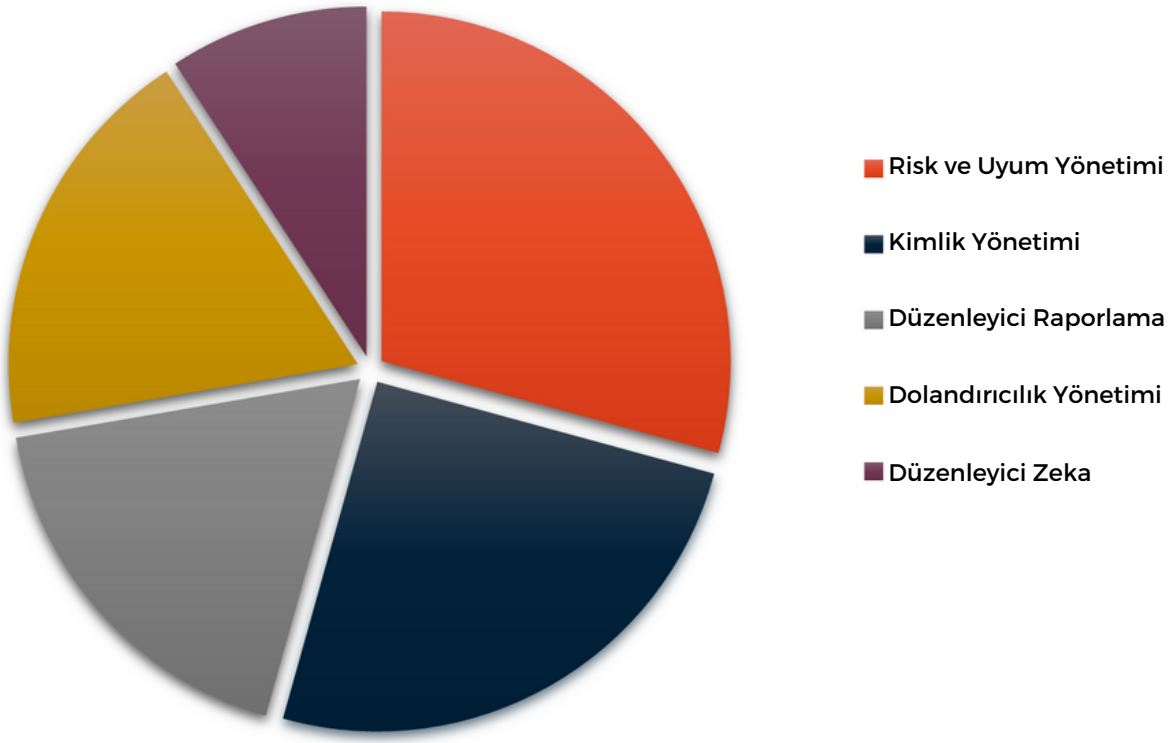
Son yıllarda dolandırıcılık tespiti için yenilikçi çözümler sunmaya başlandı. Örneğin, dijital kimlik doğrulama hizmetleri, müşterilerin iddia ettikleri kişi olduklarından emin olunmasına yardımcı olabilir ve dijital katılım süreçleri, finans kurumlarının AML düzenlemelerine uymak için müşterilerden gerekli bilgileri almasını kolaylaştırabilir. Böylece finansal sistemin şeffaflığının artmasına yardımcı olurlar.

Kurumsal şirketler, özellikle dijitalleşme ve büyük veri çağında uyumluluk sistemlerini otomatikleştirmenin ne kadar önemli olduğunu deneyimliyor. Regtech'ler, şirketlerin çok büyük hacimli tarama ve izleme ihtiyaçlarını karşılamak için burada sahneye çıkıyor. Müşteri durum tespiti, işlem izleme ve uyumlulukla ilgili diğer görevleri otomatikleştirerek kurumların AML yönetmeliklerine uymasına yardımcı olabilirler. Bu, finansal kurumlara yalnızca zaman ve para tasarrufu sağlamakla kalmaz, aynı zamanda uyum süreçlerinin doğruluğunu da artırır. Otomasyon aynı zamanda uyumluluk süreçlerinde olası kör noktalara yol açabilecek insan hatalarını ve ön yargıları da azaltır.

Ek olarak, bazı Regtech'ler daha basit raporlama süreçleri için çözümler sunar. Sektördeki her aktör, şüpheli faaliyet bildirimlerinin doldurulması ve yetkililere bildirim süreçlerinin sıkıntılı olabileceğini bilir. Gerçek zamanlı izleme, finans kurumlarının herhangi bir şüpheli faaliyeti anında ilgili makamlara bildirmesini sağlar.

Regtech pazarının 2025'te %24,4'lük bir CAGR ile 18,89 milyar dolara ulaşması bekleniyor.

Küresel Regtech Pazar Payı



Uyumluluk yazılımı, finansal kurumların pahalı iç sistemlere ve kalabalık operasyon ekiplerine yatırım yapma ihtiyacını azaltarak şirketler için uygun maliyetli bir çözümdür. Regtech firmalarının sunduğu çözümler mevcut sistemlere kolaylıkla entegre edilebilmektedir. Teknoloji, kurumun özel gereksinimlerine uyacak şekilde ayarlanabilir. Bu, finansal kurumların AML düzenlemelerine uyumu korurken maliyetleri düşürmesine olanak tanır.

Günümüzde regtech şirketlerinin AML sektörü için gerekliliği açık ve köklü bir gerçektir. Kara para aklamanın tespit edilip önlenmesine yardımcı olabilecek benzersiz yeteneklere ve kaynaklara sahiptirler ve finansal kurumların AML düzenlemelerine uymasına yardımcı olacak iyi bir konumdadırlar. Ayrıca artan teknoloji kullanımı ve dijitalleşme ile birlikte önümüzdeki yıllarda kara para aklama ve terörün finansmanı ile mücadelede önemli rol oynayacaktır.

Etkili AML Uyumluluğunun Temel Bir Unsuru: İşlemler ve Zorlukları Üzerinde Dikkatli Bir Göz

Finansal kurumlar üzerinde AML düzenlemelerine uyma yönündeki artan baskı nedeniyle ve finansal suç tehdidi gelişmeye devam ettikçe, işlem izlemenin önemi artıyor. Özellikle covid-19 sonrası suçların artan karmaşıklığı ve tüm süreçlerin dijitalleşmesi bunun başlıca nedenlerinden biri. Ek olarak, suç grupları sürekli olarak kara para aklama ve yakalanmaktan kaçınmanın yeni yollarını buluyor ve finansal kurumlar bu faaliyetlere karşı genellikle ilk savunma hattını oluşturuyor. Finans kuruluşları, işlemleri izleyerek kara para aklama veya diğer mali suçların göstergesi olabilecek şüpheli faaliyetleri tespit edip rapor edebilir.

AML uyumluluğu için öneminin yanı sıra, işlem izleme, sahtekarlığın tespit edilmesinde ve bunlarla mücadelede de hayati bir rol oynar. Hileli işlemler, basit çek dolandırıcılığından birden fazla tarafı içeren karmaşık planlara kadar çeşitli şekillerde olabilir. Finansal kuruluşlar, finansal ilişkilere dikkat ederek, hileli davranışa işaret edebilecek, kayıpları önlemeye ve müşterileri korumaya yardımcı olabilecek şüpheli etkinlikleri tespit edebilir ve raporlayabilir.

