CELENT

OPERACIONALIZANDO A PREVENÇÃO DE FRAUDES NO IBM Z16

Como reduzir perdas em transações bancárias, com cartões e pagamentos

Neil Katkov

5 de abril de 2022

Este relatório foi encomendado à Celent pela IBM, que solicitou a criação e execução do estudo, em seu nome. As análises e conclusões foram elaboradas pela Celent, e a IBM não teve controle editorial sobre o conteúdo.

ÍNDICE

SUMÁRIO EXECUTIVO

Os avanços na inteligência artificial (IA), como o deep learning, estão viabilizando melhorias significativas na detecção de fraudes. No entanto, grandes bancos e processadores de pagamentos muitas vezes só usam modelos de IA em uma fração das transações devido a limitações na taxa de transferência e na latência nos sistemas de detecção de fraudes. O resultado disso é que muitas transações fraudulentas não são monitoradas nem detectadas.

O IBM Integrated Accelerator para IA, que faz parte do novo processador de mainframe Telum da IBM, foi criado para executar inferências em cargas de trabalho em tempo real, em escala e com baixa latência. O chip foi desenvolvido para possibilitar a detecção de fraudes em tempo real, mesmo em um ambiente de processamento de grande volume de transações bancárias, cartões e pagamentos.

Para ajudar bancos e processadores de pagamentos a entender os possíveis benefícios dessa inovação nas operações de fraudes, a Celent criou estimativas da potencial redução de perdas com fraudes, se essas entidades aplicarem inferência de IA em 100% das transações.

Benefícios quantificáveis da detecção de fraudes com IA, nos mainframes IBM z16:

Redução de perdas com fraudes no setor em		Redução das perdas por banco em		Redução da rejeição de transações com cartão em
Nos EUA	Globalmente	Banco de nível 1, EUA	Banco de nível 2, EUA	46%
5,6 cents por US$ 100	2,0 cents por US$ 100	US$ 105 milhões	US$ 18 milhões	

A Celent estima que a aplicação de modelos de inferência avançados a, teoricamente, todas as transações bancárias, com cartão e de pagamentos nos mainframes dos sistemas IBM Z16 pode reduzir as perdas com fraudes em cerca de US$ 161 bilhões em todo o mundo. Nesse caso, as transações bancárias potencialmente evitariam US$ 140 bilhões em perdas enquanto cartões e pagamentos evitariam perdas de US$ 21 bilhões. Só nos EUA, as perdas com fraudes bancárias poderiam ser reduzidas em cerca de US$ 44 bilhões e em até US$ 6 bilhões, no caso de cartões e pagamentos.

Precisamente, existem barreiras à adoção da inferência de IA no mainframe para operações de fraude, como problemas no modelo de governança, custos das substituições, disponibilidade dos recursos internos de ciência de dados e a demonstração do caso de negócios.

Ainda assim, a execução de modelos avançados de IA diretamente no ambiente do mainframe é uma grande inovação num setor em que aproximadamente 70% do valor das transações globais é processado em mainframes da IBM. A detecção de fraudes é um caso de uso importante desse novo recurso da IBM, com benefícios visíveis, tanto no lucro quanto na experiência dos clientes.

O ALTO CUSTO DAS FRAUDES EM TRANSAÇÕES BANCÁRIAS, COM CARTÕES E EM PAGAMENTOS

As fraudes geraram uma perda global de cerca de US$ 385 bilhões nos setores bancário, de cartões e de pagamentos em 2021.

Nos setores corporativo e de varejo, as fraudes bancárias e em pagamentos podem ter várias formas. As fraudes em bancos incluem controle de contas, fraudes de pagamentos por push autorizados (APP), fraude de boletos falsos e vários esquemas de phishing e engenharia social criados para acionar transferências de dinheiro legítimas ou obter credenciais de contas. Cartões e pagamentos também são vulneráveis a fraude de controle de conta e phishing, além de esquemas específicos que incluem ID sintético, fraude de forja de limite alto e ataques man-in-the-middle.

