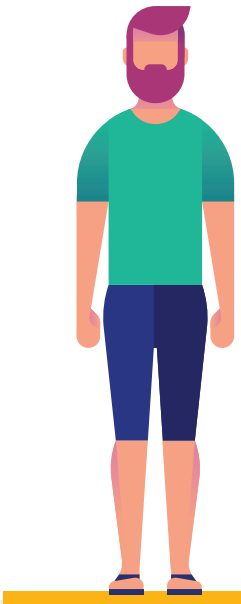
Transformando a segurança no pagamento por meio da inteligência artificial

VISA

Sumário



Resumo executivo

Em um setor tão dinâmico quanto o de pagamentos, o poder e o alcance da inteligência artificial (IA) são amplos. A IA alavanca a base de segurança necessária para oferecer uma experiência de pagamento simples e segura aos consumidores. Este artigo oferece uma visão geral de como a IA está preparada para transformar o panorama da segurança no setor de pagamentos e como a Visa utiliza IA para desenvolver recursos que permitam aos seus parceiros aprimorar a tomada de decisões, melhorar a gestão de risco e superar a difícil escolha entre garantir segurança aos pagamentos e proporcionar a experiência ideal.

Conheça o Pedro

Siga a rotina do Pedro para ver como suas experiências cotidianas são afetadas e moldadas por IA.

Inteligência artificial: introdução

Nas últimas décadas, a inovação tecnológica se concentrou em maior automação e conectividade, resultando em significativos benefícios sociais e econômicos. A próxima transformação tecnológica, impulsionada pela inteligência artificial (IA), promete ganhos inéditos ao permitir que os consumidores realizem uma ampla variedade de atividades cotidianas com maior facilidade e eficiência.

O possível impacto de IA sobre os serviços financeiros e os pagamentos não será menos acentuado. Com IA, os pagamentos podem ir além da transação e ficar cada vez mais automatizados, interativos e personalizados, integrados com as experiências cotidianas e em todos os canais e dispositivos. Porém, esta evolução nos pagamentos só pode ser alcançada com estruturas de segurança que evoluem e se desenvolvem da mesma forma que as ameaças à segurança progridem.

Inteligência artificial: Definição e casos de uso

IA é a teoria e o desenvolvimento de sistemas computadorizados para executar tarefas que normalmente exigem inteligência humana. IA permite que as máquinas aprendam com a experiência, se ajustem a novos inputs e executem tarefas. A IA se manifesta em três principais aplicações de negócios: **machine learning, processamento de linguagem natural** e **reconhecimento de imagens.**

Machine Learning

Machine learning permite que as máquinas aprendam iterativamente com os dados para executar uma tarefa específica, sem serem explicitamente programadas para fazer isso. Aprendizagem profunda é uma classe particular de machine learning baseada em redes neurais artificiais, uma abordagem computacional inspirada no uso de conexões sinápticas do cérebro humano para resolver problemas.

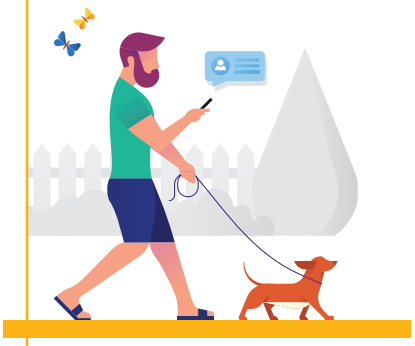
Machine learning oferece aos emissores uma nova maneira de avaliarem, aprovarem e gerenciarem solicitações de crédito. Com machine learning, os emissores podem aproveitar dados não tradicionais, como o histórico de pagamento de contas de serviços públicos e de telecomunicações para aprovar crédito para pessoas que não tenham um histórico de crédito tradicional. Este caso de uso pode afetar 1,7 bilhão de pessoas que não dispõem de serviços bancários, ao oferecer a elas acesso a redes formais de crédito.[1]

Em casa, Pedro entra em uma loja online para comprar um livro e vê outras opções em uma seção chamada "clientes que compraram este item também compraram" e adiciona um livro sugerido ao seu carrinho. Depois, Pedro acessa seu serviço de streaming e a página inicial exibe uma seção "recomendados para você", que reflete suas preferências de programas.

