BLOG · MERCADO DE SEGUROS & FRAUDE DIGITAL

Fraude de imagem em seguros: como um arquivo JPEG pode custar R$ 1,1 bilhão por ano

Por **Comitê de Tecnologia e Compliance da Provvi**

Uma fotografia tirada com um smartphone comum pode ser editada em segundos por qualquer pessoa com acesso a um aplicativo gratuito. Danos que nunca existiram aparecem em para-choques. Veículos que estavam intactos ganham amassados. Objetos desaparecem de cenas de sinistro. Propriedades que jamais pegaram fogo mostram fumaça e chamas convincentes.

Esse não é um cenário futurista. É o que o mercado segurador brasileiro enfrentou em 2024, e os números do relatório mais recente da CNseg — a Confederação Nacional das Seguradoras — deixam a dimensão do problema em evidência.

Os números do problema: o que o CNseg revela

O 22º Ciclo do Sistema de Quantificação de Fraudes (SQF), divulgado pela CNseg em 2025, traz um retrato preciso e preocupante:

Indicador	Valor 2024	Variação vs. 2023
Sinistros ocorridos (total)	R$ 41 bilhões	—
Sinistros classificados como suspeitos	R$ 5,4 bilhões (13,3%)	↑
Fraudes efetivamente comprovadas	R$ 1,1 bilhão	↑
Fraudes / sinistros ocorridos	2,7%	↑ de 2,2%
Transportes: sinistros suspeitos (1º sem.)	34,4% das ocorrências	Alta vulnerabilidade

O ramo de Automóveis concentra a maior fatia — 34,2% de todo o prêmio ganho do mercado — e segue como o mais representativo em termos financeiros de fraude. Em seguida aparecem Pessoas Coletivo (25,4%) e Patrimonial (17,3%).

> *R$ 5,4 bilhões em sinistros suspeitos. R$ 1,1 bilhão confirmado como fraude. Esses números excluem a Saúde Suplementar — ou seja, o problema real é ainda maior.*

O papel da imagem na fraude de sinistros

A fotografia é o principal instrumento de prova em um sinistro. É dela que parte a análise do ajustador, a decisão do perito e, em última instância, o pagamento ou a negativa da indenização. É exatamente por isso que ela se tornou o principal vetor de fraude.

As modalidades mais comuns envolvendo manipulação de imagem incluem:

- **Reutilização de imagens:** fotos de danos em veículos capturadas em sinistros anteriores ou de terceiros, apresentadas como o evento atual.
- **Adulteração de fotos:** edição digital para acrescentar ou ampliar danos que não existiam ou eram menores.
- **Síntese por inteligência artificial:** imagens geradas ou modificadas por IA para criar cenas de sinistro convincentes.
- **Falsificação de metadados:** coordenadas e timestamps alterados para deslocar geograficamente ou temporalmente o evento.
- **Recaptura de tela:** captura de uma foto de uma foto exibida em tela, tornando difícil rastrear a origem.

O problema técnico central é simples: um arquivo JPEG não carrega nenhuma prova intrínseca de sua origem. O nome do arquivo, a data gravada nos metadados EXIF e as coordenadas GPS são todos dados facilmente editáveis com ferramentas gratuitas disponíveis em qualquer sistema operacional.

> *Metadados EXIF podem ser alterados em segundos. Um arquivo com data, hora e localização "corretos" pode ter sido criado ontem a partir de uma foto de 2019 tirada em outro estado.*

O cenário internacional: o problema é global e se acelera

O Brasil não está sozinho. A fraude de imagem em seguros é um fenômeno global que se intensificou com a popularização de ferramentas de IA generativa.

No Reino Unido, a Association of British Insurers (ABI) registrou £1,16 bilhão em sinistros fraudulentos detectados em 2024 — alta de 2% em relação ao ano anterior. Fraudes de automóvel representaram 53% do total, com 51.700 casos detectados. A ABI aponta crescimento acelerado no uso de deepfakes e imagens manipuladas por IA nas solicitações de sinistros.

Nos Estados Unidos, o Coalition Against Insurance Fraud estima que fraudes custam ao setor mais de US$ 308 bilhões por ano. Entre 10% e 20% das solicitações de indenização nos EUA são classificadas como fraudulentas, e o custo médio recai sobre o consumidor honesto na forma de prêmios mais altos — estimados em US$ 700 a US$ 900 por família por ano.

Estudos recentes apontam que 25% a 30% das solicitações de sinistro hoje envolvem imagens, laudos médicos ou certificados de avaliação alterados por IA generativa — uma proporção que cresce a cada trimestre. A Swiss Re, em relatório de 2025, documenta uso crescente de deepfakes em claims de seguros em múltiplos países europeus e asiáticos.

A Pindrop registrou alta de 475% em ataques de voz sintética contra seguradoras em 2024. Especialistas projetam crescimento de 162% em ataques de deepfake contra o setor no próximo ciclo anual.

