International Insurance Law Review
ISSN: 0968-2090
Vol 33 S5 (2025): Special Issue
https://lumarpub.com/iilr

Five Emerging Strategies to Detect and Control Fraud: Multiple Case Studies

Ruchi Agarwal
Assistant Professor, MDI Gurgaon (India), Department of Strategic Management
Email id: ruchi.agarwal@mdi.ac.in , ORCID ID :0000-0002-9836-5045
Sanjiv Dwivedi
Department of Commerce,
Applied Economics and Business Management Barkatullah Vishwavidyalaya, Bhopal, (India)
Ayushi Singh
Teaching and Research Assistant, MDI Gurgaon (India)
Email id: tra_ayushi_s@mdi.ac.in,
Correspondence Address: Ruchi, Block C, Sukhrali, Sector 17, Gurugram, Haryana 122007

Abstract

Fraud continues to pose a significant threat to companies, particularly in digitally-driven, high-volume environments such as the insurance sector. This article examines five emerging strategies—reactive, proactive, preventive, curative, and deterrence—used to detect and control fraud in Indian insurance companies over the last decade. A qualitative multiple-case study methodology was employed, focusing on three leading insurers. Data were analyzed using Dynamic Capability theory, emphasizing absorptive, adaptive, and innovative capacities to understand how firms anticipate, respond to, and mitigate fraud risks. Findings reveal that reactive strategies facilitate post-incident investigations and learning, proactive strategies leverage analytics and field investigations to anticipate fraud, preventive strategies strengthen internal controls and due diligence, curative strategies address systemic weaknesses from prior incidents, and deterrence strategies employ sanctions, regulatory escalation, and industry-wide collaboration. Companies effectively integrate these strategies, using dynamic capabilities to enhance resilience, reduce losses, and build stakeholder trust. The study contributes to the literature by empirically demonstrating the application of multi-layered fraud management strategies in the insurance context, bridging gaps in operationalizing traditional fraud theories such as the Fraud Triangle, Diamond, and Pentagon. Practically, the article highlights how insurers can combine multiple strategies and leverage organizational capacities to mitigate risks efficiently. These insights are valuable for policymakers, regulators, and industry practitioners seeking to strengthen fraud governance frameworks in emerging markets.

Keywords: Fraud management, insurance, reactive strategies, proactive strategies, preventive strategies, curative strategies, deterrence, dynamic capabilities

1. Introduction

Fraud control has historically been approached from a risk-reduction perspective, with internal audit departments primarily responsible for detecting and reporting irregularities to senior management or audit committees under the Three Lines of Defense model (White, 1995; White, 2016; Hillison et al., 1999; Agarwal & Kallapur, 2018). However, with the rapid growth of business

Citation: Agarwal, R.; Dwivedi, S.; Singh, A. (2025). Five Emerging Strategies to Detect and Control Fraud: Multiple Case Studies. *International Insurance Law Review,33(S5),57-71*

activities, the volume and complexity of fraud have increased substantially, especially in emerging markets.

Insurance professionals are now expected not only to ensure the accuracy of financial statements and due diligence but also to evaluate the effectiveness of organizational processes. Simultaneously, independent fraud control units have been established to prevent fraud, uncover misconduct, protect stakeholders, and mitigate financial and reputational risks, thereby enhancing profitability and corporate governance (Agarwal et al., 2025; Agarwal, 2025a). Despite the availability of traditional fraud models such as the Fraud Triangle (Cressey, 1953), Diamond (Wolfe & Hermanson, 2004), and Pentagon, existing literature reveals gaps in operationalizing these frameworks in high-volume, digitally-driven insurance environments.

The complexity of emerging markets, coupled with the proliferation of e-commerce, virtual insurance models, and digital payment channels post-COVID, challenges firms to understand the interplay of motivation, opportunity, and rationalization in daily transactions (Cressey, 1950, 1953). Moreover, while reactive and proactive strategies have been discussed in accounting and information systems research (Riney, 2018; Taherdoost, 2021), there is limited empirical evidence on how insurance companies integrate multiple strategies—including preventive, curative, and deterrence measures—into a cohesive fraud management framework.

To address this gap, this study adopts a qualitative research was conducted across three leading Indian insurance companies. Data was analyzed using Dynamic Capability (DC) theory (Teece, 1997; Eisenhardt & Martin, 2000; Winter, 2003; Teece, 2007; Wang & Ahmed, 2007). The findings reveal that companies employ a multi-layered fraud management framework structured around five interlinked strategies: reactive, proactive, preventive, curative, and deterrence. Collectively, these approaches strengthen operational resilience, reduce losses, and enhance stakeholder trust and compliance.