Processamento de linguagem natural

O processamento de linguagem natural (Natural language processing, PNL) permite que uma máquina reconheça as palavras faladas, convertendo-as em texto e inserindo este texto em um mecanismo de busca que então devolve resultados para o comando inicial. Assistentes digitais virtuais são a aplicação mais comum deste caso de uso.
De fato, espera-se que o número de assistentes digitais virtuais cresça para mais de 1 bilhão de usuários até 2025. Além das populares assistentes digitais, como a Alexa da Amazon, emissores de todo o mundo estão oferecendo chatbots para os seus clientes, para digitalizar a experiência de atendimento ao cliente e criar um diferencial para clientes já acostumados com o mundo digital. O SEB Group, um banco da Suécia, lançou um chatbot chamado Aida, que ajuda os clientes do banco com várias questões relacionadas a cartões e perguntas sobre a conta. Além de melhorar a experiência dos consumidores, espera-se que os chatbots economizem mais de US$ 8 bilhões por ano para as empresas até 2022.[2]

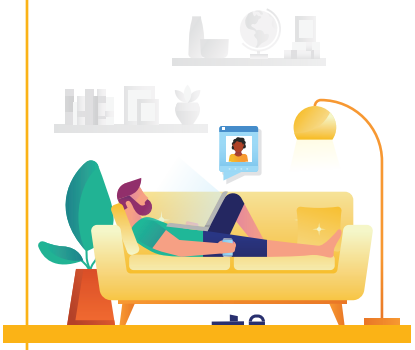
As aplicações do processamento de linguagem natural vão muito além de chatbots. Por exemplo, o processamento de linguagem natural pode também ser usado para extrair informações de formulários, ajudando no complicado processo de cadastro, em que 25% dos consumidores desistem da sua solicitação em razão de problemas resultantes de atritos com Conheça seu Cliente (Know-Your-Customer, KYC) e reduzindo o tempo de cadastro. Além disso, o processamento de linguagem natural pode classificar automaticamente os documentos, facilitando aos profissionais financeiros verificar se têm todos os detalhes necessários para manter conformidade com as normas KYC.



Pedro observa uma transação no extrato de seu cartão de débito que ele não reconhece. Com facilidade, Pedro conversa com o chatbot pelo app de seu emissor. E, em 30 minutos, o problema de Pedro estava resolvido. Pedro foi incentivado a entrar em contato com o serviço de atendimento ao cliente porque seu emissor lhe ofereceu uma opção acessível, segura e rápida.

Reconhecimento de imagem

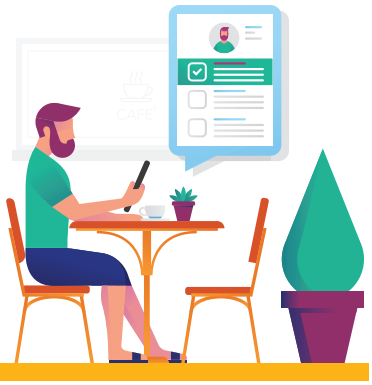
O reconhecimento de imagem usa IA para identificar lugares, pessoas, logos, objetos e edifícios. Amazon Go, uma experiência de varejista automatizada, é um exemplo desta tecnologia. Nas lojas Amazon Go, os consumidores retiram suas compras da loja sem esperar para pagar no caixa, porque a loja emprega o reconhecimento de imagens para detectar quando os produtos são retirados ou devolvidos às prateleiras, e acompanha os produtos no carrinho virtual do cliente. Do ponto de vista de serviços financeiros, os emissores estão cada vez mais aproveitando o reconhecimento facial para permitir acesso móvel, reduzindo significativamente o tempo que seus usuários levam para acessar suas contas e completar suas atividades bancárias.



Pedro entra em sua conta de mídia social e carrega um álbum de fotos. Quando Pedro marca seus amigos nas fotos, o serviço de mídia social lhe recomenda algumas pessoas. Hoje, a visão do computador pode reconhecer pessoas com 98% de precisão, com o mesmo nível de desempenho humano, criando um processo de marcação rápida e precisa para usuários como Pedro.[3]

Instalação de inteligência artificial da Visa para segurança no pagamento

As soluções orientadas para IA da Visa buscam criar um ecossistema de pagamentos mais seguro e protegido. Como afirma Scott Boding vice-presidente da Visa e especialista em IA, "estamos tentando usar IA como um meio para cercar e automatizar o trabalho pesado de detecção de fraude – uma tarefa que consome muito tempo e que muitos clientes fazem manualmente hoje. Estamos tentando usar IA para gerar eficiências para nossos clientes". [4]



Oferecendo uma experiência segura e simples

Cadastro de contas

Conforme os ataques cibernéticos ampliam seu escopo, os criminosos exploram elementos dos dados de consumidores para cometer fraude de identidade sintética combinando informações verdadeiras e falsas para criar uma nova identidade que é usada para abrir novas contas e fazer compras e empréstimos fraudulentos. Em um estudo da Forrester Consulting, encomendado pela Visa, 39% das empresas consultadas globalmente sofreram fraudes com novas contas (por exemplo, usando informações de identificação roubadas para abrir uma conta fraudulenta) nos últimos dois anos, e 32% das empresas consultadas globalmente sofreram fraudes de identidade sintética no mesmo período.