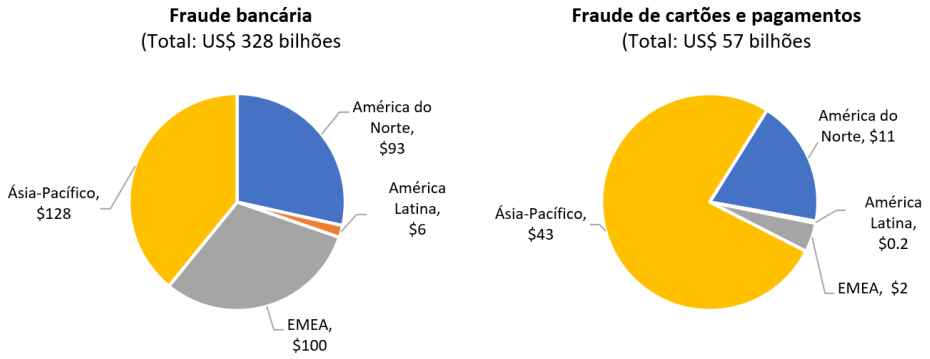
Figura 1: Esquemas comuns de fraude em transações bancárias e com cartão

Fraude bancária	Fraude de cartão
Controle de conta	Fraude de aplicativo
Pagamentos por push autorizados (APP, authorized push payments)	Fraude de desbloqueio (bust-out)
Fraude de cheque	Man-in-the-middle
Fraude de boleto	Phishing
Engenharia social	ID sintético

Fonte: Celent

Essas e outras fraudes em contas bancárias, cartões e pagamentos são uma grande preocupação para as instituições financeiras. A Celent estima perdas anuais com fraudes de cerca de US$ 209 milhões para bancos de nível 1 nos EUA (com total de ativos que supera US$ 100 bilhões) e de US$ 35 milhões para bancos de nível 2 (com total de ativos entre US$ 50 e US$ 100 bilhões). Se consideramos o setor como um todo, os bancos tiveram perdas com fraudes de US$ 328 bilhões, globalmente, em 2021. Os setores de cartões e pagamentos tiveram uma perda adicional de US$ 57 bilhões. No total, as fraudes geraram perda global de cerca de US$ 385 bilhões nos setores bancário, de cartões e de pagamentos em 2021.

Figura 2: Perdas com fraudes bancárias, de cartões e pagamentos em 2021



Fonte: As estimativas da Celent são baseadas em dados sobre transações do BIS e em dados sobre fraudes do Banco Central dos EUA.
Observação: As fraudes bancárias incluem transferências, débitos diretos e em cheques. Fraudes em cartões e pagamentos incluem cartões de crédito e débito, pagamentos eletrônicos e outros pagamentos.

Embora os bancos e processadores de pagamentos travem há décadas uma batalha contra fraudes com sistemas de detecção e cartões com chip, as perdas continuam aumentando porque os criminosos estão sempre desenvolvendo novas tecnologias e novos esquemas, com base em engenharia social.

A pandemia da COVID-19 aumentou o número de fraudes. No caso dos bancos, muitas dessas fraudes são relacionadas a esquemas de phishing e engenharia social, que exploram as ansiedades e necessidades médicas geradas pela pandemia. No caso das transações com cartão, a pandemia gerou um aumento nas operações de digital banking e e-commerce, pois as pessoas evitaram transações em lojas físicas. Como as transações com cartão não presente (CNP) são a maior parte das fraudes de cartão (cerca de 65%), as perdas com esse tipo de fraude aumentaram.

Solução para o problema: modelos de fraude com base em deep learning

Com os avanços na inteligência artificial, como o deep learning, agora os bancos têm ferramentas para evitar fraudes com muito mais eficiência. Isso é feito com a análise de dados em escala para encontrar padrões que indiquem fraudes, inclusive tipologias novas e nunca vistas.

