pipl

Identidade online e a economia digital do futuro

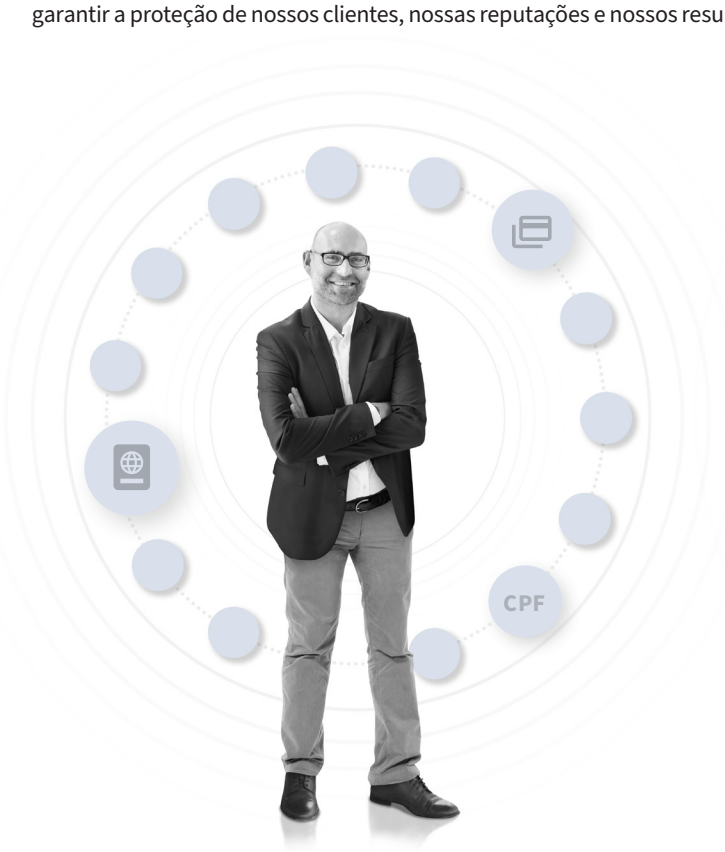
O contexto histórico

O atual ambiente digital de pagamento e verificação foi estabelecido em uma infraestrutura projetada para a verificação tradicional de pagamentos, com base em crédito e débito. A segurança das transações dependia de um ambiente com cartões físicos. A identidade era verificada com a apresentação de documentos oficiais tradicionais, como carteira de habilitação, número de seguro social ou algum outro documento emitido pelo governo. Esses documentos apontavam para vínculos físicos com o cliente, como endereços e números de telefone.

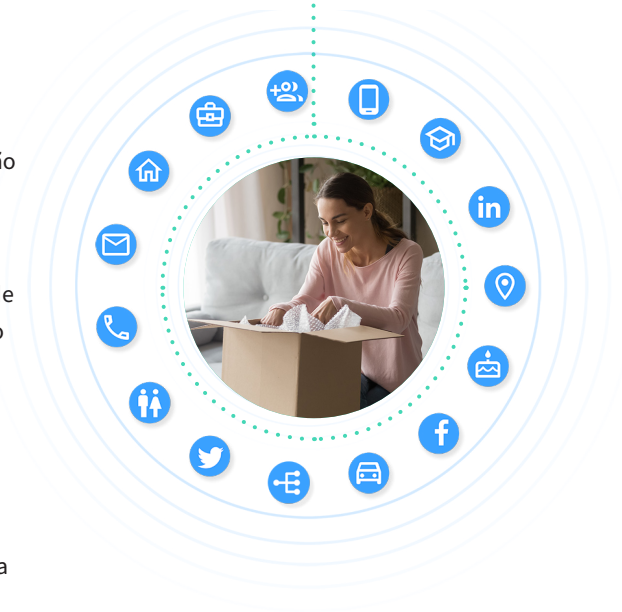
Outros elementos de verificação foram sendo adicionados. Senhas e números de identificação pessoal (PINs) aprimoraram a segurança das transações tradicionais, mas também aumentaram o atrito com o cliente e trouxeram uma nova geração de desafios tecnológicos.

Na virada para o século 21, as organizações começaram a migrar para ambientes de transações online e perceberam que era inadequado confiar exclusivamente na antiga infraestrutura de verificação para administrar os riscos transacionais. A tendência é que os métodos tradicionais continuem cedendo espaço para as interações online e pagamentos eletrônicos, e as organizações precisam desenvolver estratégias adaptáveis para lidar com o crescente número de ameaças ao atual ambiente de comércio eletrônico.

Com a entrada do comércio na era digital, as inadequações dos métodos tradicionais de verificação e autenticação se acentuaram e ficaram mais evidentes. O mundo online nos permite interagir com inúmeros desconhecidos ao redor do mundo real, sem qualquer confirmação física de que eles realmente são quem alegam ser. Isso exige o desenvolvimento de novas maneiras de garantir a proteção de nossos clientes, nossas reputações e nossos resultados.



O cenário atual



Falsos positivos, falsos negativos e desafios reais

Usar apenas métodos tradicionais de verificação não é o suficiente para atender às necessidades da maioria das organizações digitais. Torna-se cada vez mais importante — e frequentemente mais difícil — identificar usuários maliciosos que tentam tirar vantagem de um ambiente online. Também é cada vez mais difícil identificar usuários legítimos, que podem demonstrar um comportamento mais arriscado que o normal. Os clientes já não se enquadram mais em simples padrões de "alto risco" e "baixo risco", o que leva a um aumento nos casos de falsos positivos.

Infelizmente, as diligências necessárias para identificar transações fraudulentas com precisão podem afetar negativamente a experiência de clientes legítimos e os resultados financeiros.