Finansal kurumlar, işlem izleme risklerini azaltmak için süreci otomatikleştirmek için yazılımı kullanabilir. AML yazılımı, finansal kurumların şüpheli işlemleri daha hızlı ve doğru bir şekilde tanımlamasına yardımcı olabilir ve bir izleme sisteminin uygulanması ve sürdürülmesinin maliyetini azaltabilir. Ek olarak, bu teknolojik çözümler, büyük işlemler veya belirli ülkeleri veya bireyleri içeren işlemler gibi belirli kriterleri karşılayan işlemleri işaretleyecek şekilde programlanabilir. Bu, finansal kurumların en şüpheli işlemlere odaklanmasına yardımcı olabilir ve ayrıca yanlış pozitiflerin sayısını azaltmaya yardımcı olabilir. Aksine yazılım sistemleri, şirketlerin kullanmadan önce dikkat etmesi gereken kritik noktalara sahiptir.

Tüm bunların yanı sıra AML kapsamındaki risk bileşenleri arasında finansal ve hukuki risklerin yanı sıra itibar riski de önemli bir yer tutmaktadır. AML risklerinin doğru yönetilmemesi, mevzuatın ihlali nedeniyle parasal cezalara neden olacağı gibi, ilgili şirketin hem ulusal hem de uluslararası alanda itibar riski üzerinde olumsuz etki yaratacak, mevcut/gelecekteki işbirliği ve ilişkiler açısından sorun yaratabilecektir. Günümüzde itibar, finansal kurumlar için parayla ölçülemeyen en önemli varlıktır ve onu korumak ve sürdürmek mücadelenin önemli alanlarından biri olmaya devam edecektir.

İŞLEM İZLEMENİN ZORLUKLARI

Artan önemine rağmen, işlem izlemenin bazı zorlukları vardır. Şirketlerin yardıma ihtiyaç duyduğu temel zorluklardan biri, izlenmesi gereken işlem hacmidir. Finans kurumları her gün milyonlarca işlem gerçekleştirir ve şüpheli olan küçük yüzdeyi belirlemek zor olabilir. Ek olarak, şüpheli işlemleri belirlemek için genellikle net kriterlere ihtiyaç vardır ve finans kuruluşlarının meşru ve gayri meşru faaliyetler arasında ayrım yapmak için yardıma ihtiyacı olabilir. Ayrıca, kapsamlı bir işlem izleme sisteminin uygulanması ve sürdürülmesinin maliyeti yüksek olabilir ve finansal kuruluşlar maliyetleri potansiyel faydalara karşı tartmak zorunda kalabilir.

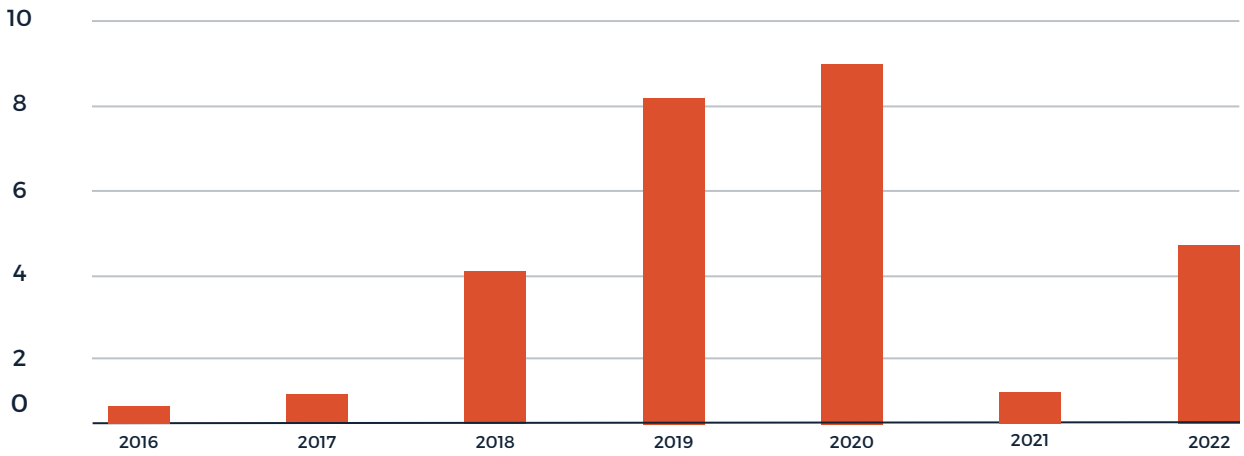
İşlem izleme yazılımını entegre etmek zordur ve bir çözüm olmasına rağmen bunu yürütmek de kolay değildir.

Buna rağmen, etkisiz veya geleneksel işlem izleme çözümlerine sahip kuruluşlar, uyum konusunda zorluklarla ve düzenlemelere uymadıkları için cezalarla karşılaşabilirler. Zorluklardan biri, işlem izleme sisteminde uygulanabilen ancak kurumun risk iştahına uygun olmayabilecek, kullanıma hazır kurallardır. Diğer bir zorluk da yanlış pozitif sonuçlardır, çünkü geleneksel işlem izleme sistemleri vakaların %90'ında yanlış anlayarak zaman ve insan gücü kaybına neden olabilir. Ayrıca, kural tabanlı işlem izleme sistemlerini belirli eşikler dahilinde çalıştırarak aldatmak kolaydır ve bu da şüpheli faaliyetlerin fark edilmemesine neden olabilir.

İşlem izlemede Yapay Zekanın (AI) kullanımı, tüm veriler için tek bir doğruluk kaynağına dayanır, ancak AI dağıtımı için veri hazırlama süreci kolay ve basit değildir ve herhangi bir yolsuzluk belirtisine dikkat edilmelidir. Farklı düzenleyiciler, işlem izlemede neyin kabul edilebilir olduğu konusunda farklı görüşlere sahip olduğundan ve bu da uyumluluk zorluklarını artırdığından, farklı düzenleyici yaklaşımlardan kaynaklanan bir kafa karışıklığı da bulunmakta. COVID-19 salgını aynı zamanda dolandırıcılık risklerini ve etkili AML işlem izleme ihtiyacını artıran dijital öncelikli tüketiciliğe geçişi de hızlandırdı. Bu nedenle, etkili bir yazılım çözümü seçmek, yalnızca birini uymak için kullanmaktan daha önemlidir.

İşlem izleme protokolleri, kara para aklama veya diğer mali suç faaliyetlerini önerebilecek şüpheli faaliyetlerin belirlenmesinde ve raporlanmasında önemli bir faktördür. Mali suç tehdidi devam ettikçe, işlem izlemenin önemi yalnızca artacaktır. Finansal kurumlar, kendilerini ve müşterilerini finansal suçlardan korumak ve AML uyum yükümlülüklerini yerine getirmek için sağlam işlem izleme sistemlerine sahip olmalıdır. Yazılım kullanımı, finansal kurumların süreci otomatikleştirmesine yardımcı olabilir ve ayrıca işlem izlemeyle ilgili risk ve maliyetleri azaltmaya yardımcı olabilir. Ancak firmanızın ihtiyaçlarına göre doğru ve etkili yazılımı kullanmak, yazılımı kullanmak kadar gereklidir.