Buscando resolver os problemas associados ao processo de cadastro de clientes, a Visa Advanced Identity Solution (VAIS), que utiliza machine learning para analisar padrões de migração de fraudes entre emissores e o uso irregular de elementos de identidade durante o processo. VAIS gera uma pontuação de risco que os emissores podem usar para fundamentar sua decisão sobre o solicitante. O sistema aproveita os dados do serviço de câmara de compensação dos emissores, que reúne solicitações de todos os emissores que foram aprovadas ou recusadas de um consumidor em particular, a velocidade das solicitações do consumidor e outros elementos relevantes. Depois, incorpora estes dados e usa reconhecimento de padrões e inteligência de máquina para criar perfis dinâmicos do consumidor baseados em personas, permitindo que a verificação da solicitação seja realizada em tempo real e em escala.

Pedro gostaria de solicitar um cartão de crédito de um novo emissor, First Digital. É sua primeira interação com o emissor e permite à First Digital a oportunidade de entregar um processo fácil de solicitação e cadastro para conquistar a conta de Pedro. Ao executar dados tradicionais e não tradicionais por meio do seu modelo de aprendizagem de máquina, a First Digital pode desenvolver uma visão sob medida do histórico de crédito de Pedro e aprovar sua solicitação de modo eficiente.

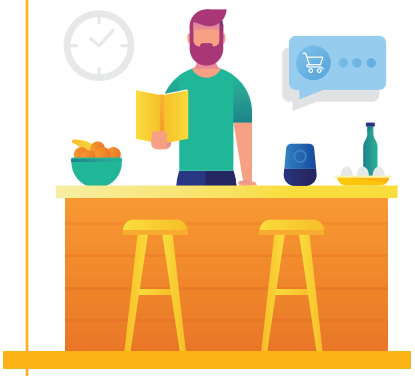
Quando Pedro solicitou um cartão de crédito, o processo foi rápido e relativamente sem barreiras, graças a utilização de IA pela First Digital para agilizar o importante processo de segurança conhecido como Conheça seu cliente (Know-Your-Customer, KYC), para verificar sua identidade e avaliar os potenciais riscos associados à sua solicitação.

Autenticação

À medida que as interações do consumidor migram para canais digitais, autenticar consumidores digitalmente usando formas tradicionais se mostra desafiador – especialmente quando as expectativas dos consumidores por experiências sem fricção são cada vez maiores. Em um estudo da Forrester Consulting, solicitado pela Visa, 34% dos participantes globais afirmaram que a complicada autenticação do usuário final é um grande desafio que enfrentam ao gerenciar a segurança no pagamento. As empresas precisam simplificar o processo de autenticação para os seus consumidores, além de investir nas ferramentas certas que lhes permita avaliar com precisão se o usuário é quem ele diz ser. Isso é especialmente importante levando em conta a crescente complexidade da fraude: no mesmo estudo da Forrester, 32% das empresas globais sofreram fraude por roubo do controle de contas nos dois anos anteriores.

No esforço de efetuar autenticação simples, porém segura, as empresas estão implementando diversos métodos de autenticação, por exemplo, biometria. Visa Biometrics é uma solução que oferece autenticação multifatorial e fora da banda, permitindo que os consumidores sejam autenticados de modo seguro e uniforme por meio de rosto, impressão digital e voz, reduzindo assim a fricção associada a senhas e PINs. Além disto, esta solução de biometria usa machine learning para validar a correspondência biométrica e identificar "ataques falsos", adicionando uma camada extra de segurança para o cliente.