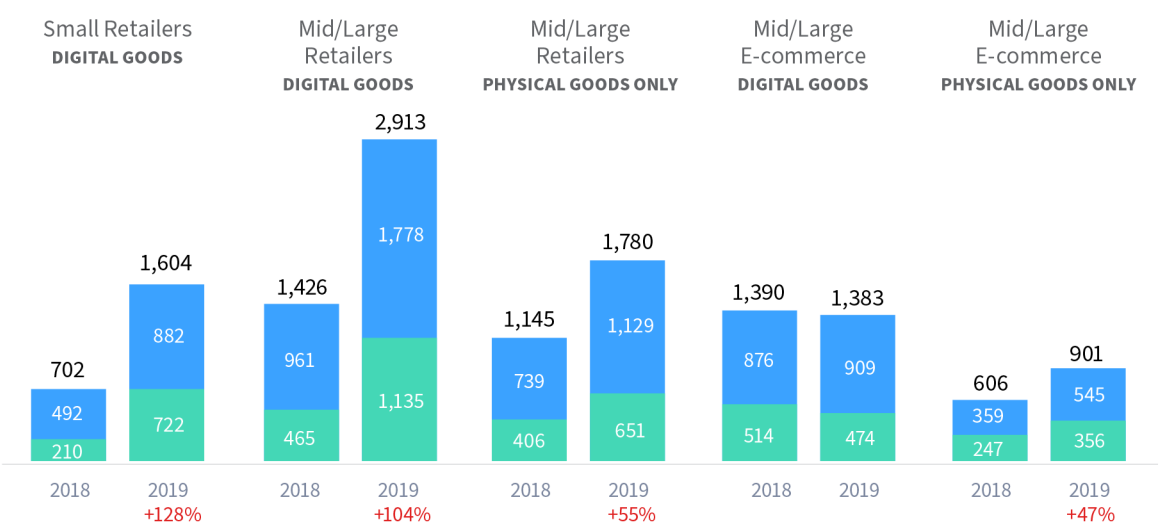
A verificação de identidade é importante; mas igualmente importante é considerar os clientes legítimos, que exigem experiências sem atritos e proteção contra o uso indevido de suas contas e informações pessoais. As atividades envolvendo transações e acessos, como criação de contas, login de usuários e gestão de contas, devem ser intuitivas e seguras, independentemente do contexto em que ocorrem.

Novas ameaças

O combate às fraudes é travado contra um alvo em constante movimento — e esse alvo se mostra cada vez mais rápido e imprevisível a cada ano. Ameaças de fraude que evoluem rapidamente e uma economia cada vez mais digital são fatores que estão levando as organizações a dedicarem mais recursos ao desenvolvimento de estratégias defensivas que se antecipem às ameaças, mas, com muita frequência, elas sequer conseguem acompanhar o ritmo.

De acordo com uma pesquisa da LexisNexis de 2019 chamada “True Cost Of Fraud” (O verdadeiro custo da fraude), as tentativas de transações fraudulentas estão aumentando exponencialmente.

Número médio de tentativas de fraude por mês



Esse aumento vertiginoso está sendo alimentado por uma elevação drástica das violações de dados de alto nível, o que leva a um aumento das tentativas de **Sequestro de Contas** (ATO, de Account Take Over) e ajuda a deteriorar ainda mais a eficácia dos elementos tradicionais de verificação de identidade. Os arquivos de identidade furtados agora estão disponíveis na deep e dark web, deixando as empresas que dependem dessas identidades cada vez mais vulneráveis a sequestros de contas e uso malicioso das informações de seus clientes.

Com uma combinação de informações reais que foram roubadas e informações forjadas, os criminosos conseguem criar contas fraudulentas mais facilmente, usando identidades sintéticas que eles desenvolvem e alimentam durante longos períodos. **Identidades sintéticas** são particularmente difíceis de detectar com os métodos tradicionais, e ainda mais difíceis de prever, uma vez que os crimes em si podem levar anos para se materializar.

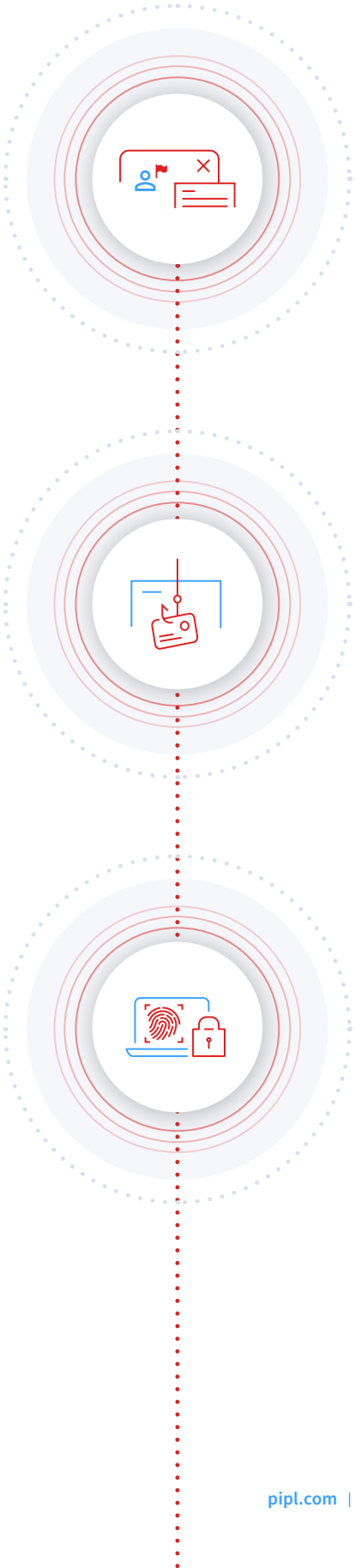
Como resultado, as fraudes de novas contas estão aumentando. Com fácil acesso a dados offline e credenciais de pagamento que atendem aos requisitos de pagamentos **sem cartão físico** (ou CNP, de Card Not Present), tornou-se muito fácil forjar identidades online e criar contas que possam ser usadas em compras fraudulentas, transferências e lavagem de dinheiro.

