

Başvuru Dolandırıcılığını Önleyin

Ürünlerimiz > Bilgi Güvenliği

Başvuru Dolandırıcılığı Tespit

Platformumuz, sentetik kimlikler, sahte adresler ve organize dolandırıcılık çeteleri gibi karmaşık dolandırıcılıkları başvuru aşamasında tespit ederek finans kuruluşlarını korur. Gelişmiş kural motoru ve yapay zeka motoru sayesinde şüpheli başvuruları engeller. Bu, hem finansal kayıpları azaltır hem de operasyonel verimliliği artırırken, meşru başvuruların gecikmeden işlenmesini sağlar.



Başvuru Dolandırıcılığı Nedir?

Başvuru Dolandırıcılığı, başta finans ve bankacılık olmak üzere birçok sektörde yaygın bir siber dolandırıcılık yöntemidir. Bu tür dolandırıcılıkta, şahıslar veya gruplar, sahte ya da çalıntı kimlik, gelir ve adres bilgileri gibi verilerle finansal ürünlere başvurur. **Bu başvurular, hesap açılışları veya kredi kartı talepleri gibi çeşitli şekillerde olabilir ve sahte belgeler ya da manipüle edilmiş bilgiler içerebilir. Kurumlardaki yetersiz güvenlik önlemleri, bu durumun maddi kayıplara ve hukuki problemlere yol açmasına neden olur.**

Öne Çıkan Özellikler

Başvuru Dolandırıcılığı tespit platformumuz, makine öğrenimi ve veri analizi kullanarak başvuru süreçlerindeki dolandırıcılığı erken ve doğru bir şekilde tespit eder. Temel özellikleri arasında gerçek zamanlı tespit, makine öğrenimi destekli analiz, kapsamlı veri entegrasyonu, anomali tespiti, risk puanlama sistemi, özelleştirilebilir kurallar, detaylı raporlama, kullanıcı dostu arayüz ve ölçeklenebilirlik bulunur. **Platform, finans, e-ticaret, telekomünikasyon, sigorta ve perakende gibi sektörlerde işletmelerin güvenliğini ve karlılığını artırmayı hedefler.**



Gerçek Zamanlı Analiz: Başvurular sisteme ulaştığı anda, gelişmiş algoritmalarımız ve yapay zeka destekli analiz motorumuz anında devreye girer. Bu sayede, olası dolandırıcılık riskleri saniyeler içinde belirlenir. Finans kuruluşları için hızlı ve doğru karar alma imkanı sunularak hem kayıplar en aza indirilir hem de operasyonel verimlilik artırılır.



Sentetik Kimlik Tespiti: Gelişmiş veri analizi ve yapay zeka yöntemleri kullanarak, sentetik kimliklerin ve bunlarla ilişkili sahte bilgilerin kökenini tespit edilir. Bu sayede, geleneksel sistemlerin gözden kaçırdığı, gerçek mağduru olmayan sofistike dolandırıcılık türlerini başvuru aşamasında yakalanır ve finansal kayıpları önlenir.

Başvuru Dolandırıcılığını Önleyin

Ürünlerimiz > Bilgi Güvenliği



Sahte Adres ve Bilgi Doğrulama: Başvuru sahiplerinin sağladığı adres, telefon ve e-posta gibi bilgiler, güvenilir harici veri tabanları ve tescilli kaynaklar kullanılarak doğrulanır. Bu çapraz kontrol, bilgilerin gerçekliğini ve tutarlılığını teyit eder. Böylece, potansiyel dolandırıcılık girişimleri ve sahte kimlikler başvuru sırasında tespit edilir.



Kural ve Yapay Zeka Motoru: Çözümümüz dolandırıcılık trendlerini yakından takip eden ve sürekli güncellenen esnek kural setlerini, geçmiş verilerden öğrenen gelişmiş makine öğrenimi modelleriyle birleştirir. Bu hibrit yaklaşım, hem bilinen dolandırıcılık kalıplarına karşı anında koruma sağlar hem de yeni ortaya çıkan, karmaşık tehditleri otomatik olarak tespit etme yeteneği sunar. Böylece, operasyonel ekiplerin yükünü azaltırken, finansal kayıpları en aza indirerek kuruluşların her zaman bir adım önde olmasını sağlar.



Davranışsal Analiz: Başvuru formunun doldurulma hızı, kullanılan cihaz bilgisi ve IP adresi gibi parametreler incelenerek, insan dışı veya dolandırıcılık amaçlı olabilecek olağan dışı davranış kalıpları tespit edilir. Bu sayede, potansiyel riskler henüz başvuru anında belirlenerek otomatik olarak engellenir veya ek incelemeye yönlendirilir.



