United against fraud: Are you part of the solution?

How four of the top five insurers use IDN to stay one step ahead

Carriers using IDN are pulling ahead—are you keeping up?

IDN ingests 100+ claim data points across carriers, auto-matches records, and feeds them into detection models—no manual checks. It then summarizes loss histories into clear, actionable insights to speed fraud decisions and streamline claims. Keep reading to see how IDN gives carriers the edge.

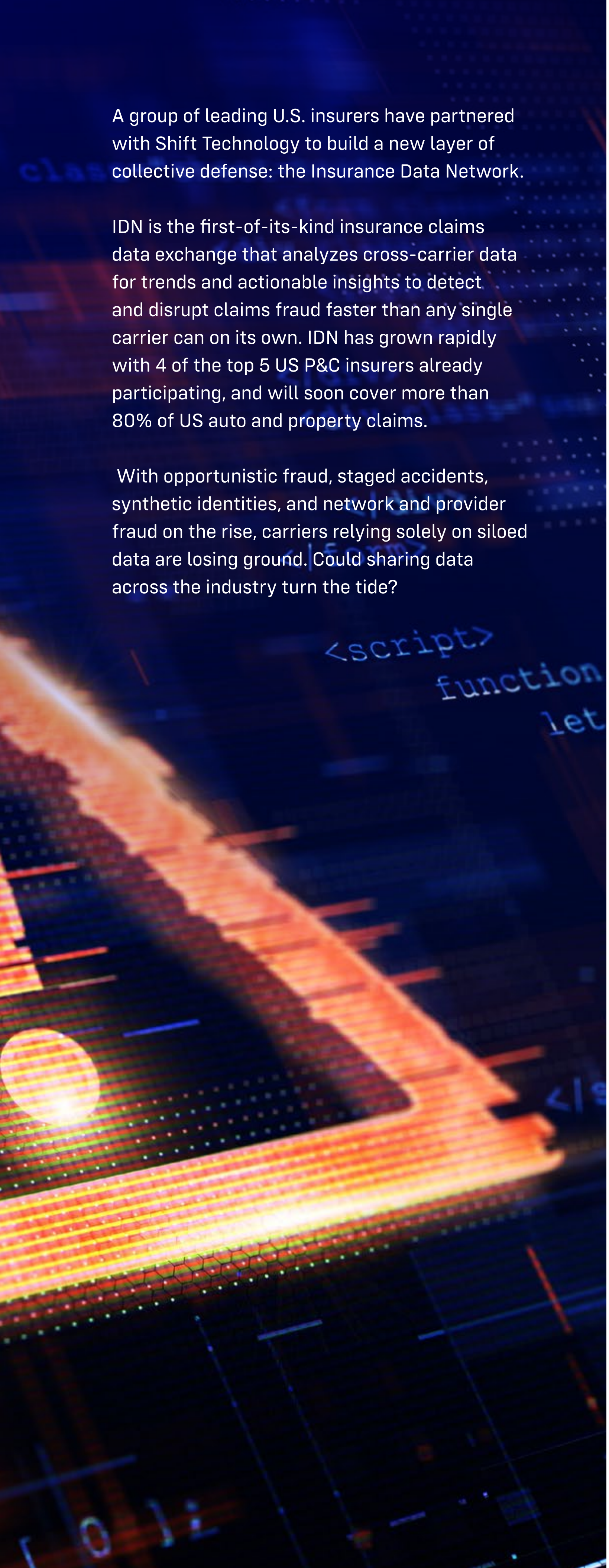
IDN

SHIFT

A group of leading U.S. insurers have partnered with Shift Technology to build a new layer of collective defense: the Insurance Data Network.

IDN is the first-of-its-kind insurance claims data exchange that analyzes cross-carrier data for trends and actionable insights to detect and disrupt claims fraud faster than any single carrier can on its own. IDN has grown rapidly with 4 of the top 5 US P&C insurers already participating, and will soon cover more than 80% of US auto and property claims.

With opportunistic fraud, staged accidents, synthetic identities, and network and provider fraud on the rise, carriers relying solely on siloed data are losing ground. Could sharing data across the industry turn the tide?



The rising threat: Why intelligence sharing is no longer optional

Insurance fraud is growing in frequency, severity, and sophistication. The rise in organized staged-accident schemes prompted the introduction of the Staged Accident Fraud Prevention Act of 2025, which aims to make this type of fraud a federal offense. And the industry is experiencing higher incidence of synthetic identity and opportunistic fraud across personal and commercial lines. Two structural realities make this trend especially dangerous for individual carriers:

Fraud rings operate across carriers, geographies, and channels. A pattern that is invisible within one insurer's claims data may be obvious when viewed at scale across multiple carriers claims data.