Também temos observado um aumento dos **ataques de phishing**. Assim como os vazamentos de dados em grande escala, as tentativas de phishing bem-sucedidas estão levando os dados diretamente para as mãos dos criminosos. Enquanto os vazamentos de dados envolvem grandes grupos de pessoas, os ataques de phishing se concentram em pessoas vulneráveis. Isso ocorre especialmente nos casos de "spear phishing" ou "whaling", quando usuários que têm acesso de alto nível a materiais sensíveis ou valiosos se tornam alvos, em uma tentativa de acessar informações ainda mais valiosas e potencialmente prejudiciais.

E há regulamentações — leis confusas, conflitantes e aplicadas aleatoriamente, como GDPR e CCPA — que dificultam ainda mais a coleta e retenção de informações que possam ser usadas para detectar e impedir criminosos reincidentes. A regulamentação das informações de privacidade e identidade continuará evoluindo e se expandindo e, à medida que isso acontece, a sofisticação das práticas de prevenção de fraudes precisará acompanhar o ritmo.

Enquanto este texto está sendo redigido, a COVID-19 ainda se espalha pelo mundo e cobra um alto preço. O caos subsequente foi a oportunidade que os inescrupulosos esperavam para lançar uma onda de ataques contra pessoas desesperadas, usando recursos como phishing de credenciais, anexos e links maliciosos, **comprometimento de e-mail empresarial** (ou BEC, de business email compromise), páginas falsas, downloaders, spam, malware e ransomware. Medos e falsas esperanças são as iscas para atrair possíveis vítimas, levando a uma série de golpes perigosos. Nas últimas semanas, surgiram campanhas maliciosas envolvendo instituições de saúde, empresas farmacêuticas e organizações de ajuda que oferecem curas falsas e canais de auxílio fictícios, tentando enganar pessoas ingênuas que estão em busca de dinheiro e esperança.

Essas ameaças não são totalmente novas, mas aumentam a um ritmo que supera o crescimento das transações online em geral — um indício preocupante de que estamos perdendo a batalha contra a fraude.



Elementos de identidade online e offline: **mais poderosos em conjunto**

Assim como as batalhas não são travadas com uma única estratégia de defesa, as empresas também não devem confiar em um único método de verificação de identidade para detectar e prevenir fraudes. A combinação e corroboração de dados online e offline permite uma defesa muito mais eficaz contra as ameaças modernas do que os métodos tradicionais, que usam uma única fonte.

Verificação de endereço

Os serviços de verificação de endereço (ou AVS, de address verification services) são um bom começo para verificar conexões entre um titular de cartão e o endereço de entrega correspondente, mas o que fazer quando as informações não batem? Não é incomum que os clientes façam compras em nome de algum familiar, empresa ou funcionário com endereço diferente daquele indicado no cartão. Uma simples verificação tradicional de dados offline é capaz de identificar a incongruência, mas não é capaz de revelar possíveis relações entre o titular do cartão e o endereço de entrega incompatível. Para isso, um perfil de identidade online pode revelar conexões com múltiplos endereços de pessoas da família, empresas e funcionários. A pesquisa reversa de um endereço físico usando ferramentas de identidade online também pode revelar insights sobre a pessoa que está associada ao endereço de entrega incompatível. Por exemplo, uma pessoa com o mesmo sobrenome, uma empresa associada ao titular do cartão ou uma pessoa com um histórico confirmado de atividades fraudulentas.

E-mails e telefones celulares

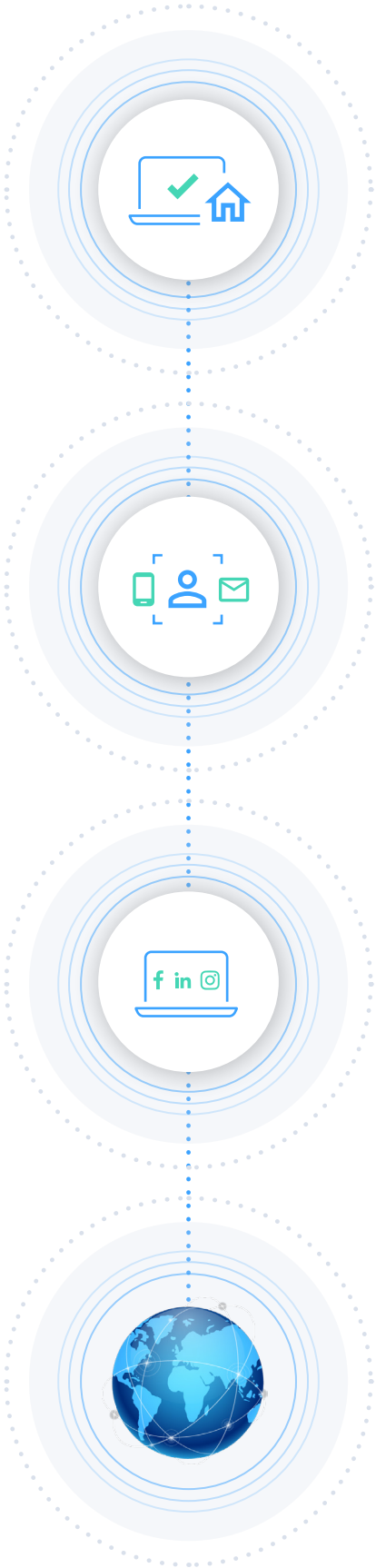
Conexões entre nomes, números de telefone celular e endereços de e-mail também são indicadores confiáveis para descobrir se a atividade é legítima ou fraudulenta. Quando esses elementos de identidade podem ser verificados por meio de uma fonte com referência cruzada ou utilizando várias fontes, a probabilidade de atividades legítimas cresce exponencialmente. O mesmo é válido no sentido inverso: quando os elementos não podem ser verificados por meio de conexões, as atividades são mais suspeitas.