O deep learning é um tipo de modelo de aprendizado de máquina com base em uma rede neural profunda (DNN, deep neural network). Esse tipo de rede é composto por nós computacionais, ou neurônios, que usam pesos progressivos para reforçar conexões entre os nós. Os nós são organizados em várias camadas, criando uma rede “profunda” (daí, o "deep") que aumenta a capacidade e a taxa de aprendizado do modelo. Os modelos de deep learning são treinados com base em dados existentes, como o histórico de transações, no caso dos modelos de fraude. O modelo treinado é executado nos dados atuais, como transações em tempo real, para gerar um resultado, também chamado de inferência. Nos modelos de fraude, a inferência é geralmente uma pontuação que indica a probabilidade de a transação ser fraudulenta.

Com base em conversas e pesquisas no setor, a Celent estima que a inferência de IA com modelos de deep learning pode gerar um aumento de 60% na precisão da detecção de fraudes em comparação com os modelos de fraude atuais.

No entanto, o potencial de inferência para melhorar as taxas de fraude é muito limitado. Isso acontece porque, em ambiente de mainframe com muito volume, esses modelos costumam ser executados apenas em uma fração das transações (menos de 10%) devido a fatores como latência, custo e atritos com clientes. Isso significa que cerca de 90% das fraudes possivelmente evitáveis ainda não são detectadas. Isso limita muito a capacidade de os bancos aproveitarem os avanços da IA para recuperar perdas com fraudes.

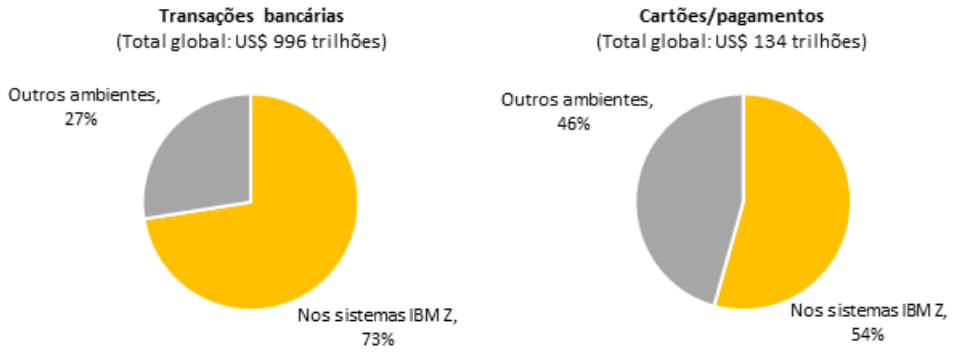
A latência e o custo para passar 100% das transações bancárias e com cartão por modelos avançados não são mais problema. O novo processador IBM z16 Telum contém um acelerador de IA que, pela primeira vez nos sistemas IBM Z16, executa modelos de IA direto no chip, em tempo real. Isso aumenta exponencialmente a taxa de transferência e os tempos de resposta, possibilitando, pela primeira vez, passar virtualmente todas as transações por modelos de detecção de fraudes com base em deep learning.

LIMITAÇÕES DA DETECÇÃO DE FRAUDES PADRÃO

A tecnologia típica de detecção de fraudes e as abordagens operacionais dos ambientes de mainframe incluem simulação de fraudes em sistemas fora da plataforma em transações selecionadas e/ou após a transação. Isso limita muito a possibilidade de bancos e processadores de pagamentos executarem modelos de IA avançados em todas as transações.

Muitos bancos e processadores de pagamentos de grande porte executam seus sistemas principais em ambientes de computação com mainframe. A IBM estima que 45 dos 50 maiores bancos do mundo usam mainframes do sistema IBM Z16. A maioria dos principais processadores de cartões e pagamentos também usa a plataforma. Em todo o mundo, a Celent estima que 70% do valor das transações bancárias, de cartões e de pagamentos passa por ambientes do sistema IBM Z16.

