feedzai

Fraude de abertura de conta

fiserv. Santander LLOYDS BANKING GROUP

O processo de criação de conta online pode dar início a um relacionamento vitalício com um cliente legítimo e a respectiva instituição financeira. Ou pode dar a criminosos a oportunidade de criar contas de laranja, explorar ofertas promocionais ou abusar de serviços financeiros. Fraudadores usam PII (informações de identificação pessoal) roubadas, fraude de identidade sintética e bots para cometer fraudes de abertura de conta digitalmente. Muitas vezes, eles podem passar despercebidos por meses após a criação da conta – levando a graves perdas financeiras e até mesmo a reprimendas regulatórias.

Pare os fraudadores na porta de entrada

Identifique solicitações fraudulentas

Tire proveito da inteligência de dispositivos, da biometria comportamental e dos dados de rede para quantificar o risco de fraude. Defenda sua empresa contra tentativas de preenchimento de credenciais, identidades sintéticas, ataques de bots e contas de laranja.

Alinhe os processos de abertura de conta digital

Obtenha insights claros e unificados em uma interface do usuário para diferenciar candidatos fraudulentos de candidatos genuínos. Acelere com segurança o processo de criação de conta e crie receitas adicionais ao não recusar clientes verdadeiros.

Aumente a eficiência operacional e economize custos

Consuma indicadores de risco por meio de uma API REST que enriquece os sistemas downstream. Obtenha decisões contextuais sobre a probabilidade de abertura de uma conta fraudulenta. A detecção precoce de fraudes no processo de integração elimina etapas dispendiosas de verificação de identidade de terceiros.

Características principais

Inteligência de dispositivos

Determine se o dispositivo foi adulterado. Investigue se alguém o utilizou em outras solicitações. Avalie se o dispositivo está em uma lista de dispositivos fraudulentos conhecidos. Meça a probabilidade de haver contas de laranja, identidades sintéticas ou abuso de crédito na abertura de contas.

Análise de rede e geolocalização

Identifique anomalias na geolocalização e em endereços IP em comparação com os dados da solicitação. Entenda se alguém já usou a rede para outras solicitações. Verifique se uma conexão proxy, TOR ou VPN está mascarando a rede verdadeira.

Monitoramento de comportamentos não humanos

Identifique o uso de scripts, automação ou emulação para ataques de força bruta. Pare os bots antes que eles abram centenas de contas falsas em poucos minutos.

Cobertura para Web e dispositivos móveis

Encontre o usuário no canal de integração preferido dele. Implemente os SDKs e os coletores de JavaScript da Feedzai para realizar análises de risco precisas em solicitações feitas pela Web e por dispositivos móveis.

Biometria comportamental

Analise as nuances de como o titular da conta interage com seu aplicativo. Os indicadores de risco de fraude incluem atalhos de teclado, padrões de navegação suspeitos, fluência na entrada de dados e experiência em formulários dos usuários.

Prêmios e reconhecimentos

Quadrant Knowledge Solutions — A Feedzai foi nomeada líder em Biometria comportamental

datos INSIGHTS — A Feedzai foi nomeada concorrente líder em Biometria comportamental

FORRESTER® — A Feedzai foi reconhecida na categoria "Desempenho Forte em Gestão de Fraudes Corporativas"

Pronto para atualizar sua estratégia de prevenção de fraudes?

Fale com um especialista