Sites de mídias e redes sociais

Os nomes de usuário em sites de mídias e redes sociais evoluíram no sentido de dificultar qualquer tentativa de ligá-los a pessoas reais. De fato, é comum que os nomes de usuário guardem pouca relação com uma pessoa conhecida, ou podem ser totalmente desprovidos de significado. No entanto, a vinculação de múltiplas fontes de dados entre si pode revelar conexões com outras informações conhecidas, ligando nomes de usuário obscuros a identidades online consistentes, e vice-versa. Isso permite que os investigadores de fraudes estabeleçam conexões com fontes de informação que seriam difíceis e demoradas de obter por outros meios.

Dados globais

Em uma economia global, na qual as transações internacionais são comuns e fundamentais para a existência de muitas empresas, precisamos de uma fonte de dados de identidade com alcance mundial. Muitos fornecedores de dados que usam fontes únicas oferecem informações de identidade apenas de suas respectivas localidades. Empresas que dependem do crescimento em mercados estrangeiros sabem que o risco aumenta exponencialmente conforme as transações cruzam fronteiras, assim como aumentam as oportunidades de conquistar espaço em novos mercados. Essas empresas estão descobrindo que o risco pode ser reduzido substancialmente se puderem estabelecer conexões a identidades online.



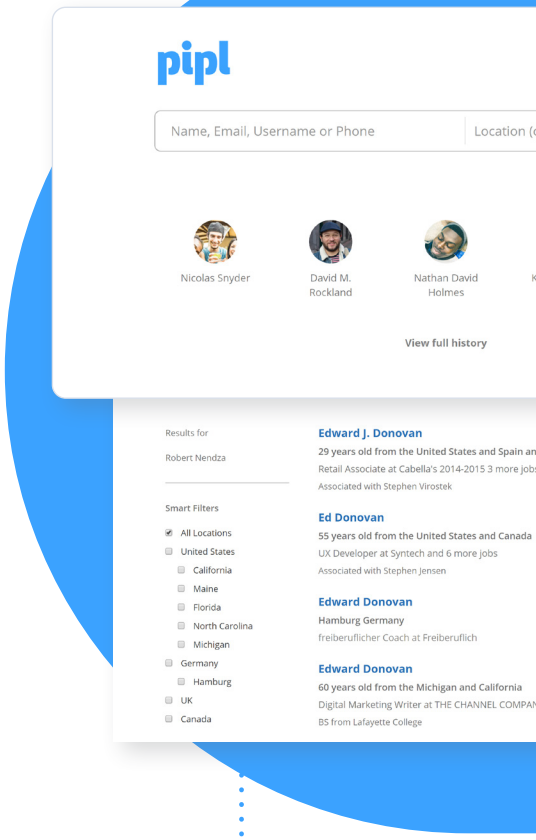
Ao buscarem melhores métodos para controlar fraudes e proteger os clientes, as organizações perceberam que é necessário desenvolver soluções exclusivas para seus negócios e o ambiente onde atuam. Elas descobriram que uma abordagem única para verificação de identidade não garante nenhuma vantagem contra as tentativas de fraude e estornos indevidos. Para criar conjuntos de ferramentas eficazes, muitas organizaçoes estão integrando múltiplos recursos e fontes de dados em seus processos. Algumas estão incorporando suas próprias tecnologias de aprendizado de máquina e inteligência artificial, buscando assim otimizar as decisões de acordo com suas bases de clientes e ofertas de produtos.

Automação

A automação é necessária ao processar grandes volumes de transações. Ela é mais eficaz quando é usada como uma primeira verificação no processo. A conexão automática entre as informações fornecidas pelo cliente e fontes online e offline verificadas aumenta a confiança das decisões e pode separar automaticamente as transações mais arriscadas das menos arriscadas.

Uma solução automatizada pode gerar uma pontuação com base no número de elementos de identidade correspondentes ou conectados. E também pode ajustar automaticamente o peso dessas pontuações à medida que identifica padrões com certos elementos. Por exemplo, pode determinar que os e-mails de clientes vinculados a contas de mídias sociais com um histórico de mais de dois anos dificilmente são fraudulentos, ou que a ausência de contas de mídias sociais conectadas quando há divergências com o endereço de entrega indica uma alta probabilidade de fraude.

Sejam os algoritmos ajustados por seres humanos ou por meio de aprendizado de máquina, a automação oferece às empresas que possuem essa capacidade a vantagem de tomar decisões com base em dados.

