

SHIFT

SHIFT TECHNOLOGY INSURANCE PERSPECTIVES

EDIÇÃO DE TENDÊNCIAS DE FRAUDE DIGITAL

Do editor

A Inteligência Artificial (IA) e, mais especificamente, a IA Generativa (GenAI), chamaram a atenção de empresas e consumidores. Para as seguradoras, essas tecnologias estão apoiando e melhorando processos como sinistros e subscrição, entre muitos outros, que são essenciais para o sucesso contínuo dos negócios. A inteligência artificial está gerando ganhos de eficiência e ajudando as seguradoras a preencher a lacuna de talentos criada pela disparidade entre o número de funcionários que deixam o setor e os que entram nele. Essas soluções poderosas estão ajudando as seguradoras a ver o panorama geral, a tomar as melhores decisões possíveis e a reduzir pontos dos índices combinados.

Ao mesmo tempo, as mesmas ferramentas que estão proporcionando enormes benefícios ao setor de seguros também estão criando um conjunto totalmente novo de riscos. Os fraudadores estão usando a IA e a GenAI para inventar novos esquemas de fraude. Eles estão usando essas tecnologias para tornar os esquemas existentes mais difíceis de detectar. E ferramentas fáceis de usar e disponíveis publicamente estão permitindo que os fraudadores criem

fotos, documentos e outras “evidências” convincentes necessárias para estabelecer apólices ilegítimas e sinistros falsificados. A era da “falsificação profunda de seguros” está chegando.

Nesta edição do Shift Insurance Perspectives, exploraremos algumas das maneiras pelas quais a IA e a GenAI estão sendo usadas para impulsionar os avanços na fraude digital voltada para o setor de seguros. Como o desejo de criar mais oportunidades para o autoatendimento do cliente e menos intervenção humana por parte das seguradoras abriu a porta para mais fraudes? Qual é a aparência dos novos esquemas digitais e como eles estão explorando as lacunas existentes nas estratégias antifraude? Onde a IA e a GenAI estão sendo usadas por agentes mal-intencionados? E, talvez o mais importante, como a IA e a GenAI podem ser usadas pelas seguradoras na luta contra as fraudes de subscrição e sinistros?

Como sempre, este relatório só é possível graças aos talentos combinados de muitos funcionários da Shift em toda a organização. Obrigado por suas contínuas contribuições para o relatório Perspectivas de Seguros da Shift.

Redes de fraude de apólices

Os consumidores comemoraram quando o setor de seguros começou a adotar os avanços digitais aos quais estavam acostumados por meio do comércio on-line e móvel. Infelizmente, o mesmo aconteceu com corretores mal-intencionados que tentavam tirar proveito do sistema. A capacidade de solicitar cobertura on-line, sem a necessidade de intervenção humana, significava que os possíveis segurados agora podiam comprar seguros da mesma forma que compravam quase tudo em suas vidas. Usar um portal ou aplicativo on-line era rápido, conveniente e eficiente. O mesmo acontecia com o processo de sinistros e a mudança para iniciativas “sem contato, com pouco contato” e de processamento direto (STP). Para as seguradoras, a adoção de abordagens digitais significou que seus experientes corretores, subscritores e profissionais de sinistros puderam dedicar tempo às solicitações e aos sinistros mais complicados, nos quais sua experiência era necessária.

Para aqueles que procuram fraudar o setor, a remoção do elemento humano da subscrição e dos sinistros criou efetivamente novas oportunidades para fraudes em grande escala.

Para aqueles que procuram fraudar o setor, a remoção do elemento humano da subscrição e dos sinistros criou efetivamente novas oportunidades para fraudes em grande escala. Muitos desses

esquemas se baseiam no uso de identidades roubadas e documentos fraudulentos para obter apólices ilegítimas. Vamos examinar um exemplo recente de uma rede de fraude de apólices identificada pela Shift, que incluía 146 novas apólices geradas ao longo de seis meses. Essas apólices cobriam veículos de maior valor e todos os motoristas correspondentes apresentavam um registro limpo. A realidade, entretanto, era bem diferente. A seguradora nessa situação enfrentou posteriormente uma série de reclamações de terceiros contra essas apólices. Embora nenhuma tenha sido significativa o suficiente para levantar uma bandeira vermelha individualmente, a rede de fraudes de apólices gerou custos para a seguradora que chegaram a centenas de milhares de dólares. É por isso que a IA é tão importante no combate a esse tipo de fraude digital.

Nessa situação, a resolução de entidades com tecnologia de IA é o primeiro passo para identificar uma rede de fraude de apólices antes que danos significativos sejam causados. A análise dos dados de apólices e sinistros identifica semelhanças nas informações fornecidas que podem não ser facilmente percebidas quando se analisam aplicações ou sinistros individuais. Quando essas conexões são identificadas, fica mais fácil para as seguradoras tomarem medidas contra a rede. As soluções podem incluir a investigação automática de sinistros associados à rede, o encaminhamento de apólices para não renovação e a análise cuidadosa de solicitações suspeitas de fazerem parte de uma rede.