Elementos adicionais de dados, como biometria, podem ser usados para avaliar a identidade do usuário com maior precisão, sem incluir uma fricção desnecessária ao processo. O Visa Consumer Authentication Service (VCAS) – Serviço de autenticação do consumidor Visa – aproveita os dados, como perfis de conta e geolocalização, para apoiar a estratégia de autenticação do emissor e pontuar todas as solicitações de autenticação. O VCAS usa a autenticação baseada em risco, que permite aos emissores avaliar de forma rápida e dinâmica, o risco de uma transação, aplicar regras baseadas em modelagem de dados e determinar se têm um alto nível de confiança para autenticar seu portador do cartão passivamente no segundo plano, ou se precisam engajar o portador do cartão de forma ativa. Do outro lado da transação, os estabelecimentos comerciais podem usar o Cardinal Consumer Authentication para se engajar em um sistema sofisticado de monitoramento e detecção das anomalias potencializado por IA. O grande volume de dados trocado entre estabelecimentos comerciais e emissores otimiza as decisões de risco ao longo do tempo, resultando em menor fricção para o consumidor. A Visa está usando IA para criar soluções de autenticação seguras, que habilitam nossos parceiros a navegar com sucesso no panorama de pagamentos em constante evolução.



Pedro vai à cozinha preparar seu jantar, e se dá conta de que esqueceu de comprar ingredientes importantes e usa seu assistente de voz para fazer um pedido. Com o tempo, o assistente de voz aprendeu a voz de Pedro, reconhece a voz como sendo a de Pedro e pode autenticar sua identidade usando sua biometria de voz.

Autorização

Um grande obstáculo que as empresas enfrentam é a geração de falsos positivos, ao tentar identificar transações fraudulentas, significando que frequentemente elas não conseguem separar transações legítimas das ilícitas. Isso é especialmente relevante nos canais digitais, onde a gestão de risco é tão importante para habilitar boas vendas quanto para evitar fraude. Em 2018, US$ 278 bilhões em transações com cartão não presente foram recusadas em todo o mundo, representando um crescimento de 27% em relação ao ano anterior.[5] IA pode analisar grandes quantidades de dados de transações, ajudando a identificar atividades criminosas sofisticadas com maior precisão e, finalmente, permitir às empresas minimizar seus falsos positivos e aprovar mais transações legítimas.

Usando o poder de IA, a Visa criou ferramentas sofisticadas para garantir que o consumidor esteja protegido contra fraudes, os estabelecimentos comerciais possam enviar seus pedidos com confiança e os emissores possam aprovar transações legítimas, recusando as ilegítimas. Os emissores podem aproveitar a Visa Advanced Authorization (VAA), que avalia as autorizações VisaNet em tempo real, ajudando os emissores a identificar e responder prontamente a padrões e tendências emergentes de fraude. Usando sofisticadas tecnologias de detecção de risco, a VAA avalia 100% das autorizações de cartões Visa que passam por sua rede. Ao processar as transações, a VAA atribui uma pontuação de risco e, com a VAA, os emissores podem impedir possíveis perdas com fraudes antes que a transação seja concluída. Atualmente, a VAA é usada por mais de 8.000 emissores em 129 países e, apenas em 2018, estima-se que impediu US$ 25 bilhões em fraudes.[6]

A VAA é complementada pelo Visa Strategy Manager, um serviço que aplica algoritmos aos dados históricos de um cliente para identificar correlações entre áreas de fraudes, que poderiam não ser detectadas de outro modo. Estes algoritmos são posteriormente inseridos no Visa Risk Manager, que é a solução para a tomada inteligente de decisões potencializada pela VisaNet, permitindo que os emissores recusem apenas as transações de maior risco e otimizando as taxas de aprovação no ponto de venda.

Para habilitar e qualificar os estabelecimentos comerciais neste espaço, a Visa oferece o CyberSource Decision Manager (CyberSource DM). O CyberSource DM tem mais de 260 detectores de anomalias e 15 modelos de risco específicos da região, do canal e da indústria, cada um deles otimizado para identificar fraude em cenários diversos. Enquanto isso, machine learning está enraizada em seus recursos de combate à fraude, como parte da abordagem patenteada, chamada modelagem por fusão em tempo real. A modelagem por fusão em tempo real aproveita a comprovada eficácia dos modelos estáticos convencionais, com os recursos mais ágeis de análises de dados dos atuais e mais avançados modelos de autoaprendizagem, para ajudar as empresas a gerenciar e a detectar fraudes com mais eficiência e eficácia.

Com estes produtos, os emissores e estabelecimentos comerciais podem confiar que uma camada extra de proteção será adicionada quando os portadores de cartão e consumidores estiverem realizando uma transação.