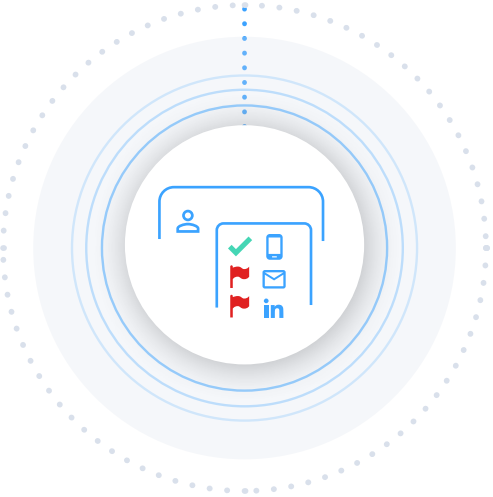


Revisão humana

A revisão humana costuma ser a segunda etapa em um processo de detecção de fraudes. Quando atividades ou dados anômalos são detectados, o sistema normalmente responde de duas formas: ou rejeita a transação, ou a encaminha para outro sistema continuar a revisão. Essa revisão muitas vezes é realizada pessoalmente.

Os analistas de fraude com acesso a informações de identidade online aprovam as transações verificando múltiplos pontos de informação pessoal, incluindo idade, endereços de e-mail, números de celular e nomes de usuário do cliente. A velocidade é de extrema importância nas revisões humanas, tanto para preservar a experiência do cliente quanto para a própria eficiência da operação de revisão.

Não faz muito tempo, os usuários de cartão de crédito precisavam notificar o emissor antes de fazerem uma viagem atípica, ou corriam o risco de ter suas contas suspensas por suspeita de fraude. Esse ponto de atrito agora é quase sempre evitado devido à conexão entre cartões de crédito, endereços de e-mail, números de telefone celular e contas de mídias sociais. Agora, os analistas de fraude possuem ferramentas para determinar rapidamente se cobranças no exterior ou fora da região habitual são decorrentes de viagens ou de informações de identidade roubadas.



Fraudes envolvendo sequestro de contas podem ser detectadas pela presença de mudanças questionáveis nas informações de uma conta existente, que podem estar ligadas a identidades online totalmente diferentes. Ao identificar inconsistências entre os elementos novos e antigos, os analistas são capazes de identificar sequestros de contas com rapidez e precisão.

Ambos

Os sistemas antifraude mais eficazes utilizam uma combinação de ferramentas e métodos. Em geral, convém automatizar o maior número possível de elementos, deixando apenas as decisões mais sutis e de alto valor para a revisão humana. A capacidade de adaptação dos sistemas às mudanças comportamentais, ao ambiente e ao cenário de ameaças em constante evolução também é crucial para o sucesso e a manutenção do sistema.

É difícil dizer se (ou quando) haverá sistemas comerciais que sejam capazes de se configurar e adaptar automaticamente a ambientes específicos. Por enquanto, parece que o sistema de defesa e proteção contra fraudes mais eficaz é uma pilha tecnológica personalizada capaz de conectar dados fornecidos pelos usuários a identidades online, junto com um processo de duas etapas que inclui automação e revisão humana.

Por enquanto, parece que o sistema de defesa e proteção contra fraudes mais eficaz é uma pilha tecnológica personalizada capaz de conectar dados fornecidos pelos usuários a identidades online, junto com um processo de duas etapas que inclui automação e revisão humana.

Benefícios de um sistema de detecção de fraudes integrado e de múltiplos estágios

- Maior confiança na tomada de decisões
- Experiência do cliente sem atritos
- Proteção de contas e dados do cliente
- Maior taxa de aprovação de transações
- Maior taxa de detecção/prevenção de fraudes
- Conformidade regulatória
- Maior alcance de mercado
- Eficiência operacional

Informações de identidade online da Pipl

A Pipl é líder em fornecimento de informações sobre identidades online. Com uma cobertura global inigualável de mais de 3 bilhões de identidades online, cruzadas e coletadas com base em mais de 25 bilhões de registros de identidade individuais, a Pipl possui as informações e ferramentas que os profissionais precisam para identificar fraudes com precisão e proteger clientes legítimos.

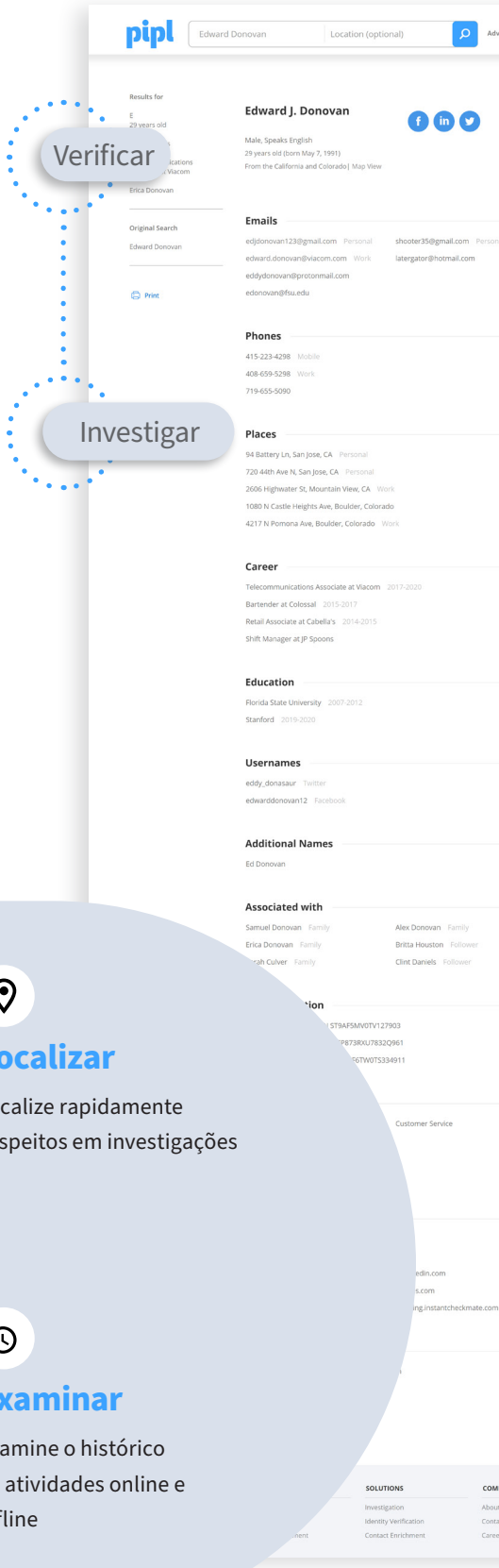
O valor mais importante da solução de identidade online da Pipl é a capacidade de identificar e validar uma pessoa, determinando sua confiabilidade e intenção.