Gelişmiş Raporlama ve Uyarı Sistemleri: Platformumuz, tespit edilen dolandırıcılık girişimlerine dair kapsamlı ve detaylı raporlar sunar. Bu raporlar, dolandırıcılık eğilimlerini anlamana yardımcı olurken, ilgili departmanlara anında otomatik uyarılar gönderilerek hızlı müdahale imkanı sağlar. Bu sayede, operasyonel ekiplerin etkinliği artırılır ve finansal kayıplar minimize edilir.

Şüpheli Başvuruları Nasıl Tespit Ediyoruz?

Sahtekarlar, kimliklerini gizlemek veya çoklu hesaplar oluşturmak amacıyla isim ve adres bilgilerinde kasıtlı olarak küçük değişiklikler yapma veya yazım hataları kullanma eğilimindedir.

Gelişmiş Fuzzy Match (Yaklaşık Eşleşme) algoritmamız, bu tür küçük tutarsızlıkları, yazım hatalarını ve hatta kasıtlı değişiklikleri bile olağanüstü bir hassasiyetle yakalar. Bu algoritma, tam eşleşme olmasa bile belirli bir benzerlik oranına sahip verileri tespit ederek, sahtekarlık girişimlerinin gözden kaçmamasını sağlar. Örneğin, "Mehmet Yılmaz" yerine "M. Yılmaz" yazılması veya adreslerdeki küçük harf-büyük harf farkları gibi detaylar bu algoritma sayesinde kolaylıkla tespit edilebilir. Bu özellik, sahtekarların kullandığı en yaygın gizlenme yöntemlerinden biri olan bu tür varyasyonları etkisiz hale getirir.



Başvuru Dolandırıcılığını Önleyin

Ürünlerimiz > Bilgi Güvenliği

Sentetik kimlikler, genellikle tamamen uydurma bilgilerle veya farklı kişilere ait bilgilerin bir araya getirilmesiyle oluşturulan kimliklerdir. Bu tür sentetik kimliklerin gizlenmesinde en sık başvurulan yöntemlerden biri sahte adres kullanımıdır. Sahte Adres Tespiti motorumuz, bu sahte adres kullanımını etkili bir şekilde engeller. Motorumuz, adreslerin gerçekliğini, geçerliliğini ve geçmişte sahtekarlık faaliyetlerinde kullanılıp kullanılmadığını analiz eder. Coğrafi veri tabanları, posta kodu doğrulamaları ve bilinen sahtekarlık kalıplarıyla entegre çalışarak şüpheli adresleri anında tespit eder. Bu sayede, sahtekarların kurduğu karmaşık ağlar ve oluşturduğu sahte kimlikler ortaya çıkarılır.

Başvuru Risk Skoru Nasıl Hesaplanıyor?

Geleneksel dolandırıcılık tespit yöntemleri sadece uyarılar sunarken, platformumuz şeffaf bir risk puanı sağlar. Bu puan, bir başvuru veya işlemin dolandırıcılık potansiyelini belirtirken, aynı zamanda bu olasılığın altında yatan temel nedenleri de net bir şekilde açıklar. Risk skorumuz, kapsamlı veri analiziyle desteklenir. **Bu sayede, sahtekarlık riskini ve nedenlerini (IP adresi, tutarsız bilgiler, anormal işlem deseni gibi) niceliksel olarak ölçebilirsiniz, riskin somut verilere dayandığını net bir şekilde görebilirsiniz.**

Bu kapsamlı risk skoru sayesinde, operasyonel süreçlerinizi önemli ölçüde optimize edebilirsiniz:

Otomatik Onay/Red Kararları



Düşük riskli başvurular için sistem tarafından otomatik onay kararları verilebilir. Bu, manuel inceleme gereksinimini azaltır ve süreçleri hızlandırır. Benzer şekilde, çok yüksek ve bariz sahtekarlık riski taşıyan başvurular otomatik olarak reddedilerek insan kaynaklarının gereksiz yere meşgul edilmesi önlenir. Bu otomasyon, karar verme süreçlerinizde güven ve verimlilik sağlar.

Manuel İnceleme için Önceliklendirme



Yüksek riskli başvurular/işlemler, manuel inceleme için otomatik olarak önceliklendirilir. Bu sayede insan kaynakları en çok dikkat gerektiren alanlara odaklanır. Analistler, her başvuruyu baştan sona incelemek yerine, sistemin belirlediği potansiyel risk noktalarına odaklanarak hızlı ve isabetli kararlar alabilir. Bu önceliklendirme, operasyonel verimliliği artırır ve sahtekarlıkla mücadelede proaktif bir yaklaşım sağlar.