Considerando a facilidade com que Pedro pode fazer seu pedido, ele ficaria frustrado se o emissor recusasse a transação. Por outro lado, se seu emissor autorizasse uma transação fraudulenta, Pedro teria que entrar em contato com o emissor e iniciar um litígio contra a cobrança, o que é uma experiência frustrante. Por sorte, o emissor de Pedro usa sofisticados algoritmos para pontuar o risco da transação e, quando identifica o nível de risco como relativamente baixo, aprova o pagamento.

Protegendo o ecossistema por meio de serviços de segurança cibernética

Nosso mundo hiperconectado está criando novos meios de explorar as informações e os dados dos consumidores. Em 2018, estima-se que os crimes cibernéticos totalizaram US$ 600 bilhões[7] e o custo médio de uma violação de dados foi de aproximadamente US$ 1,2 milhão.[8] Apenas em 2018, 2,7 bilhões de registros foram expostos em todo o mundo.[9] Considerando a magnitude deste problema, a segurança cibernética é a principal preocupação de consumidores e empresas.

IA pode ser usada para resolver este grande problema. Como os ataques continuam evoluindo, é fundamental que as empresas também adaptem e desenvolvam uma abordagem fluida e dinâmica para detectar e interromper esses ataques. A Visa reconhece a importância de desenvolver sua estratégia, e criou soluções que protegem os consumidores e as empresas para além da transação. Por exemplo, o Visa Account Attack Intelligence, uma solução orientada por IA, aplica aprendizagem profunda ao vasto número de transações processadas pela VisaNet, para identificar emissores e estabelecimentos comerciais, além de BINs em uso por criminosos cibernéticos para adivinhar PANs, datas de validade e códigos CVV2 por meio de testagem de contas. A tecnologia de machine learning detecta padrões sofisticados de enumeração, elimina falsos positivos e alerta as instituições financeiras e os estabelecimentos comerciais afetados antes que as transações fraudulentas aconteçam. A Visa está comprometida em proteger a integridade do ecossistema de pagamentos e as informações dos consumidores, e esta solução permite à Visa alcançar esta meta com sucesso.

A Visa está inovando e aproveitando IA para proteger as transações em todo o ciclo de vida

A Visa reconhece a importância de desenvolver sua estratégia, e criou soluções que servem para proteger os consumidores e as empresas que vão além da transação.

Fraudadores inovadores e inteligência artificial

Os fraudadores estão sempre inovando em suas metodologias e vetores de ataque, e provavelmente usarão IA para avançar além das simples técnicas de hacking. Com a IA, os fraudadores podem dinamizar táticas de engenharia social e otimizar a evasão da segurança cibernética. Além do mais, com avanços na tecnologia de IA, os fraudadores podem, com facilidade (e menor custo) conduzir ataques paralelos e distribuídos. Eles precisam apenas de acesso a servidores prontamente disponíveis e habilidades básicas de codificação.

No caso de engenharia social, os fraudadores criam o que parece ser vídeos, arquivos de áudio e e-mails legítimos, para enganar as pessoas e induzi-las a cometer ações comprometedoras. Como resultado, o consumidor pode clicar em um link ilegítimo, permitindo que o fraudador capture suas informações pessoais ou tenha acesso a um sistema particular de TI corporativa, em uma escala maior do que ocorre atualmente; este é um problema crescente, e uma em cada três empresas no mundo foi afetada pela engenharia social.[10]

Os fraudadores também podem aproveitar a IA e combiná-la com técnicas existentes de malware para criar uma nova e desafiadora espécie de malware. Assim que o alvo é identificado, seja por reconhecimento facial, geolocalização ou reconhecimento de voz, a ação maliciosa é iniciada; porém, antes do ataque, o malware passará desapercebido.

Para combater estes desafios potenciais, é fundamental continuar a compartilhar inteligência entre o ecossistema e colaborar em estratégias que ofereçam soluções para a indústria.

Para combater estes possíveis desafios, é fundamental que o ecossistema continue compartilhando informações e colaborando com estratégias que proporcionem soluções para todo o setor.