Figura 3: Valor de transações de bancos, cartões e pagamentos em sistemas IBM Z16



Fonte: Celent

A latência entre os sistemas principais e os sistemas de detecção fora da plataforma pode ser tolerada em algumas transações. No entanto, no caso das rotinas de inferência de IA com uso intensivo de dados, aplicadas a transações em tempo real, tais como pagamentos, transações com cartão e transações de digital banking, a latência impede a realização de todas as transações em uma plataforma de detecção com IA, em ambientes de grande volume. Quando as principais transações do sistema são movidas do mainframe para um sistema de detecção fora da plataforma para análise em tempo real, os tempos de resposta para receber os resultados variam de 50 a 80 milissegundos enquanto as transações esperam a conclusão desse processo. Isso aumenta o tempo de aprovação das transações, que pode criar atritos com os clientes, principalmente nas transações com cartão.

Mais especificamente, a latência alta pode inviabilizar a realização de todas as transações em um sistema de detecção fora da plataforma. A latência entre o sistema principal e o software de identificação pode atrasar o recebimento dos resultados no sistema principal a ponto de

fazer as transações em tempo real expirarem. Por isso, alguns bancos só executam modelos de deep learning para fraudes depois das transações.

Isso também faz os bancos processarem apenas uma fração das transações (menos de 10%) usando seus mecanismos de detecção de fraudes em tempo real. Essa abordagem tem consequências sérias. Agora, os modelos de deep learning estão possibilitando melhorias significativas de cerca de 60% nas taxas de detecção. No entanto, os bancos não estão aproveitando todos os benefícios porque processam apenas uma amostra das transações usando esses modelos. Isso significa que uma maior proporção das fraudes não é detectada, aumentando as perdas. Como as fraudes se tornaram o foco das estratégias de conformidade para evitar crimes financeiros, os bancos também correm mais risco de violar regulamentações se não conseguirem processar todas as transações usando a detecção antifraude.

Problemas de legados em um banco de nível 1, EUA

Um banco de nível 1 dos EUA, que executa seu sistema principal em uma plataforma dos sistemas IBM Z16, implementou um sistema de detecção de fraudes com base em IA fora da plataforma. Devido a problemas relacionados ao custo e à latência, o banco só processa transações de alto risco pelo sistema de IA. A maioria das transações são processadas com uma pontuação baseada em regras, aprovadas como uma conveniência para o cliente e enviada para análise depois da conclusão. Os benefícios da IA são muito limitados pela impossibilidade de usar os modelos em todas as transações, ou seja, a IA não é aproveitada em todo o seu potencial.

REDUÇÃO DE PERDAS CAUSADAS POR FRAUDES COM INFERÊNCIA DE IA NO MAINFRAME

A IBM desenvolveu um processador para seu computador mainframe IBM z16 com acelerador de IA que faz a inferência avançada no chip, em escala. A Celent estima que o novo processador IBM z16 pode identificar fraudes usando deep learning em praticamente todas as transações, reduzindo potenciais perdas causadas por fraudes em transações bancárias, com cartões e em pagamentos, em até US$ 161 bilhões, mundialmente.

Os algoritmos de deep learning tendem a usar mais recursos de computação do que os modelos de fraude legados. Com a implantação da inferência de IA com base em deep learning para fraudes, os bancos estão enfrentando dificuldades para gerenciar essas cargas de trabalho de missão crítica. Quando a identificação é feita em sistemas fora da plataforma, os tempos de resposta podem chegar a 80 milissegundos, com taxas de transferência médias de 1.000 a 1.500 transações por segundo (tps).

Devido a essas limitações de latência e taxa de transferência, as transações expiraram enquanto os bancos aguardavam os resultados da identificação. Esses e outros problemas fizeram os bancos enviarem apenas uma fração das transações (menos de 10%) para seus mecanismos de detecção.

Deep learning no mainframe

Baseados em um modelo que usa deep learning para identificar fraudes em cartões de crédito, 32 chips IBM Telum em um único servidor podem fazer até 3,5 milhões de inferências por segundo com um tempo de resposta médio de 1,2 milissegundo.

