When Fraudsters Have AI Too

What the AI Arms Race in Insurance Means for Advisors and Their Clients

By Virendra Singh Chawra
Specialist, Data Engineering, AI & Data

Picture this: a claims adjuster receives a voicemail from a policyholder reporting a total loss. The voice is familiar, the details check out, the story is airtight. Except the policyholder never called. The voice was synthetic, generated in seconds, and the claim was engineered by a fraud ring that had scraped social media for just enough personal detail to make the story convincing.

This isn't a hypothetical from a cybersecurity conference. It's already happening across the insurance industry, and it's part of why global financial fraud losses topped an estimated $12.5 billion in a single recent year. For advisors, this shift matters more than it might first appear, because when fraud gets smarter, so does everything downstream of it: underwriting, pricing, claims timelines, and the conversations you have with clients.

THE FRAUDSTERS HAVE AI TOO

For years, insurers have talked about AI as a defensive tool — a way to flag suspicious claims, detect anomalies in transaction patterns, and speed up underwriting decisions. That story is still true, but it's now only half the picture.

The same machine learning and generative AI capabilities carriers use to catch bad actors are increasingly available to bad actors themselves. Synthetic identities, AI-generated documentation, deepfake audio and video, and automated social engineering scripts have turned fraud from a manual, opportunistic crime into a scalable, industrialized one. Fraud rings can now run thousands of synthetic applications or claims simultaneously — each individually plausible — testing an insurer's defenses the way a hacker probes a firewall.

In response, the industry is moving toward what researchers call “next-generation” fraud management: systems that combine traditional machine learning with graph analytics (which map relationships between people, policies, and claims to expose hidden networks) and, increasingly, agentic AI — autonomous systems that don't just flag a suspicious claim but actively investigate it, pulling data from multiple sources and building a case file the way a human investigator would, only faster and at far greater scale.

WHAT'S CHANGING IN UNDERWRITING

This arms race isn't confined to claims. It's reshaping underwriting itself.

Modern underwriting increasingly relies on explainable AI: models sophisticated enough to assess risk in real time, yet transparent enough that an underwriter — and a regulator — can understand why a given applicant received a given price. This matters enormously in casualty and commercial lines, where graph-based models can now surface hidden connections between applicants, prior claims, and known fraud networks that a traditional rules-based system would never catch.

At the same time, regulators are watching closely. State insurance commissioners and international bodies alike are pushing for algorithmic accountability, meaning insurers can no longer treat AI-driven pricing or underwriting decisions as a black box. Explainability isn't just a nice technical feature anymore; it's becoming a compliance requirement. Enterprise risk management (ERM) frameworks are being rebuilt around this reality, with fraud detection, model transparency, and regulatory reporting increasingly treated as a single, integrated discipline rather than separate silos.

For carriers, this means faster, more accurate underwriting decisions. For advisors, it means the underwriting process your clients experience today looks fundamentally different than it did even three years ago — and it will keep changing.

WHAT THIS MEANS FOR YOU AND YOUR CLIENTS

Here's where the technical shift becomes a practical one for advisors:

Clients will ask why. As AI plays a larger role in pricing and claims decisions, expect more clients to ask why their premium changed, why a claim is under additional review, or why an application triggered extra questions. Advisors who understand the broad strokes of explainable AI and fraud analytics will be far better positioned to answer confidently than those who simply defer to “that's what the system said.”

Speed cuts both ways. Agentic AI investigation tools mean legitimate claims can be resolved faster than ever — a genuine win for client satisfaction. But it also means fraud investigations can escalate quickly, and a client caught in a false positive needs an advocate who understands the process well enough to intervene effectively.

Trust becomes your differentiator. As underwriting and claims become more automated, the human relationship doesn't become less important — it becomes more important. Clients increasingly want someone who can translate what the algorithm decided into something that makes sense for their life, their business, and their risk tolerance. That translation work is not something AI does well, and it's not going away.

Your own vigilance matters. Advisors handle sensitive client data and are themselves potential targets for social engineering, including AI-generated impersonation attempts aimed directly at agencies. Basic awareness of these tactics — verifying unusual requests through a second channel, for instance — is quickly becoming as essential as any other part of professional practice.

THE OPPORTUNITY AHEAD

It's tempting to view all of this as a threat to advisors' relevance, to client trust, to the pace of an already complex industry. I'd argue the opposite. Every technological shift in insurance, from actuarial tables to telematics, has ultimately raised the value of advisors who understand the technology well enough to guide clients through it, rather than simply operate downstream of it.

The advisors who thrive over the next several years won't be the ones who ignore AI, nor the ones who defer to it blindly. They'll be the ones who understand it well enough to ask good questions, explain decisions clearly, and remain the trusted human presence their clients turn to when the stakes are real. That's a role no algorithm — however capable — can fill.

ABOUT THE AUTHOR

Virendra Singh Chawra is a Specialist in Data Engineering, AI & Data and a NAIFA member, with extensive, long-standing experience architecting AI, machine learning, and data engineering solutions across banking, insurance, and life sciences globally. He holds an MS in Computer Science and specializes in fraud, risk, and compliance analytics, building governed, secure AI platforms that safeguard institutions from financial crime and regulatory exposure. A recognized industry speaker, thought leader, and published researcher, his original contributions have significantly advanced enterprise AI adoption worldwide, and he plays a leading role bridging cutting-edge innovation with data governance, security, and regulatory compliance across highly regulated global industries.