AML ve İlgili Suçlar İçin Küresel Para Cezaları (Milyar Dolar)



Yeni Ufuklar: İklim Değişikliğinin Mali Suçlar Üzerindeki Etkileri

İklim Değişikliği ve Mali Suç Arasındaki İlişkiyi Keşfetmek

Son on yılın en çok mücadele edilen konularından biri olan iklim değişikliğinin etkileri kara para aklamayla mücadele de dahil olmak üzere hayatımızın birçok alanında hissediliyor. Küresel ekonomiyi ve finansal sistemlerin bütünlüğünü baltalayan önemli bir sorundur. Ekstrem hava olayları, yükselen deniz seviyeleri ve biyolojik çeşitlilik kaybı gibi etkileri, kara para aklama sorununu, özellikle sigorta sektörü için çeşitli şekillerde şiddetlendirme potansiyeline sahiptir.

İklim değişikliği, ekonomideki kötü aktörler için yeni finansal fırsatlar yaratarak kara para aklama riskini artırabilir. Dünyanın iklimi değiştikçe, çeşitli endüstrileri yöneten ekonomik koşullar da değişir. Örneğin, tarım, ormancılık ve balıkçılık gibi doğal kaynaklarla ilişkili endüstriler, hava durumu modellerindeki ve su mevcudiyetindeki değişikliklere karşı özellikle savunmasızdır. Bu endüstriler yeni koşullara uyum sağlamakta zorlanırken, ayakta kalabilmek için yasa dışı ürünler satmak gibi yasa dışı faaliyetlere yönelebilirler. Bu da kara para aklayıcılar için yasadışı fonları finansal sistem aracılığıyla hareket ettirmek için yeni fırsatlar yaratır.

İklim değişikliği, nüfusun göçünde ve yerinden edilmesinde bir artışa neden oluyor. Alçak kıyı bölgeleri ve kuraklık ve sellerden etkilenen bölgeler gibi artık insan yerleşimini destekleyemeyen bölgelerden daha fazla insanın göç etmesine neden olur. Ayrıca tarımsal üretime olumsuz etkileri nedeniyle kırdan kente göçe yol açmaktadır. Bu henüz tüm lokasyonlar için yaygın bir sorun olmasa da dünyanın bazı bölgeleri bu sorunu yaşamaya başlamıştır. İnsanlar değiştiremedikleri veya kontrol edemedikleri nedenlerle yerlerinden ayrılmak zorunda kaldıkça, hayatta kalabilmek için gayri resmi veya yasadışı faaliyetlere güvenme potansiyelleri artar. Bu aynı zamanda kara para aklama faaliyetlerini tespit etmeyi zorlaştırmaktadır, çünkü bu kayıt dışı ekonomilerde yasadışı fonların izlenmesi zor olabilir. Öte yandan, bu insanlar insan kaçakçılığı için göçmen olarak savunmasız hedefler haline geliyor. Bu, özellikle kaynakların ve desteğin sınırlı olduğu düşük gelirli ülkelerde artan bir endişe kaynağıdır. İklim değişikliğine bağlı yerinden edilme, insan ticareti ve diğer sömürü biçimlerini artırabilecek sosyal ağların, ekonomik fırsatların ve yasal korumaların kaybına yol açabilir. Dahası, halihazırda insan kaçakçılığı yaşayan bölgelerde iklim değişikliği, insan tacirleri için yeni yollar ve fırsatlar yaratarak sorunu daha da kötüleştirebilir.

Ayrıca, kara para aklama riskini daha da artırabilecek küresel ekonomi üzerinde bir etkisi olması bekleniyor. Küresel sıcaklıktaki artış ve sık görülen aşırı hava olayları gibi iklim değişikliği etkileri daha yaygın hale geldiğinden, ekonomik büyümenin etkilenmesi muhtemeldir. Bu, özellikle iklim değişikliğinin sonuçlarına karşı daha savunmasız bölgelerde ekonomik gerilemelere neden olabilir. Ekonomi mücadele ederken, insanların geçimlerini sağlamak için yasadışı faaliyetlere yönelmeleri daha olasıdır ve bu, kara para aklayıcılar için yeni fırsatlar yaratabilir.

2022 yılında dünyanın farklı bölgeleri kuraklık, sel, fırtına, orman yangını ve kasırgalardan zarar gördü. Avrupa Birliği üyeleri önlemlerini düzenleyici ölçekte hızlandırdı. 2030 yılına kadar sera gazı emisyonlarını en az %55 oranında azaltmayı hedefliyorlar. Öte yandan, düzenlemeler ekonomik aktivitelerini ve Avrupa ülkeleriyle çalışan tarafları etkiliyor. İşletmeler bu konuyu ciddiye almalı ve aktif olarak iklim değişikliğinin etkilerini azaltmanın ve ortaya çıkardığı potansiyel risklere hazırlanmanın yollarını aramalıdır. Bu tür düzenlemeler sadece yasal bir uyum meselesi değil, aynı zamanda gezegenimizi korumak için sosyal ve etik bir sorumluluktur.

Deprem ve sel gibi doğal afetler topluluklar üzerinde yıkıcı bir etkiye sahip olabilir, bu da yaygın hasara, can kaybına ve temel hizmetlerde kesintilere neden olabilir. Etkilenebilecek temel hizmetlerden biri finans sektörüdür. Kriz zamanlarında, finansal hizmetlere erişim, yalnızca ihtiyacı olan bireyler için değil, aynı zamanda etkilenen bölgelerde gerçekleştirilmesi gereken felaketle ilgili faaliyetler için de giderek daha önemli hale geliyor.

Doğal afetler sırasında işlevsel bir finansal sisteme sahip olmak zorunludur, çünkü bu sistem bireylerin ihtiyaçlarını karşılamada, afet yardımı çabalarını desteklemede ve yardım faaliyetlerinin verimli ve etkin bir şekilde yürütülmesini sağlamada çok önemli bir rol oynayabilir. İşlevsel bir finansal sistemin olmaması hileli faaliyetler için fırsatlar sağlayabileceğinden, işlevsel bir finansal sistem savunmasız bireylerin sömürülmesini de önleyebilir.

İklim değişikliği ile ilgili riskleri azaltmak için kara para aklama ile mücadele tedbirlerimizi güçlendirmemiz esastır. Bu, iklim değişikliğinin kara para aklama faaliyetlerini kolaylaştırabileceği yolları dikkate alarak daha kapsamlı ve koordineli bir yaklaşım gerektirecektir. Mali Eylem Görev Gücü (FATF), ülkelerin AML ve CFT düzenlemelerinde iklim değişikliği ve çevresel bozulma ile bağlantılı olanlar da dahil olmak üzere risklerin tanımlanmasını ve değerlendirilmesini içermelerini tavsiye etmiştir. Bu, finansal kurumların ve devlet kurumlarının iklim değişikliğiyle bağlantılı olabilecek kara para aklama faaliyetlerini tespit etmek ve önlemek için daha donanımlı olmalarını sağlamaya yardımcı olacaktır.

Sigorta Sektöründeki Riskler

İklim değişikliğinin son yıllarda sigorta sektörü için en büyük riski oluşturduğu iddia ediliyor. Dünyanın sıcaklığı yükseldikçe ve şiddetli hava olayları daha sık hale geldikçe, sigorta şirketleri sel, fırtına ve diğer doğal afetlerin neden olduğu hasarlar için daha fazla taleple karşı karşıya kalmaktadır. Ek olarak, iklim değişikliği sigorta şirketlerinin riski değerlendirme ve fiyatlama şeklini de etkiliyor ve sigorta sektörünün sunduğu ürün ve hizmetleri de etkiliyor. İklim değişikliği, sigorta ürünlerine olan talebi artırarak sigorta sektörünü de etkiliyor. Ekstrem hava olaylarının ve ilgili risklerin artan sıklığıyla birlikte, daha fazla insan kendilerini ve mülklerini korumakla ilgilenmeye başlıyor. Sigorta şirketleri artık bu artan talebi karşılama zorluğuyla karşı karşıya.