Detectando falsificação de avisos e declarações

As seguradoras lidam com avisos e declarações fraudulentas desde o início dos tempos do seguro. Na tentativa de obter prêmios melhores, os solicitantes podem ser tentados a fornecer informações sobre si mesmos, seus veículos ou suas propriedades que apresentem sua solicitação da melhor forma possível. No caso de pessoas físicas, isso pode significar a subnotificação do número de quilômetros dirigidos por ano ou indicar um endereço mais desejável para a garagem permanente do veículo. Ou pode significar negligenciar a notificação de que um veículo ou parte da residência está sendo usado para fins comerciais ou de negócios. Essas inconsistências aparentemente pequenas têm o potencial muito real de levar a um vazamento significativo do prêmio e a custos futuros de sinistros.

Mas o que acontece quando as declarações falsas ocorrem em grande escala? O vazamento de prêmios e os custos de sinistros associados podem aumentar exponencialmente. A Shift já viu exemplos de como empresas desonestas podem usar declarações falsas para criar problemas reais para as seguradoras. Em um caso específico, um único endereço em um bairro desejável foi associado a mais de 10 veículos diferentes, todos identificados como sendo de uso exclusivamente pessoal. Essa fachada ocultava o fato de que nenhum dos veículos estava realmente estacionado no endereço fornecido na solicitação. Mais importante ainda, todos os veículos estavam sendo usados para fins comerciais. Se isso não tivesse sido



descoberto, a seguradora poderia perder dezenas de milhares de reais em custos de sinistros mais altos no caso de um incidente.

Com as declarações falsas e as redes de declarações falsas, encontramos outro esquema de fraude possibilitado pela mudança das seguradoras para mais interações digitais, mas também altamente suscetível de ser descoberto por meio da adoção de soluções de detecção de riscos e fraudes baseadas em IA. A resolução de entidades e a detecção de redes são capazes de analisar aplicativos e políticas existentes em busca de informações compartilhadas, como números de telefone e endereços de e-mail. A inclusão de dados de terceiros na análise, como registros comerciais e outros registros públicos, bem como mídias sociais disponíveis publicamente, pode ajudar a determinar a verdadeira natureza de quem está por trás da apólice (por exemplo, se é uma entidade comercial ou um indivíduo).

Corretagem fantasma assistida digitalmente ghost broking

A corretagem fantasma pode ser praticada tanto por corretores credenciados que vendem apólices e embolsam os prêmios sem realmente segurar os segurados quanto por “corretores” não credenciados que vendem apólices fraudulentas aos clientes. Estamos examinando esse último caso neste relatório. Esse tipo de

No próprio trabalho da Shift relacionado o às redes de Ghost Broking que operam no Reino Unido, as seguradoras descobriram redes com até 400 apólices afetadas.

esquema tem como alvo específico os indivíduos que buscam seguros baratos ou cujos prêmios podem ser afetados negativamente devido ao histórico de sinistros, localização, idade ou outros fatores. A capacidade dos fraudadores de manipular digitalmente a documentação de suporte a uma solicitação ou apólice levou a um aumento desse tipo de fraude.

Um exemplo recente relatado na Itália destaca os métodos pelos quais os corretores fraudulentos lucram. Criminosos agindo como corretores de seguros usaram identidades roubadas e identidades de indivíduos falecidos para adquirir apólices baratas por meio

de declarações falsas. Essas apólices eram então vendidas a consumidores desavisados. A documentação forjada da venda do veículo fazia parecer que o veículo da apólice de seguro era do novo segurado. O corretor fraudulento embolsa a diferença nos prêmios. Na eventualidade de um incidente, o corretor desaparece, deixando a seguradora com a responsabilidade de resolver o sinistro.

Estima-se que o custo para as seguradoras afetadas pelo esquema italiano foi de mais de 700.000 euros, com 274 pessoas suspeitas de participar da fraude. No próprio trabalho da Shift relacionado às redes de Ghost Broking que operam no Reino Unido, as seguradoras descobriram redes com até 400 apólices afetadas. Isso representa o potencial de centenas de milhares de perdas em cada rede.

Assim como em outras formas de fraude de apólices, a IA é fundamental para descobrir e impedir esse tipo de Ghost Broking. A capacidade de identificar links de rede por meio da proliferação de informações bancárias, informações de contato ou outras PII idênticas nas apólices é fundamental. As seguradoras que conseguem fazer isso estão bem equipadas para identificar links de rede associados a novas solicitações em tempo real, ajudando a impedir que essas solicitações registradas de forma fraudulenta se tornem apólices.