Fonte: IBM microbenchmark, agosto de 2021

AVISO LEGAL: O resultado do desempenho é baseado em testes internos da IBM.

A IBM desenvolveu um acelerador para seu computador mainframe IBM z16 que executa modelos de inferência de IA diretamente no chip. De acordo com a IBM, a taxa de transferência e as melhorias desses modelos de IA no mainframe são suficientes para analisar fraudes em tempo real em praticamente todas as transações. Isso é válido mesmo para ambientes que processam um grande volume de transações bancárias, com cartão e de pagamento.

Além disso, os modelos podem ser executados virtualmente sem impacto no tempo de processamento das transações. A IBM afirma que o IBM Integrated Accelerator for AI, que faz parte do novo processador Telum, pode executar modelos de IA no mainframe com um tempo de resposta muito rápido de 1,2 milissegundo para cada solicitação de inferência. No caso específico da detecção de fraudes em cartões, os primeiros benchmarks indicaram que uma configuração com 32 chips Telum possibilita até 3,5 inferências por segundo.

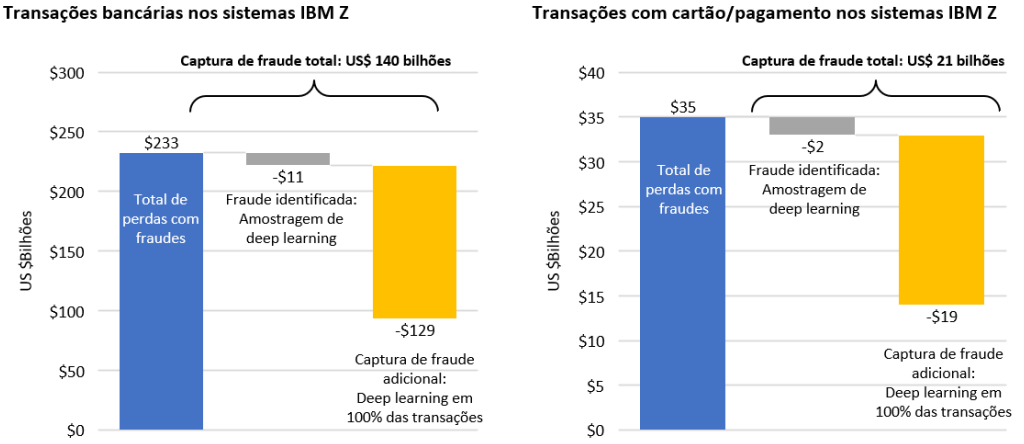
Essa escala é suficiente até para picos nos fluxos de transação, permitindo que bancos e processadores de pagamentos executem praticamente todas as transações usando modelos de deep learning.

Os bancos e processadores de cartão e pagamentos podem aproveitar todo o potencial da tecnologia moderna de inferência executando modelos avançados em todas as transações. A Celent estima que a aplicação de modelos avançados de inferência a todas as transações possa reduzir as perdas com fraudes em 2 centavos de dólar para cada US$ 100 de transações no mundo todo.

Nos EUA, onde a taxa de fraudes é maior do que a média mundial (9,3 centavos de dólar para cada US$ 100 em comparação com 3,7 centavos no resto do mundo), as perdas devido a fraudes foram reduzidas em 5,6 centavos para cada US$ 100. Para os bancos, isso equivale a uma economia de US$ 1,33 em um valor médio de transação de US$ 2.375.

A Celent estima que, teoricamente, processar todas as transações nos sistemas IBM Z16 usando modelos de deep learning pode reduzir as perdas causadas por fraudes em US$ 161 bilhões no mundo todo. Os bancos podem evitar US$ 140 bilhões em perdas causadas por fraudes, e os processadores de cartões e pagamentos podem evitar perdas de US$ 21 bilhões. Só nos EUA, o potencial de redução de perdas causadas por fraudes é de US$ 44 bilhões para bancos e US$ 6 bilhões para processadores de cartões e pagamentos.