Um olhar para o futuro

O impacto da inteligência artificial sobre a vida dos consumidores é transformador. Atualmente, a IA é inteiramente diferente da sua criação, há 50 anos, e ficará ainda mais diferente daqui a 50 anos. Independentemente destas mudanças, a necessidade de segurança e confiança entre consumidores, estabelecimentos comerciais e instituições financeiras permanecerá a mesma. Enquanto a maioria das pesquisas e aplicações da IA se concentram no reconhecimento de padrões e de sons, há menos trabalhos em torno de dados transacionais (ou seja, séries históricas) relativos à aprendizagem profunda. A Visa combina um significativo estoque de dados de pagamento com conhecimentos técnicos inigualáveis para liderar pesquisas importantes da indústria em aprendizagem profunda para aplicações que lidam com dados transacionais. Isso resultou em diversas patentes para soluções que não só aproveitam a aprendizagem profunda em grande escala, mas também fazem isso em menos de milissegundos. A Visa continuará a desenvolver e instalar poderosos aplicativos com IA para reforçar sua base de segurança e assumir a liderança em aprendizagem profunda para pagamentos.

Visa continuará a desenvolver e lançar aplicações poderosas de IA para reforçar sua base de segurança e estabelecer liderança em aprendizagem profunda para pagamentos.

Sobre os autores

Michael Jabbara é diretor sênior na organização de Risco Global da Visa e lidera iniciativas estratégicas em sua função. Você pode entrar em contato com ele pelo e-mail yjabbara@visa.com.

Sofia Katsaggelos é analista de desenvolvimento de negócios na estrutura de estabelecimentos comerciais e adquirentes da Visa. Você pode entrar em contato com ela pelo e-mail sokatsag@visa.com

Agradecimentos

Os autores gostariam de agradecer a muitos de seus colegas, cujas ideias e conhecimentos estão aqui refletidos, particularmente Carolina Barcenas, Melyssa Barrett, David Capezza, Ann Ewing, David Henstock, Aruna Joshi, Andrew Naumann, Penny Lane, Tara Lavelle, Shane Malloy, John Zhan e Anna Wintle.

Termos de referência

Estudos de caso, comparações, estatísticas, pesquisas e recomendações são fornecidos "COMO ESTÃO" e apenas para fins informativos, e não devem ser usados para orientações operacionais, de marketing, jurídicas, técnicas, fiscais, financeiras ou de outra natureza. A Visa Inc. não oferece nenhuma garantia ou representação em relação à completude ou precisão das informações contidas neste documento, tampouco assume qualquer responsabilidade que possa decorrer da confiança em tais informações. As informações aqui contidas não devem ser usadas como aconselhamento jurídico ou de investimentos, e os leitores são incentivados a buscar aconselhamento de um profissional competente, quando necessário.

Estes materiais e recomendações sobre melhores práticas são fornecidos apenas para fins informativos e não devem ser utilizados para aconselhamento sobre marketing, jurídico, regulatório ou de qualquer outra natureza. Os materiais de marketing recomendados devem ser avaliados de forma independente, levando em conta as suas necessidades de negócios específicas e todas as leis e normas aplicáveis. A Visa não é responsável pela forma de uso dos materiais de marketing, recomendações sobre melhores práticas ou outras informações, incluindo erros de qualquer tipo, contidos neste documento, que é apenas para fins ilustrativos. Este documento contém ilustrações de um produto que está atualmente em processo de lançamento, e devem ser compreendidas como representação dos potenciais recursos do produto lançado. A versão final deste produto pode não conter todos os recursos descritos nesta apresentação.

1. Forbes, 1.7 Billion Adults Worldwide Do Not Have Access To A Bank Account, junho de 2018
2. Financial Brand, Meet 11 of the Most Interesting Chatbots in Banking, março de 2018
3. Fortune, Facebook's new algorithm can recognize you even if your face is hidden, junho de 2015
4. PYMNTS.com, Visa CyberSource: AI's Role Is To Predict — Not to Know, maio de 2019
5. Exclui fundos insuficientes e declínios por emissores inoperantes. Compras em e-commerce para o ano calendário de 2018. Crescimento anual baseado no ano calendário de 2018 em comparação com 2017. Vendas baseadas em dados de autorização VisaNet. Fraude baseada no TC40 informado pelo emissor (incluindo transações que não foram processadas no VisaNet).
6. PYMNTS.com, 'Visa Advanced Authorization Blocks $25 Billion In Fraud', junho de 2019
7. BusinessWire, New Global Cybersecurity Report Reveals Cybercrime Takes Almost $600 Billion Toll on Global Economy, fevereiro de 2018
8. Kaspersky Lab, What is the Cost of a Data Breach, maio de 2018
9. BloomBlog, 2018: The Year of the Data Breach, dezembro de 2018
10. T-Systems, Social Engineering, 2019