The paper is structured as follows: Section 2 reviews the theoretical underpinnings of fraud models and strategies, including the Fraud Triangle, Diamond, and Pentagon. Section 3 outlines the legal and regulatory context for fraud control in the Indian insurance sector. Section 4 describes the research methodology and case study design. Section 5 presents the findings, highlighting the interplay of dynamic capabilities with multi-layered fraud management strategies. Section 6 concludes with implications for theory, practice, and policy, as well as directions for future research.

2. Literature Review

The Fraud Triangle, developed by Cressey (1953), is a foundational model for understanding the causes of fraud. It identifies three key elements: pressure, opportunity, and rationalization. Pressure represents personal or organizational incentives, such as financial stress or performance targets; opportunity reflects weaknesses in internal controls or oversight; and rationalization involves the perpetrator justifying unethical behavior to themselves (Riney, 2018). The triangle emphasizes that fraud occurs when all three elements converge, making it a useful diagnostic and preventive tool.

The Fraud Diamond extends the triangle by adding a fourth element: capability. Wolfe and Hermanson (2004) argue that even with pressure, opportunity, and rationalization, fraud requires individuals with the skills, position, or authority to exploit weaknesses. Capability includes technical expertise, decision-making power, and the ability to manipulate records, converting opportunity into actual misconduct. The diamond thus enhances predictive power for detecting potential fraudsters by highlighting personal characteristics.

Further extension to the Fraud Pentagon incorporates a fifth factor: arrogance or ethical disregard. Arrogance reflects overconfidence, greed, and a sense of invincibility that can exacerbate fraud risk. While some scholars debate the necessity of expanding beyond the triangle or diamond (Dellaportas, 2013), the pentagon model underscores the role of personality traits and moral attitudes in perpetuating fraud, providing a more holistic understanding of underlying causes.

Reactive strategies focus on detecting fraud after it occurs. According to Riney (2018), these methods rely heavily on detection tools, audits, and forensic reviews once anomalies or losses are observed. While reactive strategies, such as analyzing deviations or irregular accounting entries, provide insights into fraud patterns, they are inherently costly and reputationally damaging because financial and operational harm has already occurred. Similarly, Taherdoost (2021) highlights that reactive measures in information systems, such as post-event audits and monitoring, help refine risk databases but do little to prevent immediate losses.

In contrast, proactive strategies aim at preventing fraud before it happens. Riney (2018) notes that embedding ethical practices, robust internal controls, and accountability systems can eliminate or minimize opportunities for fraud. Tools such as governance frameworks, ethical leadership, continuous risk assessments, and preventive audits create resilient organizational structures. Taherdoost (2021) adds that predictive analytics and information system controls reduce vulnerabilities by anticipating potential fraud, emphasizing the value of forward-looking measures over mere correction.

Preventive strategies focus on eliminating opportunities for fraud. Mangala and Kumari (2015) and Hooks et al. (1994) identify mechanisms such as red flags, strong internal controls, corporate governance, whistleblowing systems, forensic accounting, and zero-tolerance policies. Red flags act as early warning indicators of potential misconduct, while whistleblowing empowers employees to report suspicious activities safely. Integration with auditing standards (e.g., SAS 55, COSO Framework) ensures systematic oversight and organizational vigilance. Effective preventive strategies reduce vulnerabilities and embed an ethical culture across all levels.

Deterrence strategies aim to discourage fraudulent behavior through consequences and visibility. Strong enforcement, regulatory frameworks, and high-profile case studies serve as psychological and operational deterrents (Mangala & Kumari, 2015; Hooks et al., 1994). Anonymous reporting systems, top management commitment to ethical standards, and public disclosure of whistleblowing activities amplify perceived detection risk, discouraging misconduct. Deterrence complements preventive measures by reinforcing accountability and demonstrating the consequences of unethical actions.

Curative strategies address fraud that has already occurred, focusing on restitution, correction, and systemic improvement. Barger (2016) illustrates this with Medicare hospice fraud, where whistleblower actions under the federal False Claims Act led to prosecution, financial recovery, and stricter oversight. Curative measures go beyond punishment; they include structural reforms, enhanced monitoring, and institutional safeguards to prevent recurrence. Such strategies ensure accountability while repairing organizational systems and restoring trust, particularly in public-private partnerships and regulated sectors.