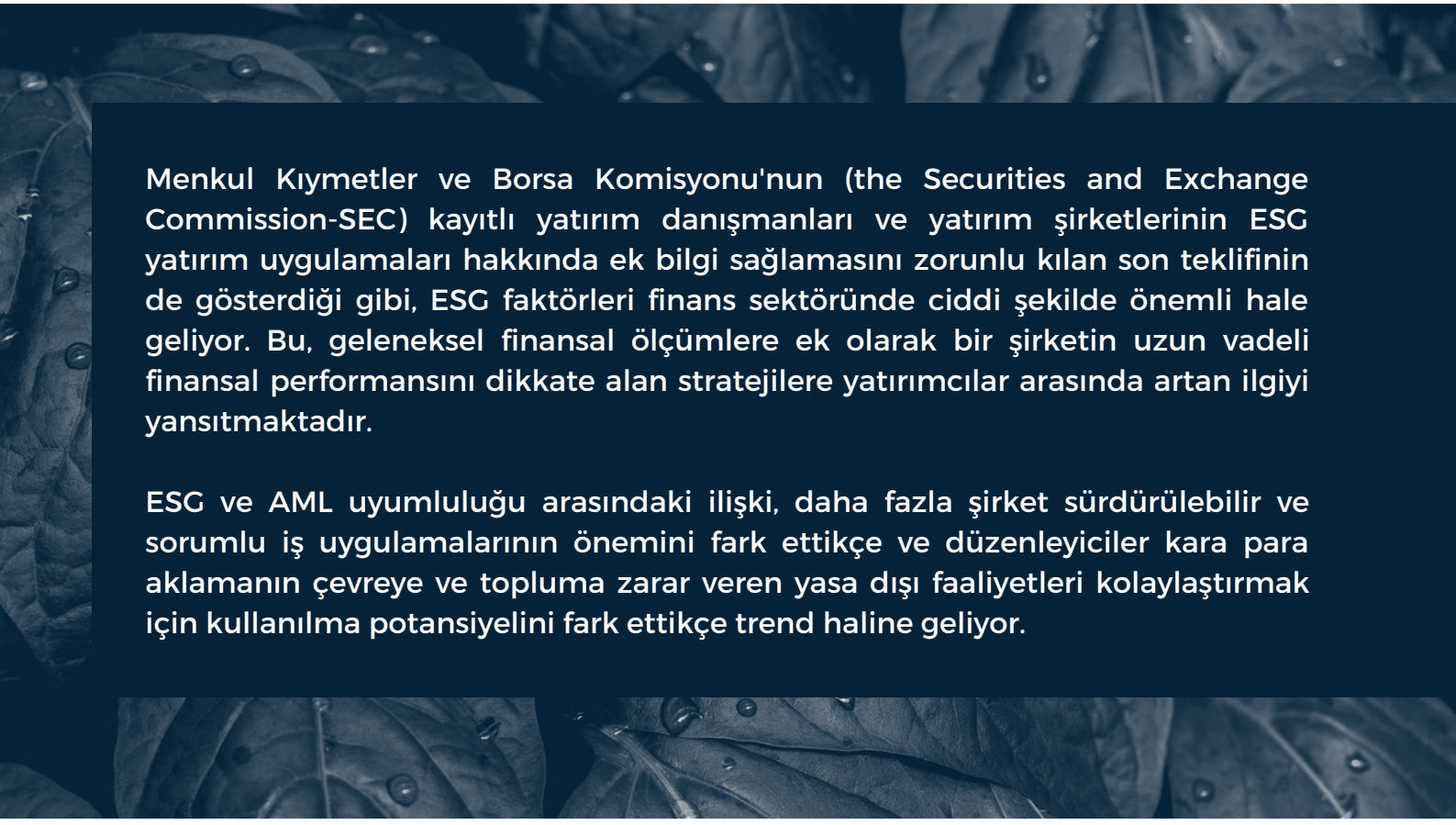
Dünyanın iklimi daha istikrarsız hale geldikçe, doğal afetlerin sıklığı ve şiddeti artmaktadır. Bu, özellikle yükselen deniz seviyelerinin sel ve fırtına dalgaları riskini artırdığı kıyı bölgelerinde geçerli. Ayrıca, dünyanın iklimi ısındıkça, sigorta şirketleri de sıcak hava dalgaları ve kuraklığın neden olduğu hasarlar için talep sayısında artış görüyor.

İklim değişikliğinin sonuçları ile sigortacıların poliçe sahiplerinin ihtiyaçlarını karşılamak için yeni ürün ve hizmetler geliştirmeleri gerekebilir. Örneğin, birçok sigorta şirketi şu anda hava koşullarıyla ilgili zorluklarla karşılaşan çiftçiler için mahsul sigortası gibi iklime özgü sigorta ürünleri sunmaktadır. Bazı şirketler ayrıca, fiili zararlardan ziyade sıcaklık gibi kararlaştırılan bir endeksin seviyesine göre ödeme yapan parametrik sigorta sunmaya başlamıştır. Bu nedenle artan talebin ve yeni ürün türlerinin risklerin artmasıyla birlikte geldiğini görüyoruz.

ESG ve AML arasındaki Bağlantı: Sürdürülebilirlik ve Risk Yönetimini Dengeleyin

Çevresel, sosyal ve yönetişim (Environmental, social, and governance-ESG), bir işletmedeki faaliyetin sürdürülebilirliğini ve toplumsal etkilerini incelemek için ana faktörleri tanımlamak için kullanılan terimdir. Bu faktörler, geleneksel finansal ölçümlere ek olarak, bir şirketin uzun vadeli finansal performansını belirlemek için sıklıkla kullanılır.

Göz önünde bulundurulması gereken hususlar, bir şirketin karbon ayak izi ve kirliliği ve atıkları azaltma çabaları gibi çevresel etkilerinin yanı sıra çalışanlara, tedarikçilere ve topluluklara yönelik davranışları gibi sosyal etkilerini içerir. Yönetişim hususları, bir şirketin liderliği ve yönetiminin yanı sıra şeffaflık ve etik iş uygulamalarına yaklaşımını içerir.



Menkul Kıymetler ve Borsa Komisyonu'nun (the Securities and Exchange Commission-SEC) kayıtlı yatırım danışmanları ve yatırım şirketlerinin ESG yatırım uygulamaları hakkında ek bilgi sağlamasını zorunlu kılan son teklifinin de gösterdiği gibi, ESG faktörleri finans sektöründe ciddi şekilde önemli hale geliyor. Bu, geleneksel finansal ölçümlere ek olarak bir şirketin uzun vadeli finansal performansını dikkate alan stratejilere yatırımcılar arasında artan ilgiyi yansıtmaktadır.

ESG ve AML uyumluluğu arasındaki ilişki, daha fazla şirket sürdürülebilir ve sorumlu iş uygulamalarının önemini fark ettikçe ve düzenleyiciler kara para aklamanın çevreye ve topluma zarar veren yasa dışı faaliyetleri kolaylaştırmak için kullanılma potansiyelini fark ettikçe trend haline geliyor.

