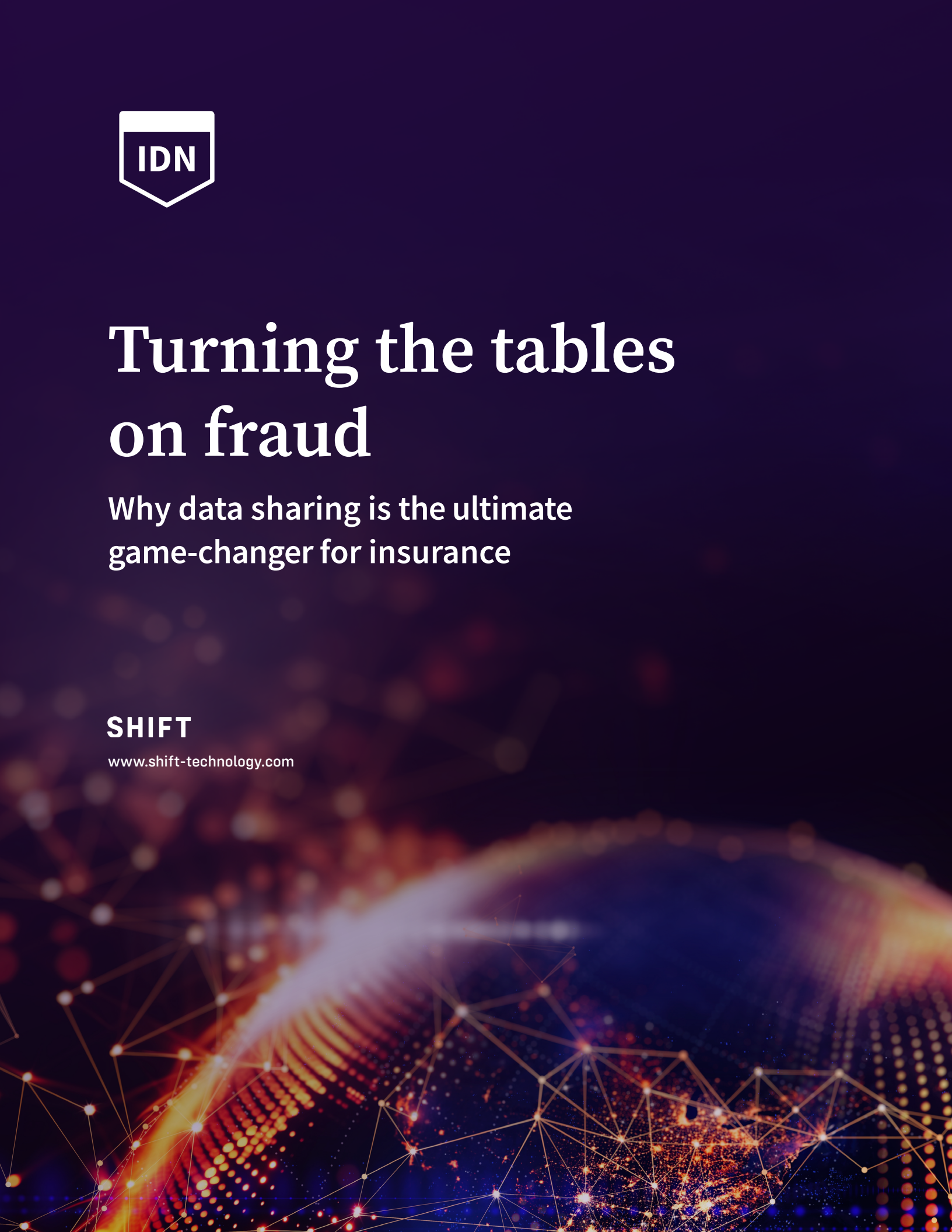
IDN

Turning the tables on fraud

Why data sharing is the ultimate game-changer for insurance

SHIFT

www.shift-technology.com



Meeting the common enemy

The insurance industry has long operated on a central paradox: carriers must fiercely compete for market share while simultaneously navigating systemic threats that target the entire industry. Historically, the battle against insurance fraud has been fought within defensive, proprietary corporate walls. However, this isolated strategy is rapidly becoming obsolete due to a fundamental shift in the risk landscape: the democratization of advanced artificial intelligence.

> **"What we're talking about is turning fraud into a living, dynamic thing... That's where the team sport idea came in. It's like, we're playing together, not against each other. When it comes to fraud, at least."**
>
> **— Bryan Falchuk, Author of "The Future of Insurance"**

Today, fraud networks leverage sophisticated, highly accessible AI infrastructure to generate hyper-realistic falsified claims documentation, images, and videos in seconds and at a fraction of traditional costs. Because these criminal syndicates operate globally and systematically across multiple companies, a single carrier looking only at its own internal data is essentially blind to the macro-patterns of modern fraud rings. To defeat an adversary armed with scaled technology, insurance carriers can no longer treat fraud as an individual problem. Fraud detection must evolve into an industry-wide collaborative effort where carriers align to protect the collective premium pool.

Demystifying the Insurance Data Network (IDN)

For decades, P&C carriers have utilized cross-carrier loss history databases. However, traditional industry repositories have been limited by critical, inherent flaws: inconsistent data quality, varying contribution volumes from participating companies, and a reactive application process. Historically, a Special Investigation Unit (SIU) investigator would only request a static loss history report after a claim had already been flagged as suspicious or referred for a fraud investigation.