Başvuru Dolandırıcılığını Önleyin

Ürünlerimiz > Bilgi Güvenliği

Mastercard Ekata Modülü

Mastercard Ekata Modülümüz, kimlik doğrulama süreçlerinde yüksek güvenlik ve hassasiyet sunar. Gelişmiş analitik yetenekleri ve geniş kapsamlı veritabanı sayesinde dolandırıcılık risklerini en aza indirir ve kullanıcının sağladığı bilgileri hızlı ve güvenilir bir şekilde doğrular. Ad, soyad, telefon numarası, e-posta adresi, IP adresi ve fiziksel adres gibi parametrelerle kimlik doğrulama ve dolandırıcılık riski skorları sunar.



Ayrıca, demografik bilgiler ve coğrafi konum analizi sağlayarak daha kapsamlı kullanıcı profilleri oluşturur.

Özetle, adres, e-posta ve telefon doğrulama ihtiyaçlarını tek bir çözümle karşılar. Bu özellikleriyle, başvuru ve hesap açılışı dolandırıcılığına karşı oyun, e-ticaret ve fintech sektörleri için idealdir.

Kimler için Uygun?

Finans Kuruluşları



Finansal kurumlar ve kredi sağlayıcıları, başvuru sahtekarlığı gibi dolandırıcılık yöntemlerinden kaynaklanan ciddi finansal ve itibari risklerle karşı karşıyadır. Sahte kimlikler ve tahrif edilmiş bilgiler kullanarak kredi ve finansal ürünlere erişim çabasıyla gerçekleştirilen bu sahtekarlıklar, doğrudan finansal kayıplara ve kurumların güvenilirliğinin zedelenmesine neden olmaktadır.

Kripto Varlık Hizmet Sağlayıcılar



Kripto Varlık Hizmet Sağlayıcıları (KVHS'ler), dijital varlık piyasasındaki büyümeyle birlikte başvuru ve sahte hesap dolandırıcılığı tehditleriyle mücadele etmektedir. Etkili bir Başvuru Dolandırıcılığı Çözümü, sahte ve sentetik kimlikler ile tekrarlanan erişim gibi dolandırıcılık göstergelerini proaktif olarak tespit ederek finansal kayıpları ve itibar zedelenmesini önler. Otomatik risk değerlendirmesi ve yapay zeka analizleri sayesinde dolandırıcılık engellenir, maliyetler düşer ve yasal düzenlemelere uyum sağlanır.

Fintechler



Fintech'lerde başvuru anındaki dolandırıcılık tespiti hayati öneme sahiptir. Manipüle edilmiş kimlikler ve "Bust-out" yöntemleri yaygın dolandırıcılık yöntemleridir. Bu yöntem, sahte kimliklerle hesap açıp kredi limitlerini sonuna kadar kullanarak borçlarını ödemediği ortadan kaybolmayı kapsar.

Başvuru Dolandırıcılığını Önleyin

Ürünlerimiz > Bilgi Güvenliği

E-ticaret ve Online Servisler



Dijital dünyada hesap açılışı sahtekarlığı (promosyon avcılığı, kupon suistimali, iade dolandırıcılığı) işletmeler için büyük bir sorun olup gelir kaybı ve itibar zedelenmesine yol açar. Bu sahtekarlığın önlenmesi, gerçek müşteri tabanı oluşturma, gelir ve müşteri sadakati artışı, pazarlama verimliliği, marka itibarı korunması ve operasyonel maliyetlerin azalması gibi faydalar sağlar. Uygulama sahtekarlığı tespit ve önleme sistemleri, işletmelerin finansal kayıpları önleyip sürdürülebilir başarıya ulaşması için kritik öneme sahiptir.

Online Oyun Firmaları



İşletmenizi bonus, kampanya ve promosyon suistimaline karşı korumanızı sağlar. Dijital dünyada organize sahtekarlık ağları, otomatik botlarla çoklu hesaplar oluşturarak pazarlama bütçenizi tüketir ve adil rekabet ortamını bozar. Gelişmiş çözümümüz sayesinde IP analizi, davranışsal izleme ve yapay zeka kullanarak sahte hesapları tespit edebilir, kampanya ve bonus suistimalini engelleyebilirsiniz. Makine öğrenimi tabanlı çözümümüz, yeni sahtekarlık taktiklerini öğrenerek gelecekteki suistimalleri önler ve sizi rakiplerinizin bir adım önünde tutar. Adil bir sistem sunarak müşteri güvenini ve memnuniyetini artırın. Güvenilir bir platform, kullanıcı tabanınızı ve marka değerinizi güçlendirir.