Timing and fragmentation favor attackers. Slow, manual information sharing gives fraudsters windows to submit repeat or parallel claims to different insurers before patterns are recognized.

No matter how advanced, unilateral countermeasures quickly reach their limits when the underlying data is sparse. Pooled insights and near-real-time intelligence are therefore essential. Cross-carrier claims data, fed into an automated AI fraud-detection engine to produce near-real-time alerts and actionable intelligence, must be a central component of every carrier's fraud strategy.

Enter IDN: The network that makes collective defense possible

IDN is a secure insurance-claims data-sharing network designed to unite insurers in the fight against fraud. It connects participating carriers' claims data and real-time analytics to reveal suspicious patterns that cross organizational boundaries and stop fraud quickly.

Key capabilities:

- **Automated cross-carrier pattern detection:** correlates claims, provider networks, and shared third-party signals.
- **Fast, scalable analytics and adaptive AI:** models that evolve with shifting fraud tactics and run at network scale.
- **Robust governance and privacy-preserving matching:** strict access controls and privacy safeguards to protect policyholder data and ensure compliance.
- **Workflow integration:** alerts that feed directly into Shift Claims Fraud so intelligence becomes immediately actionable.

In short, IDN acts as a force multiplier—more like a collective nervous system than a static data warehouse—enabling coordinated, rapid response across carriers.

CASE STUDY

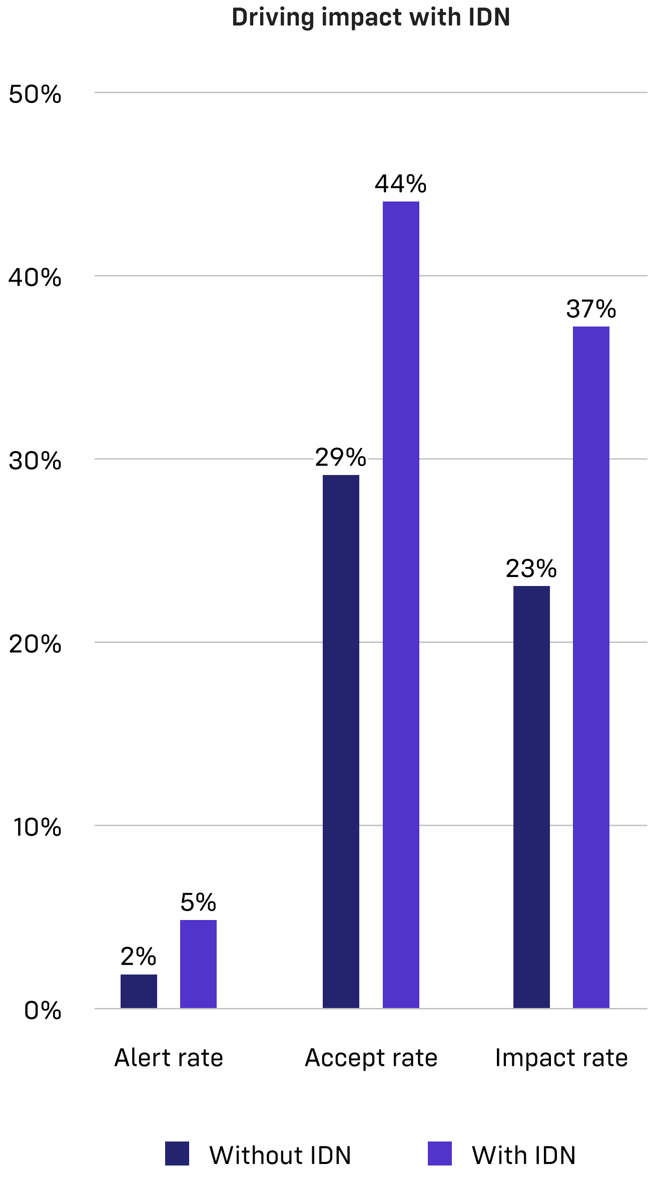
Dismantling fraud: IDN results at a top-5 insurer

A top 5 US P&C insurer joined Shift early on in the development of IDN. Already achieving millions in stopped fraud with Shift Claims Fraud detection, they were able to amplify their fraud program even further with IDN.

More, higher-quality alerts
IDN increased alert volume by 3%, with alerts 1.5x as likely to be accepted for review compared to traditional sources.

Actionable cases up
Higher-quality alerts led to more investigations and a 14% increase in impactful fraud cases detected.

Significant net-new impact
With no other detection changes, IDN nearly doubled fraud mitigation, increasing by 10's of millions in net-new fraud impact.