IDN's defining differentiator is data consistency, requiring every participating carrier to contribute 100 standardized data elements per claim. This uniform dataset allows the network to move loss history data straight to the front of the claims journey, embedding it directly into initial automated fraud analytics models. Instead of waiting for a manual referral, incoming claims are automatically cross-referenced against historical behaviors across the entire network, injecting immediate risk signals based on past entity behaviors across multiple carriers.

> **"We're taking data and we're summarizing it, and we're leveraging it at scale in analytics. And that's the big payoff... This is allowing you to see across the entire industry the patterns of behavior that might be occurring relative to specific providers or large networks of colluding individuals."**
>
> **— Dan Donovan, Head of IDN Solutions, Shift Technology**

Furthermore, IDN leverages advanced AI to automate the consumption of massive datasets. Rather than forcing a human investigator to manually parse a 20-page match report, the system summarizes the cross-carrier insights automatically, delivering actionable intelligence instantly to the user. Crucially, the network introduces a transformational "mutual flagging" capability: if a claim involves two participating carriers and one side places the claim under active SIU investigation, the other carrier is automatically notified within a 24-hour cycle.

The strategic advantages for carriers

Operating in high-risk regional environments — such as the volatile "Tornado Alley" of the American Midwest — requires carriers to maintain an exceptional focus on customer retention and long-term service. For modern insurance organizations, participating in a shared data asset like IDN acts as a massive operational amplifier, effectively providing "night vision glasses" that uncover critical fraud risks completely hidden within an individual company's data silo.

Sophisticated fraud rings operate systematically by executing isolated, low to medium value claims across multiple insurance companies to avoid triggering internal carrier thresholds. A single carrier looking only at its own data might see 10 or 15 seemingly normal claims from a specific body shop, medical provider, or contractor, completely unaware that the same entity has hit other carriers with hundreds of inflated claims. IDN exposes these macro-level patterns instantly, shifting an organization from a reactive posture to a proactive defense before massive losses are paid out.

> **"Talking about IDN and the shared responsibility that we have to combat fraud and suspicious activity, I really look at it as the night vision glasses. That's the notion I really think it is. We all— all insurance companies have different tools to combat fraud and suspicious activity, whatever technology you use it...Getting that extra edge, that extra data element that really makes it very powerful from that perspective, especially, you know, when you look at the AI."**
>
> **— Vibhor Gupta, Vice President, Shelter Insurance Company**

Crucially, experience proves that sharing structured fraud data does not degrade a carrier's competitive edge. True differentiation in the modern insurance marketplace happens through exceptional customer service, product innovation, and claims processing speed. In fact, data collaboration directly improves customer experience by enabling faster straight-through processing (STP). By instantly validating that an incoming claim has zero suspicious matches across the industry network, carriers can confidently fast-track legitimate claims, delighting honest policyholders while concentrating specialized SIU resources strictly on high-risk files.

Overcoming the blockers: perception vs. reality

When evaluating a cross-carrier data sharing model, internal corporate stakeholders frequently raise concerns regarding security, competitive risk, and corporate governance. IDN's framework addresses these concerns by replacing outdated assumptions with modern realities.

Traditional blocker / objection	IDN reality & mitigation
"Data sharing sacrifices our competitive advantage."	**False.** Fraud increases premium costs for everyone. Competitive advantage is built on customer service, coverage options, and processing speed — not on hoarding isolated fraud signals.
"We must protect proprietary customer PII and files."	**Mitigated.** The network does not ingest entire customer files. It extracts only the minimal 100 specific data elements strictly necessary to run high-quality entity matching.
"We lose ownership and control of our data asset."	**False.** Carrier data isn't unfettered within Shift's systems — it only surfaces as relevant context tied to a fraud alert on an active claim, under a rigid data privacy and access model. Shift acts strictly as an analytics processor, not a data owner.
"We can just build our own advanced AI models in-house."	**Insufficient.** While carriers possess talented data scientists, an in-house model is strictly limited by an isolated data pool. Models cannot detect cross-carrier fraud rings without a shared network.
"AI regulations and governance make this too complex."	**Managed.** The network provides clear transparency and documentation, enabling carriers in highly regulated environments to meet modern AI governance and disclosure mandates seamlessly.

Why joining the network is a must

The traditional methodology of managing fraud within defensive corporate silos is fundamentally inadequate against modern, AI-empowered criminal enterprises. As fraud rings dynamically pivot from one carrier to the next, a reactive strategy ensures that companies only see the financial damage long after the loss has been paid.

With 4 of the top 5 P&C carriers already actively contributing to the Insurance Data Network, the compounding data network effect means that visibility grows more precise every day. Carriers operating outside of this network are effectively fighting an organized, high-tech opponent in pitch-black darkness. Joining IDN is not about giving up proprietary secrets; it is about arming an organization with real-time, predictive intelligence to protect its premium pool, optimize SIU operations, and fast-track exceptional service for honest customers.

The infrastructure is built, the guardrails are proven, and the industry has established a new standard. It is time to stop playing defense in isolation and join the collaborative network winning the fight against fraud.