O **Pipl SEARCH** é um aplicativo de pesquisa SaaS intuitivo que oferece informações pessoais, profissionais, sociais, demográficas, de contato e de relacionamento detalhadas na forma de um perfil interativo. A solução é ideal para revisões humanas, investigações, pesquisas e análises.

O Pipl SEARCH permite que os profissionais realizem pesquisas com uma ampla variedade de termos combinados, que geram instantaneamente um robusto perfil de identidade contendo nomes, datas de nascimento, endereços de e-mail, endereços físicos, telefones fixos, números de celular, carros, pessoas e empresas associadas, contas de mídias sociais e nomes de usuários conhecidos. Cada elemento de dado também contém metainformações, incluindo tipos de dados, fontes e primeira/última data de visualização.

Uma varredura rápida de um perfil no Pipl Search pode verificar/confirmar as informações que o cliente insere durante uma transação ou configuração de nova conta, enquanto as informações detalhadas podem acelerar uma investigação, revelando detalhes críticos que ajudam a fortalecer casos e melhorar as taxas de resolução.

Revisão humana usando informações de identidade online:



Verificar

Verifique as informações do cliente

Detectar

Detecte e aprove comportamentos incomuns de clientes legítimos

Investigar

Investigue padrões comuns ao uso de identidades sintéticas, informações roubadas e a probabilidade de fraude e intenção maliciosa

Localizar

Localize rapidamente suspeitos em investigações

Conectar

Conecte a informações pessoais, profissionais e sociais

Descobrir

Descubra associações entre pessoas, endereços, telefones e nomes em mídias sociais

Determinar

Determine a credibilidade de fontes, testemunhas e suspeitos

Examinar

Examine o histórico de atividades online e offline

A **Pipl API** ajuda as empresas a verificarem identidades automaticamente em suas plataformas de decisão. A Pipl API é a ferramenta de avaliação de riscos usada por muitas das grandes empresas que lidam com comércio eletrônico, serviços financeiros e compliance em todo o mundo. Os clientes da Pipl API dispõem de uma abrangente API de dados com bibliotecas fáceis de usar e amostras de código em linguagens populares, facilitando a inclusão de informações de identidade em tempo real nos seus aplicativos.

Com a Pipl API, são mais de 3 bilhões de identidades online a serviço de seus aplicativos. Isso é ideal para verificação de identidades online, detecção de fraudes e apoio de investigações.

Por meio dessas duas abordagens, a Pipl ajuda os usuários a reunirem as informações que já conhecem e validá-las com informações de identidade coletadas e confirmadas a partir de diversas fontes. Para isso, usamos as informações offline tradicionais já mencionadas, como contatos associados, endereços físicos e localizações de parentes, junto com uma análise dos comportamentos online baseados em personas digitais, que são cada vez mais difíceis de falsificar.

Por trás dessa combinação está o **Mecanismo de Resolução de Identidade** de alto desempenho da Pipl, que inclui os seguintes elementos:

Repositório de identidades da Pipl

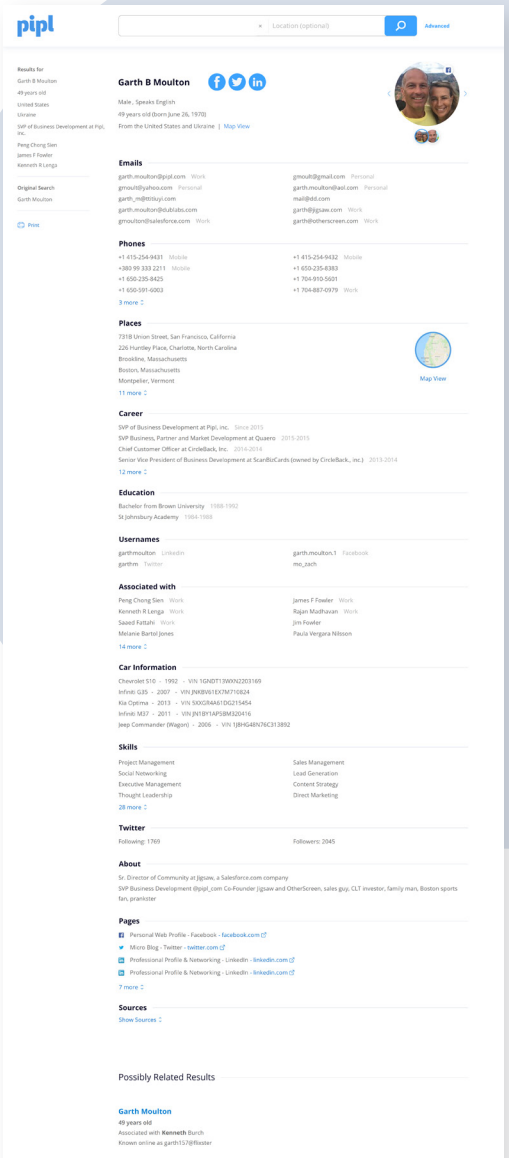
A Pipl utiliza dados obtidos de maneira ética e legal, reunidos em uma coleção de bilhões de dados compilados a partir da Internet e de registros públicos, listagens, diretórios, arquivos e fontes exclusivas.

