INDIALAW

SARFAESI

Zero-Tolerance 2025: IRDAI’s New Fraud Rule-Book for Every Insurer and Intermediary

AUTHOR Shrishail Kittad, Rahul Sundaram

PUBLISHED 14 October 2025

On 1 April 2026 the Indian insurance sector will quietly flip a page that has been in circulation since 2013. A fresh set of legally binding instructions—titled the Insurance Regulatory and Development Authority of India (Insurance Fraud Monitoring Framework) Guidelines, 2025—will become the new operating system for every life, general, health and re-insurer, every corporate broker, web-aggregator, bank-assurance partner, motor-garage, hospital and the humble neighbourhood agent. The regulator's message is blunt: fraud is no longer an operational risk to be noted in annual reports; it is a strategic threat to public trust and financial stability, and every stakeholder must own a slice of the solution.

The guidelines open with a crisp statement of intent: build a zero-tolerance ecosystem that deters, prevents, detects, reports and remedies fraud in every corner of the insurance value chain. To give the statement teeth, the document first re-sets the legal clock. It repeals the thirteen-year-old 2013 framework and makes itself applicable, unless specifically exempted, to "all insurers and distribution channels" from the first day of the new financial year 2026-27.

Definitions have been tightened so that no one can plead ignorance. "Insurance fraud" now covers any dishonest act or omission designed to grab a financial or contractual advantage, stretching from fund misappropriation and material mis-statement to the abuse of fiduciary trust. A "red-flag indicator" is formalised as an early-warning signal that must be investigated, while "cyber or new-age fraud" gets its own standalone identity, covering every tech-enabled trick that criminals can throw at companies or customers.

Knowing that jargon kills compliance, the regulator has also given the industry a common language for classifying fraud. Every suspicious event must be bucketed into one of five categories: internal fraud by employees or senior management; distribution-channel fraud; policy-holder or claims fraud; external fraud by vendors, hospitals or garages; and affinity or complex fraud where two or more parties collude. This taxonomy is not academic—quarterly and annual returns to the board and to IRDAI must use these exact heads, allowing the Insurance Information Bureau to build a single, industry-wide heat map.

The heart of the new regime is the Fraud Risk Management Framework, a living set of controls that must be approved by the board and reviewed at least once a year. The framework must be entity-specific, calibrated to the insurer's size, product mix, technology stack and distribution profile. It has to contain a board-approved anti-fraud policy that lists every red-flag indicator relevant to the business, spells out procedures from deterrence to remedy, fixes turnaround times for investigations, names the officers who must be copied on every fraud mail, and details the whistle-blower shield that protects informers. Resources must be earmarked for a dedicated Fraud Monitoring Unit, and missed-detection reviews have to be performed so that yesterday's blind spot does not become tomorrow's loss.

Running the framework on a day-to-day basis is the Fraud Monitoring Committee, chaired compulsorily by a key management person and staffed by senior heads of underwriting, claims, legal and technology. The committee can set up sub-groups, but it cannot harbour conflicts of interest. Its mandate is hands-on: recommend fresh controls when fraud patterns mutate, respond to every suspicion within pre-agreed cut-offs, maintain a forensic trail of evidence, share intelligence with peers, law-enforcement and the Insurance Information Bureau, and conduct an annual comprehensive fraud-risk assessment that stress-tests every business line against past incidents, emerging trends and the latest red-flag indicators. Each quarter the committee must send a report to the Risk Management Committee detailing incidents, financial impact and corrective steps; once a year it must place the fraud-risk assessment before the board; and every instance of internal fraud must simultaneously be reported to the audit committee so that governance and oversight stay fire-walled.

Risk identification is expected to be as scientific as pricing or reserving. Insurers have to build and refresh a library of red-flag indicators, weave them into policy-issuance, endorsement and claims workflows, and monitor their hit-rate continuously. Category-specific controls—preventive, detective and corrective—must cover each of the five fraud buckets. A central incident database of convicted or attempted fraudsters has to be maintained and referenced at the point of every new proposal or claim. Distribution-channel behaviour will be tracked for anomalies, customer grievances will be mined for hidden fraud signals, and fraud-sensitive audits will check whether controls are actually followed rather than merely documented.

Cyber fraud has been given special attention. Insurers must erect a robust cyber-security architecture that covers data leakage, identity theft, fake policy portals and ransom demands. Customer on-boarding and authentication processes have to be hardened through multi-factor checks, access controls and real-time anomaly detection. A cross-functional team combining risk and technology expertise must be empowered to monitor threats round the clock and update response playbooks after every attack.

The Insurance Information Bureau is recast as the industry's fraud intelligence hub. Every insurer must feed the bureau's platform with details of black-listed distributors, hospitals, third-party administrators and confirmed fraudsters. The bureau, in consultation with the life and general insurance councils, will issue a unique identifier for each policy-holder so that suspicious behaviour can be spotted irrespective of which company is being targeted. Real-time alerts will be pushed back to insurers, creating a collective immune system that stops a fraudster rejected by one company from re-entering through another door.

Re-insurers have not been left out. Indian companies that cede risk and foreign re-insurers that accept Indian business must apply the anti-fraud standards of the parent's home jurisdiction or these Guidelines, whichever is stricter, and must satisfy themselves that their counter-parties have adequate fraud-monitoring systems in place.

Distribution channels—corporate brokers, web-aggregators, banks, motor-dealers, hospitals and individual agents—face a two-tier obligation. Large intermediaries must create their own board-approved fraud-risk frameworks, train employees, vet sales staff, report suspicions to insurers and law-enforcement, and protect whistle-blowers. Smaller or individual channels must at minimum comply with the insurer's anti-fraud code and alert the insurer the moment they smell a scam. Failure to report can now expose the channel to regulatory action and permanent black-listing.

Training and awareness have been made non-negotiable. Insurers and intermediaries must run periodic programmes for employees, senior management, distribution partners and the general public, explaining how frauds are perpetrated, how red-flag indicators are spotted, and how confidential complaints can be lodged. The guidelines recognise that the best algorithm still cannot replace a vigilant human being at the point of sale or claim.

Reporting timelines have been compressed. Insurers must notify law-enforcement agencies without delay when legally warranted, file an annual statutory return in the new Form FMR-1 within thirty days of the close of the financial year, and escalate to IRDAI immediately if any IRDAI-registered distribution channel is involved. The twin objectives are quick restitution for victims and speedy ejection of bad actors.

Concluding paragraph

Come April 2026, insurance in India will cease to be a gentlemen's club where fraud is whispered about in closed auditoriums. The 2025 Guidelines turn every board-room, branch office, hospital cashless desk and mobile app into an outpost of a single, integrated defence network. If the industry implements the code with the same precision it brings to pricing mortality or catastrophe risk, the next decade could see fraud move from a tolerated cost of business to a rare, high-risk crime that quickly lands perpetrators in data black-lists, courtrooms and jail cells. The rule-book is now on the table; the countdown to zero tolerance has begun.

For further details write to contact@indialaw.in

Related Practice Areas

Corporate & Commercial