Por que a detecção tradicional falha

As seguradoras investem em sistemas de detecção de fraude baseados em análise comportamental, cruzamento de histórico e inteligência artificial aplicada a padrões de sinistro. Esses sistemas são eficazes para detectar fraudes repetitivas e redes organizadas.

Mas a fraude de imagem unitária — aquela em que um segurado individual edita uma foto antes de enviá-la — é estruturalmente diferente. Ela não produz padrões de comportamento anômalos detectáveis por modelos preditivos. A imagem chega ao sistema de sinistros como um arquivo aparentemente legítimo, com metadados plausíveis e danos visualmente coerentes com o relato.

A única forma de detectar essa modalidade de fraude de forma confiável é verificar a autenticidade da imagem na origem — ou seja, no momento da captura. Uma vez que o arquivo sai do dispositivo sem uma assinatura criptográfica vinculada ao hardware, o que se tem é apenas pixels sem proveniência verificável.

> *Não existe análise forense que restaure a proveniência de uma imagem que nunca teve sua origem registrada. A autenticidade precisa ser garantida no momento da captura — não depois.*

O custo oculto que recai sobre todos

R$ 1,1 bilhão em fraudes comprovadas não desaparece do sistema. Esse valor é redistribuído de três formas:

- **Aumento de prêmios:** seguradoras elevam as tarifas para compensar as perdas com fraude, e o consumidor honesto paga a conta.
- **Custos operacionais de investigação:** cada sinistro suspeito exige investigação, perícia e análise jurídica — custos que não aparecem nos R$ 1,1 bilhão mas que multiplicam o impacto real.
- **Restrição de cobertura:** seguradoras que enfrentam altos índices de fraude tornam-se mais conservadoras na aprovação de sinistros legítimos, prejudicando segurados honestos.

O estudo LexisNexis True Cost of Fraud aponta que o custo real das fraudes pode multiplicar o prejuízo inicial quando contabilizados os processos de investigação, consultorias forenses e litígios — um multiplicador estimado entre 2,5x e 4x sobre o valor nominal da fraude.

A solução técnica: autenticidade na captura

O padrão C2PA — Coalition for Content Provenance and Authenticity — resolve o problema de forma elegante: em vez de tentar detectar adulteração após o fato, ele garante que a imagem original é matematicamente vinculada ao dispositivo, ao momento e ao local da captura.

Quando uma foto é capturada com um sistema compatível com C2PA, um manifesto criptográfico é criado e embutido no arquivo. Esse manifesto contém:

- um hash SHA-256 do frame original — qualquer alteração de qualquer pixel invalida o hash
- coordenadas GPS verificadas por múltiplas fontes (GPS, rede, sensores)
- timestamp vinculado a uma autoridade de tempo confiável
- assinatura criptográfica do servidor — no caso do Brasil, um certificado ICP-Brasil

O resultado é que a tentativa de substituir a foto por uma imagem editada produz um hash diferente do registrado no manifesto, e a verificação falha imediatamente. Não há forma de contornar isso sem acesso à chave privada do servidor assinador.

No contexto brasileiro, a combinação com ICP-Brasil — a infraestrutura de chaves públicas do governo federal — eleva o nível de garantia: a assinatura tem validade jurídica reconhecida pelo ordenamento legal nacional, transformando a autenticidade técnica em prova admissível em processos administrativos e judiciais.

Implicações para a gestão de sinistros

Para uma seguradora ou gestora de risco que adota captura autenticada C2PA como padrão em sua vistoria ou no processo de abertura de sinistro, a mudança operacional é significativa:

- **Redução de custos de investigação:** imagens com manifesto C2PA válido dispensam análise forense adicional — a autenticidade está matematicamente comprovada.
- **Triagem de risco:** sinistros com imagens não autenticadas passam automaticamente para fila de revisão manual, concentrando recursos onde o risco é real.
- **Suporte legal:** o manifesto C2PA serve como documento de cadeia de custódia admissível em disputas judiciais e processos na Susep.
- **Precificação de risco:** a exigência de captura autenticada como condição de cobertura ou como elemento de precificação cria incentivos para o segurado colaborar com a prevenção à fraude.

---

provvi **Autenticidade que se prova**

O Provvi resolve na origem o problema que este artigo descreve: cada imagem capturada pelo SDK carrega um manifesto C2PA com hash SHA-256, geolocalização verificada, timestamp e assinatura ICP-Brasil — tornando tecnicamente impossível substituir ou adulterar a foto sem que a adulteração seja detectada na verificação.

Para seguradoras, isso significa evidências fotográficas de sinistros e vistorias que não podem ser questionadas. Para gestores de risco, significa cadeia de custódia completa desde o momento da captura.

→ **provvi.com.br**

Produzido por **Comitê de Tecnologia e Compliance da Provvi**

As informações contidas neste artigo têm caráter educativo e não constituem aconselhamento jurídico ou técnico. Dados do SQF/CNseg referentes ao ciclo de 2024.