Günümüzün gerçeklerinden olan doğal afetler dahi ESG ve AML uyumunun sağlanması için bir zorunluluk oluşturuyor. Günümüzde meydana gelebilecek deprem, sel gibi büyük afetlerin etki alanı büyüdükçe gerek sosyal yaşama gerekse de buna bağlı olarak finansal hizmetlere erişimi kesintiye uğratma potansiyeline sahip. Örnek olarak yakın zamanda Türkiye'de meydana gelen deprem ülkenin 10 büyük ilini ciddi bir yıkıma uğrattı, çok sayıda can kaybına ve büyük maddi hasara neden oldu. Depremden etkilenenler arasında finansal sektör de yer aldı. Böyle bir afet anında barınma, gıda, hijyen, güvenlik gibi birincil öneme sahip ihtiyaçların ardından finansal hizmetlerin kesintisiz sürdürülmesi de büyük öneme sahip hale geliyor. Gerek bireylerin afet döneminde ihtiyaçlarının karşılanması, gerekse bu bölgelerde gerçekleştirilecek başta afete yönelik yürütülen çalışmalar olmak üzere tüm faaliyetlerin yürütülmesinde doğru işleyen bir finansal hizmet ağının önemi de artıyor. Özellikle yardım faaliyetleri ve ödemelerin yürütülmesine yönelik olarak finansal systemin devre dışı kalması, bu afete maruz kalan kişiler açısından suistimal edilme risk doğurabilecektir. Böyle bir anda yardım faaliyetlerinin dolandıcılar ve benzeri kötü niyetli kişilerin kullanımından ayrıştırılabilmesi için finansal sistemin varlığının korunması kritik bir hale geliyor.

ESG ve AML uyumluluğunun entegrasyonu, şirketlerin etik ve yasal bir şekilde çalıştıklarından emin olmak için dikkate almaları gereken yeni ve önemli bir kavramdır. Bir şirketin çevresel ve sosyal etkileri gibi ESG faktörleri, bir yatırımın sürdürülebilirliğini ve toplumsal etkisini ölçmek için kullanılır. AML uyumluluğu ise kara para aklamayı ve diğer yasa dışı finansal faaliyetleri önlemek için bir dizi kanun ve düzenlemedir. Ancak bağlantı inkar edilemez; örneğin, güçlü ESG uygulamalarına sahip bir şirketin, yasa dışı ağaç kesimi veya ihtilaflı madenlerin ticareti gibi kara para aklamak için kullanılabilecek faaliyetlerde bulunma olasılığı daha düşük olabilir. Benzer şekilde, iş uygulamalarında şeffaf ve hesap verebilir olan bir şirketin kara para aklamayı gizlemek için kullanılabilecek faaliyetlerde bulunma olasılığı daha düşük.

Buna ek olarak, birçok yatırımcı artık yatırım kararlarına ESG faktörlerini dahil ediyor ve güçlü ESG ve AML uyumluluğu sergileyen şirketler arıyor. Bu, yalnızca sürdürülebilir ve sorumlu iş uygulamalarının desteklenmesine yardımcı olmakla kalmaz, aynı zamanda yatırımların yasa dışı faaliyetleri kolaylaştırmak için kullanılmamasını sağlamaya da yardımcı olur. Daha fazla yatırımcı, düzenleyici ve tüketici daha sürdürülebilir ve sorumlu iş uygulamaları talep ettikçe ve çevreye ve topluma zarar veren yasa dışı faaliyetleri kolaylaştırmak için kara para aklama potansiyeli daha belirgin hale geldikçe şirketler bu konu üzerinde çalışmaktadır. Güçlü ESG ve AML uyumu sergileyen şirketler, yatırımcılar için muhtemelen daha çekici olacak ve uzun vadede başarılı olma olasılığı daha yüksek olacaktır.

Geçen yıl, Menkul Kıymetler ve Borsa Komisyonu, daha önce de belirtildiği gibi, kayıtlı yatırım danışmanları, kayıtlı yatırım şirketleri ve diğerlerinin ESG yatırım uygulamalarına ilişkin zorunlu kılacak kural değişikliklerini duyurdu. Bu, finans sektöründe ESG hususlarının artan öneminin bir başka hatırlatıcısıdır. SEC, son yıllarda ESG ile ilgili hizmetlere ve yatırım ürünlerine önemli sermaye akışıyla birlikte ESG stratejilerine yönelik yatırımcı ilgisinin arttığını belirtti. SEC'in önerisi, finans sektöründe ESG ve AML uyumluluğunun artan öneminin açık bir göstergesidir.

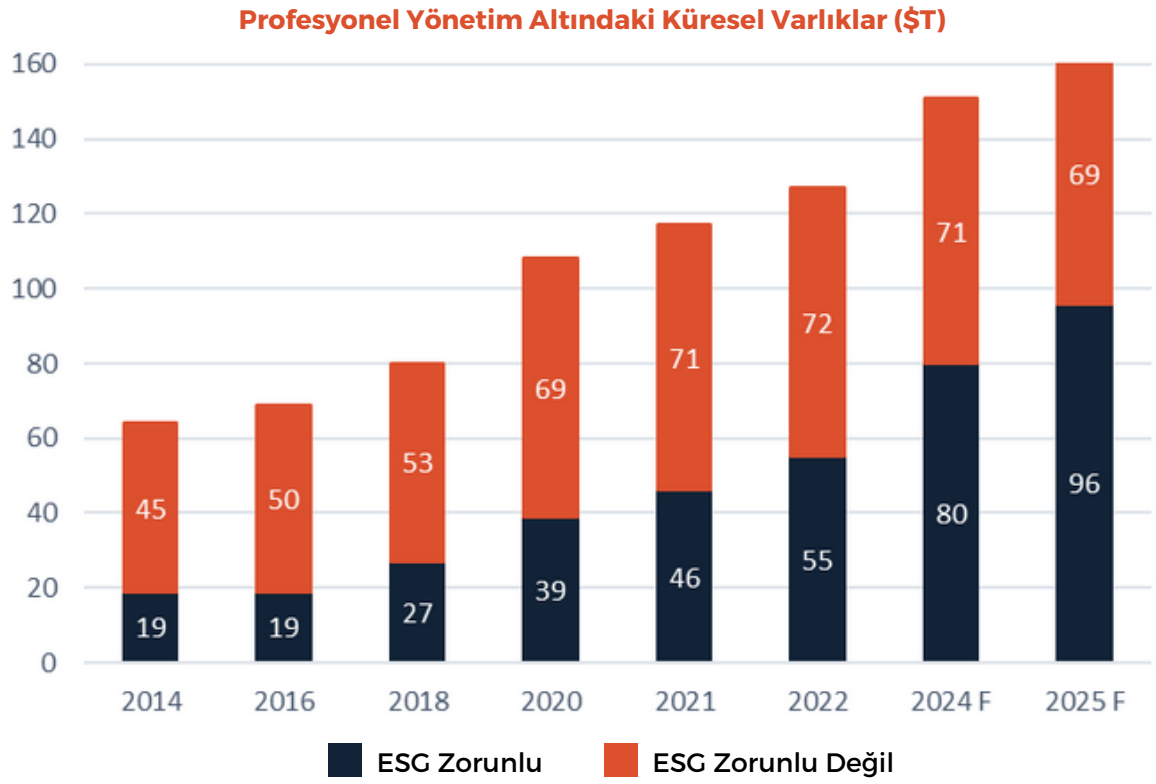
Ağaç kesme, madencilik, arazi temizleme, atık kaçakçılığı ve yasa dışı yaban hayatı ticareti gibi yasa dışı faaliyetler de dahil olmak üzere çevre suçları, önemli yasa dışı kazançlar sağlıyor ve küresel ekonomiden daha hızlı büyüyerek artıyor. Bu suçların soruşturulması ve kovuşturulması zor, çünkü yasa dışı varlıklar genellikle tedarik zinciri boyunca yasal varlıklarla karıştırılır ve sınır ötesi uygulama zor olabilir. Sonuç olarak, kara para aklama zemini olarak kabul edildikleri için bu suçlara yönelik artan bir düzenleyici ilgi bulunmakta.