Uso da IA para ajudar a cometer fraudes

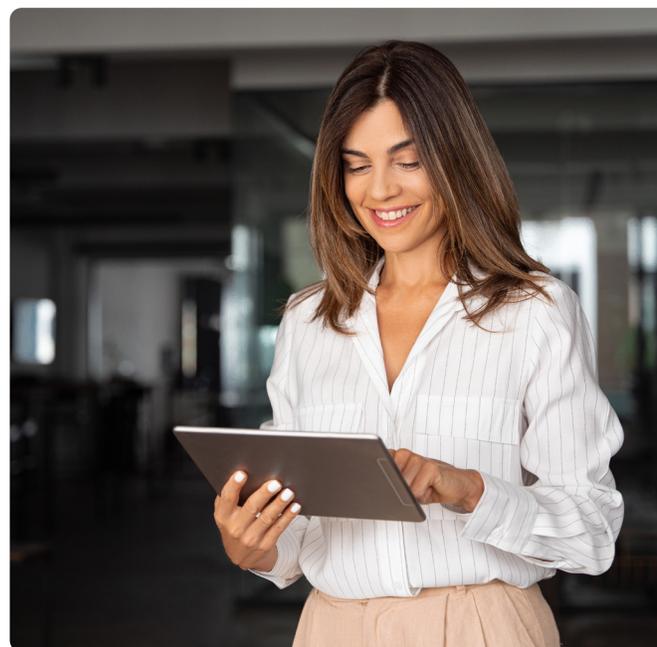
À medida que as ferramentas de IA e GenAI se tornaram amplamente disponíveis on-line e fáceis de serem consumidas tanto por novatos quanto por especialistas, sua utilidade para os Fraudadores rapidamente se tornou aparente. Os rápidos avanços na GenAI, mais especificamente, tornaram muito mais fácil criar imagens convincentes e documentação de apoio para uso em cenários de fraude de apólices ou sinistros. Os fraudadores podem produzir fotos mostrando danos extensos em um veículo ou residência. Eles podem criar ou manipular documentos, incluindo relatórios policiais, faturas ou estimativas, entre muitos outros. Para o olho

humano, essas “falsificações profundas de seguros” são difíceis de discernir dos documentos e imagens legítimos necessários para dar suporte a uma solicitação de apólice ou a um primeiro aviso de sinistro (FNOL). E, embora organizações como a Coalition for Content Provenance and Authenticity (C2PA) estejam tomando medidas para facilitar a identificação de imagens e documentos gerados por IA, sua existência por si só não resolverá o problema. Não só há um número incalculável de documentos e imagens já criados e em circulação, como também sempre haverá tecnologias disponíveis em fornecedores ou canais de código aberto que não participam da autorregulamentação do setor.

É nesse ponto que a IA pode desempenhar um papel importante para combater a fraude digital. A resolução de entidades e a detecção de redes podem ser usadas novamente para identificar PII comuns e outras formas de dados em documentos manipulados ou criados, levantando uma bandeira vermelha de que há algo suspeito acontecendo no processo de subscrição ou de sinistros. Tão importante quanto isso, a análise de documentos e imagens com IA é capaz de identificar de forma rápida, eficiente e precisa aberrações de imagens, anormalidades de metadados ou outros indicadores de esquemas de fraude baseados em IA generativa e identificar apólices ou sinistros relacionados que precisam de revisão ou investigação adicional.

Conclusão

A revolução digital abriu oportunidades incríveis para as seguradoras fazerem negócios de uma forma mais diretamente alinhada às necessidades de seus clientes. A adoção de modelos de comércio online e o acesso “em qualquer lugar, a qualquer hora” criaram novas eficiências e conveniências para as seguradoras e



seus clientes. No entanto, a remoção da interação humana de determinadas transações abriu a porta para que agentes mal-intencionados se aproveitassem do novo normal. As ferramentas digitais que deram poder à revolução do seguro estavam sendo usadas ativamente contra o setor para cometer fraudes. Mas as seguradoras mais experientes estão atentas a esses novos esquemas e usando soluções baseadas em IA para detectar e impedir fraudes digitais em seguros.

SHIFT

Sobre a Shift Technology

A Shift Technology oferece soluções de tomada de decisões baseadas em IA para beneficiar o setor global de seguros e seus clientes. Nossos produtos permitem que as principais seguradoras do mundo melhorem seus índices combinados, otimizando e automatizando decisões críticas em todo o ciclo de vida da apólice. As soluções da Shift ajudam seus clientes a mitigar fraudes e riscos, aumentar a eficiência operacional e proporcionar melhores experiências.

Saiba mais em www.shift-technology.com/pt.