Başvuru Dolandırıcılığı Senaryoları

Dolandırıcılar, genellikle kredi kartı başvuruları, banka kredileri, sigorta poliçeleri veya diğer finansal hizmetler için başvuru süreçlerini hedef alırlar. **Her senaryo, farklı bir yaklaşım ve farklı risk profilleri sunar.**

Sentetik Kimlik Sahtekarlığı



Sentetik kimlik dolandırıcılığı, en sofistike türlerdendir. Dolandırıcılar, gerçek TC kimlik numarası gibi doğrulanabilir bir bilgiyi sahte kişisel verilerle birleştirerek "sentetik" bir kimlik yaratır. Bu kimlikle düşük limitli hesaplar açıp düzenli ödemelerle kredi notunu yükseltirler. Yeterli limite ulaştıklarında, tüm limitleri kullanıp ortadan kaybolurlar. Gerçek bir mağduru olmadığı için tespiti zor ve finansal kurumlara büyük zarar verir.



Üçüncü Taraf Sahtekarlığı (Kimlik Hırsızlığı)

Bu, kamuoyunda en çok bilinen ve en yaygın dolandırıcılık türüdür. Dolandırıcı, başka bir kişinin tüm kişisel bilgilerini yasa dışı yollarla ele geçirir. Bu bilgiler arasında isim, adres, doğum tarihi, Sosyal Güvenlik Numarası/TC Kimlik Numarası, anne kızlık soyadı ve hatta banka hesap bilgileri bulunabilir. Dolandırıcı, çaldığı bu bilgileri kullanarak mağdurun adına haberi olmadan yeni hesaplar açar, kredi başvuruları yapar, telefon sözleşmeleri imzalar veya mevcut hesaplara erişim sağlamaya çalışır. Bu tür dolandırıcılıkların tespiti, mağdurun hesap ekstresinde veya kredi raporunda beklenmedik işlemler görmesiyle ya da borç tahsilat ajanslarından gelen bildirimlerle gerçekleşir. Kimlik hırsızlığı, mağdurlar için finansal ve duygusal açıdan yıkıcı sonuçlar doğurabilir.



Birinci Taraf Sahtekarlığı

Başvuru sahibi, gerçek kimliğini kullanarak finansal durumunu kasıtlı olarak yanlış beyan eder. Kredi onayı, daha yüksek limit veya uygun ödeme koşulları elde etmeyi hedefler. Gelirini şişirebilir, sahte belgeler sunabilir veya mevcut borçlarını gizleyebilir. Örneğin, gelirini %50 fazla gösterebilir veya başka banka borçlarını beyan etmeyebilir. Genellikle amacı, alınan krediyi geri ödememektir. Birden fazla kuruma aynı anda başvurup borçları ödemediği ortadan kaybolarak kurumlara büyük kredi kayıpları yaşatırlar.



'Bust-Out' Sahtekarlığı

Dolandırıcılar, yeni kredi kartları veya hesaplarla örnek müşteri gibi davranarak güven kazanır. Küçük harcamaları düzenli ödeyerek kredi notlarını yükseltir ve daha yüksek limitlere ulaşırlar. Yeterli limite ulaştıklarında, tüm limiti aniden kullanır veya nakit avans çekerler ve borçlarını ödemediği ortadan kaybolurlar. Bu "bust-out" dolandırıcılıklarını tespit etmek zordur, çünkü başlangıçta şüpheli davranış sergilenmez.

Başvuru Dolandırıcılığını Önleyin

Ürünlerimiz > Bilgi Güvenliği



Dijital Manipülasyon

Gelişmiş yazılımlar (örneğin, Adobe Photoshop, Illustrator gibi programlar) kullanılarak mevcut belgelerde değişiklik yapılır. Maaş bordrolarındaki gelir miktarları, banka ekstrelerindeki bakiye bilgileri, faturalardaki adres detayları veya kimlik belgelerindeki fotoğraflar değiştirilebilir. Örneğin, 5.000 TL olan bir maaş 15.000 TL olarak gösterilebilir, veya düşük bakiyeli bir banka ekstresi yüksek bakiyeli hale getirilebilir.



Sahte Belge Üretimi

Bazı durumlarda, dolandırıcılar sıfırdan tamamen sahte belgeler üretirler. Bu, sahte kimlik kartları, pasaportlar, elektrik/su faturaları, maaş bordroları veya banka referans mektupları olabilir. Bu belgeler, profesyonel baskı teknikleri ve gerçek belgelere benzer güvenlik özellikleriyle üretilerek tespiti zorlaştırılabilir. Amaç, başvuru sahibinin gelirini, adresini, kimliğini veya istihdam durumunu yanıltıcı bir şekilde doğrulamaktır.