ESG'nin sosyal bileşeni, şirketlerin insanlara nasıl davrandığını kapsar ve çalışan hakları, insan hakları ve tüketicinin korunması gibi konuları içerir. ESG ve AML arasındaki örtüşme alanlarından biri, önemli karlar sağlayan ve dünya çapında milyonlarca insanı modern zaman köleliğinin bir biçimi olarak etkileyen insan kaçakçılığıdır.

ESG'nin yönetişim bileşeni, pek çok biçim alan ve sürdürülebilir kalkınma hedeflerine ulaşma becerisi üzerinde önemli bir etkiye sahip olabilen yolsuzlukla mücadelede AML ile örtüşmektedir.

ESG ile ilgili suçları tespit etmek ve önlemek için şirketler, finansal aracılar tarafından kara para aklama gözetimi ve dolandırıcılık ve yolsuzlukla mücadele uyum sistemleri gibi sistemleri kullanabilir. Şirketler, ESG ve AML hususlarını genel risk yönetimi stratejilerine dahil ederek, yatırımlarının yasa dışı faaliyetleri kolaylaştırmak için kullanılmamasını sağlarken sürdürülebilir ve sorumlu iş uygulamalarını teşvik edebilir.

Kaynak: https://www.hlb.global/the-role-of-anti-money-laundering-monitoring-in-esg-compliance/



Finans sektörü, ESG ve AML uyumluluğunun entegrasyonuna artan bir önem vermektedir. SEC'in kayıtlı yatırım danışmanlarından ve şirketlerden ESG yatırım uygulamaları hakkında daha fazla bilgi talep etme yönündeki son teklifi bu eğilimi vurgulamaktadır. Yatırımcılar ESG stratejileriyle daha fazla ilgilenmeye başladıkça ve sürdürülebilir ve sorumlu iş uygulamalarına yönelik baskı arttıkça, şirketler hem ESG hem de AML uyumluluğunu dikkate aldıklarından emin olmalıdır. Yatırımcılar, düzenleyiciler ve tüketiciler de dahil olmak üzere daha fazla paydaşın daha sürdürülebilir ve sorumlu iş uygulamaları talep etmesi ve çevreye ve topluma zarar veren yasa dışı faaliyetleri kolaylaştırmak için kara para aklama potansiyelinin daha belirgin hale gelmesiyle birlikte, güçlü ESG gösterebilen şirketler ve AML uyumluluğu, yatırımcılar için muhtemelen daha çekici olacak ve uzun vadeli başarı şansı daha yüksek olacaktır.

Kaynak: https://www.hlb.global/the-role-of-anti-money-laundering-monitoring-in-esg-compliance/

Kripto Paranın Dinamik Dünyasında Gezinti

Kripto varlıklar da diğer geleneksel Finans araçları gibi suçlular tarafından suç gelirlerinin aklanması ve terörizmin finansmanı aracılığıyla kullanılabiliyor. Bununla birlikte kripto varlıkların. diğer finansal araçların sunamadığı bazı özellikleriyle suça ilişkin faaliyetler açısından artıları da bulunuyor. Kripto varlıklar yapıları gereği ağ üzerindeki trafiklerinin izlenebilmesi açısından büyük bir şeffaflık vaat ediyor. Herhangi bir cüzdan adresini kamuya açık ağ Kaynakları üzerinden sorgulayarak ilgili cüzdanın bakiyesini, bu cüzdana gelen ve giden transferleri görmek mümkün. Bununla birlikte bu duruma istisna oluşturan kripto varlıklar, bu alanı siber suçların kullanımı için daha açık bir hale getiriyor: anomim kripto varlıklar. Anonin kripto varlıklar genel olarak ağ üzerinden izlerinin sürülebilmesinin mümkün olmadığı şekilde tasarlanmış olan nitelikteki kripto varlıklar olarak adlandırılabilir. Bu kapsamdaki varlıklar, yukarıda bahsedilen ağ üzerinden takip edilme imkanını ortadan kaldırma sağlayabiliyor. Anomim kripto varlıkların kullanım ihtiyacının mahremiyet odaklı olduğunu savunanlar olsa da bu durumun özellikle suç geliri aklama, terörün finansmanı ve siber suçlarla bağlantılı olarak kullanımın önünü açtığı bir gerçek. Yapılacak olan mevzuat düzenlemelerinin bu kapsamdaki kripto varlıklara özel hükümler içermesi, anonim kripto varlıkların suç aktörlerince kullanım riskini azaltmak açısından önemlidir.

Kripto varlıkların suç gelirlerinin aklanması, terörizmin finansmanı ve siber suçlarla bağlantılı olarak kullanımını kolaylaştıran hizmetlerden birisi de mixer hizmetleridir. Mikser işlemleri bir kripto varlık transferini özel işlemlere tabi tutarak gönderici ve alıcı arasındaki bağı koparmak ve kripto varlıkların şeffaf yapısından ayrışmasını sağlayarak farklı kullanım amaçlarına açık hale getirmek şeklinde özetlemek mümkündür. Bu kapsamda A göndericisi B alıcısına transfer yapar fakat araya mikser hizmeti sunan bir aracı dahil olur ve A göndericisinin yaptığı transfer ilk olarak mikser hizmet sağlayıcısına ulaşır. İlk kullanıcıdan kripto varlık transferini alan aracı, bu işlemi mix ederek geçirdiği işlemler sonrasında B kullanıcısına gönderir. Böylece normal şekilde gerçekleştirildiğinde ağ üzerinden A kullanıcısından B kullanıcısına gerçekleştiği kolaylıkla izlenebilecek olan bir transfer işlemi mikser hizmeti sonucunda alıcı ve kullanıcı arasındaki bağı kesmiş ve işlemin şeffaflığını ortadan kaldırmış olacaktır. Bu şekilde gerçekleşen işlemlerinse yasadışı kullanım amacı taşıyan fonlar açısından büyük bir risk oluşturduğu açıktır. Bu işlemlerin de yine yasal düzenlemeler kapsamına alınması ve risklerin sınırlandırılması önemli hale gelmektedir. Mevcut durumda OFAC tarafından bu kapsamda yapılmış tespitler ve alınmış yaptırım kararları olduğu bilinmektedir.

Kripto Paranın Dinamik Dünyasında Gezinti

Kripto para dünyasında, son yıllarda ilgi gören iki moda kelime, diğer tüm konulardan daha fazla heyecan yaratan NFT'ler ve DeFi'dir. Değiştirilemez Token'ler (Non-Fungible Tokens-NFT'ler), kopyalanamayan benzersiz dijital varlıklardır. En yaygın olarak, sanatçıların dijital kreasyonlarını basıp koleksiyonerlere satabilecekleri sanat dünyasında kullanılırlar. Buna karşılık, DeFi veya merkezi olmayan finans, aracılara ihtiyaç duymadan P2P işlemlerine izin veren, blockchain teknolojisi üzerine inşa edilmiş yeni bir finansal sistemi ifade eder.