Algoritmos de identidade da Pipl

Algoritmos de clusterização exclusivos identificam e cruzam dados relacionados entre inúmeras possibilidades para construir perfis de identidade altamente precisos em tempo real.

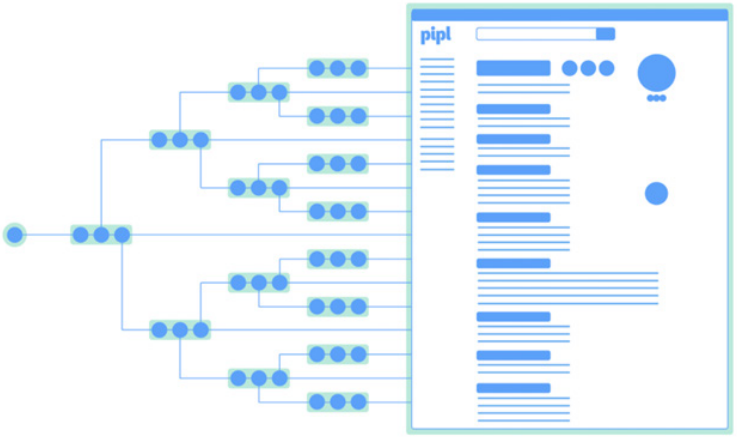
Perfis de identidade da Pipl

Um perfil de identidade da Pipl inclui endereços de e-mail, telefones celulares, telefones fixos, contas de mídias sociais, contas online, nomes de usuário, histórico de endereços, histórico de carreira e formação, automóveis, associações (trabalho, família, seguidores online), fotos, vídeos e muito mais.



Algoritmo de busca recursiva

Existem muitas informações "lá fora". Encontrar informações a partir de uma só fonte na Internet é simples, mas ainda menos confiável do que utilizar uma única fonte de identidade tradicional. O verdadeiro valor de uma identidade online está na coleta e confirmação de dados a partir de diversas fontes. É aí que a Pipl se destaca. Seu algoritmo de busca recursiva segue um processo de pesquisa em múltiplos estágios:



O algoritmo da busca recursiva da Pipl analisa os elementos individuais de cada resultado de busca e executa pesquisas adicionais recursivamente, usando os dados encontrados como uma nova entrada.

O algoritmo processa diversos resultados de pesquisa, da mesma forma que um mecanismo de buscas comum — mas ele não para por aí. Ele analisa os elementos individuais de cada resultado de busca e executa pesquisas adicionais recursivamente, usando os dados encontrados como uma nova entrada de busca. Essa estratégia descobre mais resultados, e o mais importante: corrobora dados entre diversas fontes, aumentando substancialmente a profundidade e a confiabilidade das informações.

Por exemplo, um usuário pode inserir um endereço de e-mail, número de celular ou endereço físico. O mecanismo pode encontrar diversos registros de identidade que correspondem à consulta. Vários desses registros podem incluir um nome. Outros podem conter referências a outras pessoas, empresas ou perfis de mídias sociais. O algoritmo pega cada elemento e executa pesquisas adicionais, buscando correspondências com dados que não foram originalmente pesquisados. Isso dispara dezenas de pesquisas em inúmeras fontes de dados proprietárias e online, e os resultados são compilados em um único perfil de identidade com um alto nível de confirmação.

Esse resultado seria praticamente impossível sem um enorme repositório de identidades e um sofisticado algoritmo de cluster para identificar e organizar as conexões (muitas vezes obscuras) entre várias fontes de informações de identidade.

Confirmação é fundamental

Falsificar ou mentir sobre algumas poucas informações é relativamente fácil. Nenhum sistema ou algoritmo é infalível, mas uma identidade online confirmada em diversas fontes faz com que os criminosos tenham muita dificuldade para forjá-la — ou simplesmente não vale o esforço.

Documentos governamentais e dados offline podem ser úteis, mas a verificação por estes meios pode ser difícil, com maior tendência a gerar atritos com o cliente e aumentar a complexidade tecnológica. Quando não se limitam a métodos de validação tradicionais e exploram elementos digitais para gerar identidades online, as organizações conseguem prosperar com mais confiança e segurança em um mundo conectado.

As informações de identidade online da Pipl permitem que os revisores e investigadores façam buscas com "qualquer dado" (nome, e-mail, telefone, idade, endereço, associações, formação, empregos, etc.) para descobrir "qualquer coisa" ou simplesmente "tudo" sobre uma pessoa.

Preparando-se para o futuro

O risco de fraude vai muito além do simples custo de fazer negócios. Na atual era de reputações distribuídas, as empresas não podem se dar ao luxo de perder nem mesmo alguns poucos clientes. As reputações que levaram anos ou décadas para serem construídas podem desmoronar da noite para o dia. Por outro lado, notícias de vulnerabilidades ou uma reputação frágil podem se espalhar entre os grupos de fraudadores mais rapidamente do que a maioria das empresas consegue reagir.

As organizações devem desenvolver e manter um sistema adaptável para detectar e prevenir fraudes.