Figura 4: Potencial de redução de perdas causadas por fraudes usando modelos de deep learning



Fonte: Celent

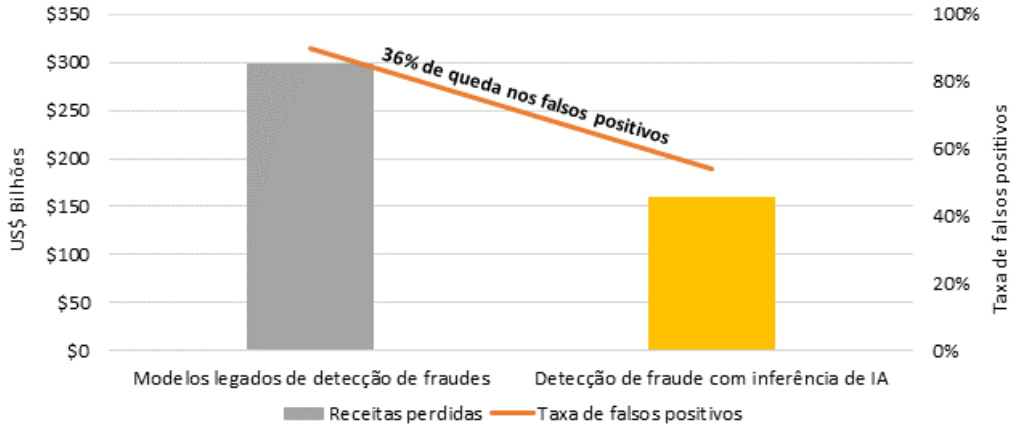
A Celent estima que um banco de nível 1 que usa o IBM z16 e processa todas as transações com modelos avançados de inferência, em comparação com a prática recomendada de aplicar modelos de IA a apenas cerca de 10% das transações, pode ter uma redução adicional das perdas causadas por fraudes de US$ 105 milhões. Um banco de nível 2 pode evitar perdas de US$ 18 milhões. Processar todas as transações com modelos avançados também melhora esses modelos. Um número maior de transações gera mais dados para treinar os modelos, aumentando a precisão da detecção de fraudes.

CONTROLE DE FALSOS POSITIVOS PARA REDUZIR A PERDA DE CLIENTES

Os modelos legados de detecção de fraudes têm taxas muito altas de falsos positivos (geralmente mais de 90% de todas as transações alertadas), o que faz os bancos rejeitarem transações legítimas. O aumento dos falsos positivos e as transações negadas criam problemas para os clientes e aumentam as perdas financeiras, porque os clientes acabam usando outro cartão de crédito ou débito para fazer a compra. A Celent estima que a diminuição das transações com cartão de crédito pode causar uma perda de receita com tarifas de US$ 298 bilhões no mundo todo.

A necessidade de equilibrar os esforços antifraude e minimizar os problemas para os clientes é outro motivo para os bancos limitarem as rotinas de detecção de fraudes a uma amostra das transações. Os falsos positivos ocorrem quando transações legítimas são sinalizadas incorretamente como fraudulentas pelo software de identificação. A maior precisão dos modelos de deep learning pode melhorar consideravelmente as altas taxas de falsos positivos do setor. Isso pode reduzir o número de transações rejeitadas erroneamente além de melhorar a experiência do cliente e reduzir as quedas na receita devido à perda de clientes. Os bancos também podem processar todas as transações identificando fraudes com menos danos, causadas por problemas com clientes.

Figura 5: Modelos de deep learning melhoram as taxas de falsos positivos



Fonte: Celent

Os modelos de deep learning aplicados a cada transação com cartão podem melhorar as taxas de falso positivos em cerca de 55%. Embora essa taxa ainda seja alta, ela pode gerar uma redução na perda de receita gerada por tarifas de cartão de crédito de US$ 137 a US$ 161 bilhões no mundo todo.