NFT'lerin popülaritesi, 2021'de birçok yüksek profilli sanatçı ve müzisyenin harekete geçmesiyle arttı. Şimdiye kadar satılan en pahalı NFT, müzayedede 69 milyon dolara satılan sanatçı Beeple'ın dijital sanat eseriydi. Bu, giderek artan sayıda sanatçı, müzisyen ve diğer içerik oluşturucunun çalışmalarından para kazanmanın yeni bir yolu olarak NFT'lerin olanaklarını keşfetmesine yol açtı.

Öte yandan DeFi, son birkaç yıldır ivme kazanıyor ve popülaritesi ancak 2023'te devam edecek. DeFi platformları, merkezi olmayan kripto para birimi ve diğer varlıkların ödünç alınmasına, ödünç alınmasına ve ticaretine izin veriyor. Bu, geleneksel finansal sistemleri bozma ve daha fazla insanın finansal hizmetlere erişmesine izin verme potansiyeline sahiptir. DeFi ayrıca yatırım için yeni fırsatların yanı sıra insanlara kripto para varlıklarından faiz kazanmaları için yeni yollar sunuyor.

Genel olarak, NFT'ler ve DeFi, önümüzdeki yıl için muazzam bir büyüme potansiyeli gösteriyor. Daha fazla insan bu yeni teknolojilere aşina oldukça, gelecekte muhtemelen daha da fazla yenilik ve benimseme göreceğiz. Her zaman olduğu gibi, herhangi bir yeni teknolojiye yatırım yapmadan önce bilgi sahibi olmak ve araştırma yapmanın önemini vurgulamakta fayda var.

NFT'ler

Değiştirilemez Token'ler (NFT'ler), bin yıllık çağımızın dijital sanatçıları için yeni bir alan olarak popülerlik kazanıyor. Bununla birlikte, herhangi bir yeni teknolojide olduğu gibi, NFT'lerin de kötüye kullanım potansiyeli bulunmakta. NFT'lerin güvenli olduğundan ve kara para aklamayı önleme (AML) kontrollerine sahip olduğundan emin olmak önemlidir.

2023 için NFT'lerle gözlemlenen en trend yasa dışı faaliyet biçimlerinden biri, kendi kendine işlemdir (wash trading). Bu, borsaların işlemlerini olduğundan daha büyük göstermeye çalıştığı kripto para birimi endüstrisinde yaygın bir endişe. Bir kişi, kendi kontrolü altındaki başka bir cüzdana satarak bir NFT'nin değerini yapay olarak artırmak için yıkama ticareti adı verilen bir taktik kullanabilir.

Kara para aklama, geleneksel sanat eserlerine ek olarak NFT'ler için başka bir ilgi alanıdır. Bireylerin fonların kaynağını gizleyerek kara para aklamak için NFT satın almaları mümkündür. Bu, yasa dışı fonlarla NFT'ler satın alarak ve daha sonra bunları meşru bir para birimi karşılığında satarak yapılabilir. NFT'lerin değişken fiyatları, onu ekonomideki kötü aktörler için cazip kılan diğer bir özelliktir. Bir NFT reddedilmeden bir milyon dolar veya daha fazla fiyatlandırılabilir ve fiyatları kontrol etme yetkisi yoktur. Bu oynaklık, NFT işlemlerinin anonimliği ve sektördeki AML düzenlemelerinin olmaması, onu kara para aklayıcılar için birincil hedef haline getiriyor. Dahası, dijital bir sanat formu olmak, lojistik süreci diğer sanat eserlerini çalmaktan daha kolay hale getiriyor.

Bu sorunlarla mücadele etmek için, NFT pazar yerlerinin ve projelerinin AML mekanizmalarını uygulaması önemlidir. Bu, kullanıcılar için kimlik doğrulaması gerektirmeyi, işlem izleme sistemlerini uygulamayı ve yasadışı faaliyetleri tespit etmek ve önlemek için kolluk kuvvetleriyle işbirliği yapmayı içerebilir. Ek olarak, düzenleyiciler uygun AML düzenlemelerini geliştirmek ve uygulamak için sektörle birlikte çalışmalıdır.

Sanatçı Pak'ın The Merge adlı eseri, **91.8 milyon dolarlık** bir meblağ karşılığında dünyada satılan en pahalı NFT'dir.

Kaynak:: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/

NFT pazarının 2021-2022'de 44 milyon dolar olacağı tahmin ediliyor.

OpenSea: en büyük NFT pazarı, aynı zamanda en çok kullanılanıdır.

Bu sorunlarla mücadele etmek için, NFT pazar yerleri ve platformlarının müşterini tanı (KYC) ve kara para aklamayı önleme (AML) prosedürlerini uygulaması önemlidir. Ulusal düzenleyicilerin çoğu yakın zamanda kripto para birimlerini düzenlemeye yetişmiş olsa da, NFT'ler gri bir alana düşüyor ve mevcut yasalar kapsamında olması gerekmiyor. Bununla birlikte, NFT'lerin artan popülaritesi ve işlem hacimleriyle birlikte, düzenleyicilerin AML kapsamlarını NFT'leri içerecek şekilde genişletmeleri yalnızca bir zaman meselesidir.

NFT'ler dijital varlıklardan para kazanma biçimimizde devrim yaratma potansiyeline sahip olsa da, potansiyel riskleri göz önünde bulundurmak ve yatırımcılar ve şirketler için bunları azaltmak için adımlar atmak önemlidir. KYC prosedürlerini ve AML uyum programlarını uygulayarak ve düzenleyicilerle çalışarak, NFT pazarları ve platformları kitlesel benimsemeyi artırabilir, kurumsal yatırımcıları çekebilir ve kara para aklama planlarına karışmaktan kaçınabilir. Ayrıca ceza ve cezalardan kaçınmak için platformların yönetmeliklere uygun olması önemlidir. Böylece, NFT endüstrisi, kullanıcılarının güvenliğini ve güvenliğini sağlarken büyümeye ve gelişmeye devam edebilir.

2021'de bir ayda 1,5 milyondan fazla NFT satışı kaydedildi.

NFT satışlarının %50'den fazlası 200$'a ulaşmıyor.

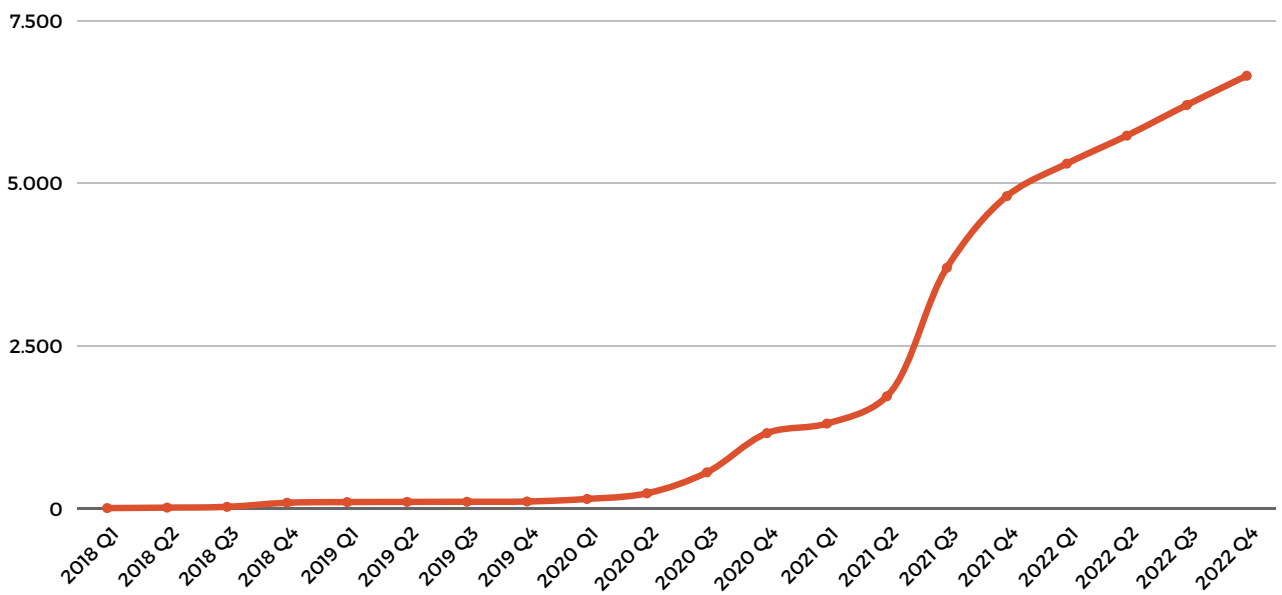
Kaynak: https://www.idnow.io/blog/nft-non-fungible-tokens-new-art-money-laundering/