Driving impact with IDN

IDN: Maximizing industry intelligence to crush claims fraud

Insurers' reliance on internal data and slow, incomplete manual searches of loss-history records has created gaps in fraud defenses that organized rings, unscrupulous providers, and opportunistic individuals exploit. IDN tackles this head on: it tears down carrier silos, surfaces cross-carrier connections in near real time, and turns data into actionable intelligence.

Faster detection
How: Cross-carrier linkages highlight prior claim fraud, reveal reused identifiers, shared vendors, and repeat behaviors.

Outcome: Suspicious claims flagged in minutes instead of days, stopping staged schemes and serial fraudsters sooner.

Fewer false positives
How: Corroborating data from multiple carriers raise model confidence and cut noise.

Outcome: Investigators focus on real leads; true-positive rates rise across both individual and organized fraud.

Automated, real-time insights
How: Automated transformation of data into actionable, fraud alerts—eliminating time consuming manual searches and analysis and streamlining decision-making.

Outcome: Faster identifications and escalations—swiftly containing high-risk claims before payouts happen.

Stronger case outcomes
How: Timely, corroborated claim loss history details enables decisive referrals and investigations.

Outcome: Non-meritorious claims are resisted, and meritorious claims are paid faster.

Lower cost per fraud case and greater deterrence
How: Faster, more accurate, fraud detection and insights that allow for targeted investigation activities.

Outcome: Reduced time to detection, faster investigation cycle times, Lower investigation costs and a measurable drop in repeat and cross-carrier fraud attempts.

Why IDN works: The mechanics behind faster, smarter detection

IDN combines four key elements that improve precision and speed:

1. Network-scale AI
AI models accessing richer, cross-carrier datasets surface complex linkages to uncover provider, network and individual fraud that single-carrier models miss.

2. Link and timeline analysis
Network methods reveal coordinated behavior patterns (shared providers, repeated touchpoints, temporal clustering) that are invisible to isolated systems.

3. Human-in-the-loop validation
Analysts validate model outputs, inject context, and feed outcomes back into model training—closing the learning loop.

4. Privacy and compliance are central
IDN relies on a highly secure environment, one-way hashing for identifiers, purpose-limited access, These safeguards help protect policyholder data while preserving analytic value.

Together, these elements enable IDN to detect sophisticated, coordinated fraud faster and more accurately while preserving strict privacy and compliance safeguards.

Industry impact: Benefits beyond fraud reduction

Beyond identifying and stopping non-meritorious claims, IDN reshapes how insurers operate and how the market behaves. By making cross-carrier claims intelligence automated and timely, IDN drives downstream benefits across operations, customer experience, and deterrence, advantages that continuously compound as more carriers collaborate.

- **Stabilized premiums:** Accurate and automated fraud detection at scale reduces upward pressure on rates, making pricing more affordable for honest policyholders.
- **Faster claims for legitimate customers:** Timely automated alerts let insurers clear high-confidence claims quickly, improving cycle times and customer satisfaction.
- **Smarter resource allocation:** With fewer false leads, and cross-carrier loss history insights, investigators focus on the most suspicious cases allowing for improved investigation quality and appropriate investigation outcomes.
- **Market deterrence:** Unified defenses raise the cost and risk for organized fraud rings, reducing the overall incidence of coordinated schemes.

Challenges with cross-carrier intelligence and how IDN overcomes them

Implementing a cross-carrier network is not trivial. Common hurdles include:

- Data standardization
- Legal and regulatory complexity
- Cultural resistance to sharing
- Integration with legacy claims systems

IDN has solved these challenges using these mitigation strategies:

Clear governance and legal templates that define roles, liabilities, and permitted uses

Standardized schemas and API-based connectors to reduce integration effort

Executive sponsorship and cross-functional working groups

Pilot programs focused on high-impact use cases to demonstrate value quickly

Future outlook: Scaling collective defense with IDN

The path forward is clear: expand participation, accelerate real-time industrywide alerts, and layer predictive risk scoring that identifies emerging fraud trends before they proliferate. Beyond fraud, the IDN model can be adapted for subrogation, claims automation, and other industry challenges where cross-carrier visibility creates outsized value.

Four of the top five insurers joining forces via an Insurance Data Network marks a pivotal shift from isolated defenses to a collective, data-driven front against fraud. The result: faster detection, improved loss ratios, better customer outcomes, and a stronger deterrent effect. With robust governance and privacy protections, this collaborative model can set a new industry standard for protecting customers and preserving market integrity. If the industry wants to turn the tide on sophisticated fraud, secure, governed collaboration is now a practical necessity.

Learn more about IDN

IDN

SHIFT