Menos falsos positivos também geram outros benefícios. Os analistas de fraudes precisam verificar menos alertas, o que reduz os custos de investigação pós-transação. Também há benefícios na reputação, porque a redução dos problemas e das frustrações dos clientes melhora a boa vontade e a confiança.

Os modelos avançados também podem gerar melhorias na detecção de comportamentos suspeitos que possam indicar lavagem de dinheiro. O Bank Secrecy Act dos EUA, as diretivas contra lavagem de dinheiro da União Europeia e outras regulamentações colocam os programas de combate à lavagem de dinheiro (AML, money laundering programs) dos bancos sob intenso escrutínio dos órgãos. Nos EUA, os órgãos reguladores sempre denunciam programas de AML inadequados com multas que passam de US$ 1 bilhão. As operações de AML também são afetadas por taxas muito altas de falsos positivos, geralmente mais de 95%, que geram uma grande sobrecarga operacional para os bancos. Além disso, o monitoramento de AML geralmente é feito depois das transações, o que aumenta o risco para os bancos. O uso de modelos com base em IA nas operações de AML pode ajudar a resolver esses problemas porque melhora a precisão da detecção do comportamento de AML e reduz os falsos positivos.

A SOLUÇÃO

Nossa análise aponta benefícios significativos e quantificáveis com o uso de modelos de deep learning em até 100% das transações. A IBM afirma que o novo acelerador da empresa pode fazer isso nas transações processadas nos mainframes IBM z16, mesmo em ambientes de grande volume. No entanto, os bancos e os processadores ainda precisam considerar vários outros fatores antes de dar esse salto.

A Celent recomenda que os bancos e os processadores de pagamentos que estão ponderando os benefícios da detecção de fraudes com base em deep learning considerem estes pontos:

- **Governança do modelo.** Os órgãos reguladores e os auditores internos exigem políticas sólidas de governança nos modelos de fraude. Isso significa que os modelos de IA precisam ser transparentes e explicáveis. Embora os fornecedores de plataformas de IA estejam evitando abordagens do tipo “caixa preta”, a governança dos modelos de IA continua sendo um tema complexo.
- **Resistência regulatória.** Os regulamentadores ficam confortáveis com a detecção baseada em regras tradicionais, mas não têm tanta familiaridade com as técnicas avançadas de deep learning. Em alguns casos, os bancos, os cientistas de dados e os fornecedores deles podem precisar mostrar aos órgãos reguladores a eficácia e a confiabilidade da IA avançada.
- **Custo de substituição.** Muitas instituições já têm sistemas de detecção de fraudes baseados em IA. Essas empresas vão precisar justificar a mudança da detecção para o mainframe, o que inclui a decisão de manter os sistemas atuais, por exemplo, para oferecer suporte à análise pós-transação ou a linhas de negócios menores, ou descartá-los inteiramente.
- **Recursos de ciência de dados.** O Integrated Accelerator for AI da IBM é otimizado para executar modelos, inclusive os desenvolvidos em frameworks de código aberto, como o Pytorch e o TensorFlow. No entanto, a compatibilidade desse produto com software de detecção de fraude em pacote ainda não foi testada. Acreditamos que, futuramente, fornecedores de produtos de combate a fraudes vão desenvolver pacotes que possam ser executados no acelerador. De qualquer forma, as instituições que estão migrando a detecção baseada em IA para o IBM z16 vão precisar de recursos de ciência de dados para desenvolver e oferecer suporte a modelos avançados de deep learning contra fraudes, internamente ou por meio de provedores de modelos especializados.

As instituições financeiras precisam avaliar esses fatores com cuidado e fazer as verificações necessárias no novo acelerador de IA da IBM. Mesmo assim, os possíveis benefícios em termos de redução de perdas causadas por fraudes e diminuição das transações, além da redução dos problemas para os clientes e da melhoria da experiência, são interessantes. As empresas que usam os sistemas IBM Z16 devem avaliar cuidadosamente os benefícios da mudança da detecção de fraudes para o mainframe.