DeFi

Merkezi Olmayan Finans (DeFi), 2020'lerin başından bu yana kripto para birimi endüstrisinde en hızlı büyüyen sektörlerden biri oldu. DeFi, blok zincirleri tarafından oluşturulan finansal protokolleri, uygulamaları ve hizmetleri ifade eder. DeFi'nin en göze çarpan özelliği, ekonominin aracılarını devre dışı bırakmasıdır. Bu nedenle ekstra fiyatları ve işletme maliyetlerini düşürür ve her kullanıcı için açık bir alan sağlar.

DeFi'nin yükselişi, 2021'de yaklaşık %6.600'lük bir büyümeyle, 40 milyar dolarlık kilitli bir toplam değere ulaşarak şaşırtıcı oldu. DeFi daha fazla ilgi ve popülerlik kazandıkça, ölçeklenebilirlik ve düzenleme gibi zorluklarla da karşı karşıya. Geleneksel Merkezi Finans (CeFİ) kripto varlık alanındaki pek çok kişi düzenlemenin meşrulaştırma getirdiğine inanıyor ancak konu DeFı alanı olduğunda bu görüş genellikle desteklenmiyor. Bununla birlikte, DeFi projelerinin düzenlemeye karşı bağışık olmadıklarını ve potansiyel uyumluluk sorunlarını proaktif olarak ele almanın kendi çıkarlarına olduğunu anlamaları önemlidir.

Dünya Çapında Satılan DeFi Varlıklarının Sayısı



DeFi'nin büyümesinin AML düzenlemeleri için önemli etkileri vardır. DeFi popülerlik ve kullanım kazanmaya devam ettikçe, düzenleyicilerin bu protokolleri ve kara para aklama için oluşturdukları potansiyel riskleri daha yakından incelemesi muhtemeldir. DeFi projeleri, uyumluluğa proaktif bir yaklaşım benimsemeli ve ekosistem içinde güven oluşturmak için düzenleyicilerle birlikte çalışmalıdır. Bu, AML kontrollerini akıllı sözleşmelere dahil etmeyi, finansal suç riski göstergelerini ve puanlarını entegre etmeyi ve akıllı sözleşme denetimleri yapmayı içerebilir.

Uygulanan düzenlemelerin şekillendirilmesine ve DeFı projeleri için en iyi sonuçların sağlanmasına yardımcı olabileceğinden, düzenleyicilerle işbirliği de çok önemlidir. Uyum bir engel olarak değil, ekosistem içinde güven ve güvenilirlik oluşturmanın bir aracı olarak görülmelidir. Mali Davranış Otoritesi zaten bir DeFi kuruluşuna kayıt vermiştir ve daha fazla düzenlemenin takip etmesi muhtemeldir.

Defi'nin gelişiminin ilk aşamalarında olduğunu ve birçok anahtar kavram ve mekanizmanın hala geliştirildiğini belirtmekte fayda var. Bu nedenle, önümüzdeki yıllarda, özellikle düzenleyici açıklık açısından birçok şey değişebilir. Büyümenin devam etmesiyle birlikte, merkezi olmayan finans için güvenli ve gelecek vaat eden bir gelecek sağlamak için DeFi projelerinin eğrinin önünde kalması ve uyum sorunlarını proaktif olarak ele alması çok önemlidir.

Türkiye'de Neler Bekleniyor?

2021 yılını pandeminin olumsuz etkileri ile geçirdikten sonra, tüm dünya gibi Türkiye'de 2022'ye büyük bir umutla başlamıştı. Özellikle kripto para piyasasında yaşanan gelişmeler insanların ilgisini çekmiş ve piyasada yoğunluk oluşmuştu. Fakat ne yazık ki, beklentilerin tam tersinin gerçekleştiği bir yıl oldu. Terra ve FTX gibi büyük platformların çöküşlerinden sonra ekosistem büyük zarar gördü. Yaşanan krizlerden sonra kriptoya bağlı sistemlerin problemli olduğunun ortaya çıktığı düşünülmeye başlanırken aynı zamanda enflasyon problemi tüm dünyada artış gösteriyordu. Bununla birlikte kripto paralara olan ilginin enflasyondan korunmak için artacağı beklenmeye başladı. Bütün bu gelişmeler de regülasyonları daha sık gündeme getirdi.

Türkiye'de kripto varlıklar ve hizmet sağlayıcılar için regülasyon çalışmaları 2021'den beri devam ediyor. Cumhurbaşkanı Recep Tayyip Erdoğan, Blokzincir İstanbul etkinliğinde yaptığı konuşmada blokzincir teknolojisinin popüler olmasını kripto paraların sağladığını ve bu teknolojinin mevcut finansal sistemi kökten değiştirme potansiyeline sahip olduğunu vurguladı. Ayrıca, dijital varlık teknolojinin yakıtı olan blokzincir teknolojisinin verimli, hızlı ve güvenli özelliklerine dikkat çekti. Cumhurbaşkanı, kamu kuruluşlarında ve Türkiye'deki üniversitelerde bu alanda katkı sağlayacak projelerin hayata geçirilmeye devam edileceğini ve Türkiye'nin bu alandaki potansiyelini değerlendirmek istediğini belirtti.

Bu açıklamalar, kripto para ekonomisinde en büyük pazarlardan birine sahip olan Türkiye'nin blokzincir teknolojisi konusundaki tutumunu ve gelecekteki yöneliminin ne yönde olacağını gösterdi. Genel seçim sonrası kripto para borsalarını düzenleyen bir yasanın meclise geleceği öngörüler arasında yer aldı. Aynı zamanda regülasyonlar ile birlikte bu alana yatırımların artacağı da beklentiler arasına eklendi.

NFT alanında da hızla büyüyen bir pazara sahip olan Türkiye'nin, projeler ile birçok ilke imza attığı görülüyor. NFT'ye ilgi gösteren ülkeler arasında 3. sırada yer alan Türkiye'deki NFT pazar büyüklüğünün 2028'de 4458,6 milyon USD'ye çıkması öngörülüyor.

Bizimle İletişime Geçin

27 Old Gloucester Street, London,
United Kingdom, WC1N 3AX

+44 20 4577 0427

Yıldız Teknik Üniversitesi Teknopark
C-1 Blok No: 106-8 Esenler, Istanbul, Türkiye

+90 (212) 963 01 84

info@sanctionscanner.com

sanctionscanner.com