Estratégia de defesa em múltiplos estágios

Até mesmo operações de baixo volume exigem processos de detecção de fraude em múltiplos estágios para competir na guerra pela fidelidade do cliente e prevenir fraudes. Sistemas eficazes começam com os freios e contrapesos tradicionais criados para sinalizar atividades anormais e suspeitas. Este é normalmente o domínio dos sistemas de pagamento atuais, que às vezes são incrementados com mecanismos de regras desenvolvidos internamente ou, em sistemas mais avançados, com algoritmos de aprendizado de máquina e inteligência artificial. O próximo estágio envolve a verificação dos dados conhecidos. Quando há um sinal de alerta, você deve fazer o que sabe — geralmente uma combinação de informações que o cliente inseriu e informações que você obteve de um processador de pagamentos — e verificar se realmente apontam para uma pessoa real. É aí que as informações de identidade online podem traçar rapidamente conexões entre as fontes singulares e facilmente falsificáveis e um perfil de cliente com vários elementos de informação, confirmados por várias fontes independentes.

Muitas vezes a verificação é o suficiente para fazer um julgamento confiável — mas nem sempre. Por definição, atividade anômala significa que algo não está em conformidade com os padrões esperados. Os investigadores humanos devem ser capazes de ver e seguir as conexões de dados que seriam difíceis de identificar por algoritmos simples. Conexões com histórico de identidade, familiares, amigos, empresas e sites de mídias sociais muitas vezes levam a uma explicação da anomalia — fornecendo aos tomadores de decisão uma base muito mais sólida para fazer julgamentos precisos.

O estágio final é fazer um julgamento com base no que já se sabe e no que foi descoberto. Esse estágio pode ser automatizado até certo ponto, mas frequentemente requer intervenção humana. A chave para essa etapa é a presença de informações conectadas e confiáveis. Decisões automatizadas são muito mais precisas quando os dados são abundantes e confiáveis. O mesmo vale para as decisões humanas, mas ainda mais importante é o conhecimento do contexto mais amplo envolvendo a pessoa e a transação.

Etapas em um processo de detecção de fraudes em vários estágios:

Detecção › **Verificação** › **Investigação** › **Julgamento**

Mercados globais

As organizações podem ter seus próprios motivos para adotar, temer ou ignorar os mercados globais, mas as transações internacionais são inevitáveis em praticamente qualquer oferta online. Os provedores de dados de identidade tradicionais nem sempre mantêm ou têm acesso a dados de consumidores de diversos países e regiões. As informações tradicionais do consumidor baseiam-se em dados bancários que são deficientes nas áreas onde a maioria da população tem pouco ou nenhum acesso a serviços financeiros. Isso ocorre com mais frequência em mercados com clientes mais jovens, onde os indivíduos têm menos histórico de crédito e, consequentemente, menos informações de identidade tradicionais.

À medida que as economias se tornam mais globalizadas e mais arriscadas, a solução pode estar, mais uma vez, nas informações de identidade online. As identidades online podem reduzir muito o risco quando as entradas são combinadas a um perfil contendo informações corroboradas por várias fontes. Muitas organizações recorrem à Pipl por sua cobertura global incomparável, que inclui números de telefone celular, conexões de mídias sociais, endereços de e-mail e endereços residenciais.

Conformidade regulatória

Os órgãos governamentais e organizações do setor reagiram ao aumento das fraudes online e à crescente preocupação com a privacidade e segurança das informações de identidade pessoal (IIP) com uma lista cada vez maior de regulamentações. Já mencionamos o GDPR e a CCPA, mas as normas de combate à lavagem de dinheiro (AML, de anti-money laundering), Know Your Customer (KYC) e adequação de conteúdo à faixa etária também pressionam as lojas e instituições financeiras a adotarem práticas de verificação e investigação de identidades que atendam aos requisitos.

Assim como o custo da fraude, o custo do incumprimento regulatório vai muito além do óbvio. Violações e batalhas judiciais dificilmente passam despercebidas pelo público, podendo agravar ainda mais a situação quando ocasionam danos reputacionais, custos legais e possíveis multas.

É importante considerar como você tratará da responsabilidade pela conformidade regulatória. Alguns aspectos da conformidade recairão exclusivamente sobre sua empresa, enquanto outros podem ser compartilhados com provedores de dados terceirizados. Você deve trabalhar com parceiros que sejam sérios e transparentes em relação a suas práticas e fontes de coleta de dados.

No momento certo

A grande mudança para uma economia digital já não é novidade, mas eventos recentes mostraram que dados de identidade online são fundamentais para aprimorar as formas tradicionais de verificação de identidade. A pandemia de COVID-19 e uma agitação política e social generalizada só fizeram com que o combate às fraudes e a proteção das informações de identidade pessoal se tornassem mais urgentes.

As organizações devem encarar de frente o problema das fraudes, para o bem de seus clientes e negócios. Os métodos tradicionais já não são mais suficientes, e as informações de identidade online podem suprir essa lacuna.

A Pipl está trabalhando para se antecipar às necessidades das organizações que lidam com transações online. Seu enorme repositório de identidades é incomparável, pois sua cobertura global e algoritmos proprietários conectam dados de identidade tradicionais a identidades online robustas, resultando em recursos de verificação e investigação que acompanham a evolução da economia digital.

As organizações devem encarar de frente o problema das fraudes, para o bem de seus clientes e negócios. Os métodos tradicionais já não são mais suficientes, e as informações de identidade online podem suprir essa lacuna.

SOBRE A PIPL

A Pipl é líder mundial em fornecimento de informações sobre identidades online. Com uma cobertura global imbatível de mais de 3 bilhões de identidades online, compiladas e referenciadas a partir de mais de 25 bilhões de registros de identidade, a Pipl é a plataforma escolhida por profissionais do mundo inteiro.