COMO APROVEITAR A EXPERTISE DA CELENT

Se você achou este relatório útil, entre em contato com a Celent para fazer análises e pesquisas personalizadas. Nossa experiência coletiva e o conhecimento gerado ao elaborar este relatório podem ajudar você a facilitar a criação, a adaptação ou a execução das suas estratégias.

Suporte para instituições financeiras

Estes são exemplos típicos de projetos aos quais damos suporte:

Triagem e seleção de fornecedores. Identificamos descobertas específicas para você e sua empresa para entender melhor suas necessidades únicas. Em seguida, criamos e enviamos solicitações de informações personalizadas para fornecedores específicos para ajudar você a fazer escolher rápidas e precisas.

Avaliações de práticas empresariais. Avaliamos criteriosamente seus processos e requisitos empresariais. Com base em nosso conhecimento do mercado, identificamos possíveis limitações em processos ou tecnologias e compartilhamos insights claros que ajudarão você a implementar as melhores práticas do setor.

Criação de estratégias de negócio e de TI. Reunimos as perspectivas da sua equipe de executivos, das equipes de atendimento e de TI e dos seus clientes. Em seguida, analisamos sua situação atual, os recursos institucionais e a tecnologia com base nas suas metas. Se necessário, ajudamos você a reformular seus planos de tecnologia e negócios para atender a necessidades de curto e longo prazo.

Suporte a fornecedores

Oferecemos serviços que ajudam você a filtrar as ofertas de produtos e serviços. Estes são alguns exemplos:

Avaliação da estratégia de produtos e serviços. Ajudamos você a avaliar sua posição no mercado em termos de funcionalidade, tecnologia e serviços. Nossos workshops de estratégia ajudarão você a mirar nos clientes certos e mapear suas ofertas com base nas necessidades deles.

Análise da mensagem e dos materiais de marketing. Com base na nossa vasta experiência com seus clientes em potencial, avaliamos os seus materiais de marketing e vendas, inclusive o site e outros materiais.

PESQUISAS RELACIONADAS DA CELENT

Remaking Risk: A Taxonomy of Regtech
Outubro de 2021

Technology Trends Previsory: Risk, 2022 Edition
Outubro de 2021

IT and Operational Spending in AML-KYC: 2021 Edition
Dezembro de 2021

IT and Operational Spending on Fraud: 2021 Edition
Fevereiro de 2021

Innovation In Risk: A Snapshot Through the Lens of Model Risk Manager 2021
Abril de 2021

Fino Payments Bank: Remote Implementation of Enterprise-Wide Fraud Management During the Pandemic
Março de 2021

Swedbank: Modernizing Card Fraud Management and Improving Customer Experience
Março de 2021

AVISO DE COPYRIGHT

Para mais informações, entre em contato com info@celent.com ou:

Neil Katkov nkatkov@celent.com

Américas

EUA
99 High Street, 32nd Floor
Boston, MA 02110-2320

+1-617-424-3200

EUA
1166 Avenue of the Americas
Nova York, NY 10036

+1-212-345-8000

EUA
Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

+1-415-743-7800

Brasil
Rua Arquiteto Olavo Redig
de Campos, 105
Edifício EZ Tower – Torre B – 26º andar
04711-904 – São Paulo

+55 11 3878 2000

EMEA

Suíça
Tessinerplatz 5
Zurique 8027

+41-44-5533-333

França
1 Rue Euler
Paris 75008

+33 1 45 02 30 00

Itália
Galleria San Babila 4B
Milão 20122

+39-02-305-771

Reino Unido
55 Baker Street
Londres W1U 8EW

+44-20-7333-8333

Ásia-Pacífico

Japão
Midtown Tower 16F
9-7-1, Akasaka
Minato-ku, Tóquio 107-6216

+81-3-6871-7008

Hong Kong
Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

+852 2301 7500

Singapura
138 Market Street
#07-01 CapitaGreen
Singapura 048946

+65-6510-9700