3. Legal Background of Strategies to Control Fraud in the Indian Insurance Sector

Fraud-related regulations highlight distinct approaches between developed markets and emerging economies like India. In developed countries such as the US and EU, reactive and deterrence strategies dominate through extraterritorial enforcement, high penalties, and stringent oversight. Laws like the FCPA (Foreign Corrupt Practices Act (United States, 1977)), UK Bribery Act, SOX (Sarbanes–Oxley Act (United States, 2002), and GDPR (General Data Protection Regulation (European Union, 2018) ensure multinational corporations maintain accurate records, prevent bribery, and protect whistleblowers, creating systemic safeguards against fraud. In contrast, India emphasizes a balanced mix of proactive, reactive, and deterrence strategies tailored to domestic institutional and technological contexts. While Indian laws—including the Companies Act (2013), Prevention of Corruption Act (2018), PMLA (Prevention of Money Laundering Act (India, 2002), and DPDP Act (Digital Personal Data Protection Act, India, 2023)—focus primarily on domestic enforcement, they gradually adopt international best practices to strengthen accountability. Indian regulators supplement these laws with proactive mechanisms such as anti-fraud cells, risk-based monitoring, and two-factor authentication in digital payments, demonstrating a preventive approach in areas where developed markets rely on complex, multi-jurisdictional frameworks.

Reactive strategies in India allow insurers to respond swiftly to fraud incidents through legal enforcement and investigations. The Companies Act, 2013, particularly Sections 177 and 447, empowers regulators like the Serious Fraud Investigation Office (SFIO) to prosecute executives for corporate fraud and establish internal reporting mechanisms. The Prevention of Corruption Act (2018) expands corporate liability and criminalizes bribery, enabling insurers to take legal action against internal malpractices and agent-related corruption. Case examples, such as the IL&FS financial scandal (2018), illustrate how reactive measures enabled the detection, prosecution, and recovery of misappropriated funds, reinforcing corporate accountability.

Proactive strategies focus on preventing fraud before it occurs. The Insurance Regulatory and Development Authority of India (IRDAI) Fraud Risk Management Guidelines (2018) require insurers to conduct structured fraud risk assessments, establish dedicated anti-fraud cells, and employ data analytics for early detection of fraudulent claims and premium diversion. RBI Know Your Customer / Anti-Money Laundering (KYC/AML) Directions (2016/2021) and the Prevention of Money Laundering Act (2002/2019) ensure preventive monitoring through Aadhaar-based e-KYC, suspicious transaction reporting, and transaction analysis, mitigating potential financial irregularities. Similarly, the Digital Personal Data Protection (DPDP) Act (2023) enables insurers to maintain anonymized fraud blacklists, protecting consumer data while enhancing early detection of repeat offenders. These proactive frameworks complement reactive enforcement, creating a dual layer of protection.

Deterrence strategies create a disincentive for fraudulent behavior through legal penalties, reporting obligations, and governance mandates. Whistleblower protection under the Whistleblower Protection Act (2011/2014) encourages internal reporting without fear of retaliation, fostering a culture of vigilance. The PCA, Companies Act provisions, and RBI/PMLA directives collectively reinforce the consequences of fraudulent conduct, deterring internal and external actors from exploiting loopholes. Industry-wide monitoring by Insurance Regulatory and Development Authority of India (IRDAI), combined with mandatory reporting of fraud incidents and escalations, further strengthens deterrence by making violations visible and actionable.

Other integrated strategies combine reactive, proactive, and deterrence elements to enhance overall resilience. Practical examples such as digital wallet compliance by Paytm and PhonePe demonstrate how regulatory frameworks—RBI Know Your Customer / Anti-Money Laundering (KYC/AML), Digital Personal Data Protection (DPDP) Act, and Insurance Regulatory and Development Authority of India (IRDAI) circulars—work in tandem to detect, prevent, and penalize fraud in real time. Together, these measures create a multi-layered regulatory environment that empowers Indian insurers to prevent, detect, and respond to fraud, thereby enhancing transparency, accountability, and financial stability in an emerging market context.

4. Methodology

This study adopts a qualitative, multi-method research design to investigate how Indian insurance firms manage fraud risks in emerging markets. The choice of a qualitative approach reflects the exploratory nature of fraud control research, where institutional forces, regulatory pressures, and technological adaptations interact in complex and evolving ways (Derrig, 2002; Langley, 1999; Yin, 2014). By combining interviews, case study analysis, and secondary document review, the methodology ensures both depth and triangulation, enhancing the credibility and transferability of findings (Creswell and Poth, 2007, 2018).

India's insurance sector provides an appropriate setting, given its rapid liberalization following the establishment of the Insurance Regulatory and Development Authority of India (IRDAI) in 1999. The sector now comprises 57 insurers, and fraud remains a critical concern as firms expand digital channels and customer bases. Emerging markets like India exemplify environments where coercive, mimetic, and normative institutional pressures shape organizational responses to fraud (DiMaggio and Powell, 1983). Focusing on this setting allows examination of both global best practices and locally adapted innovations in fraud management.

Data was collected from three Companies named Company A, Company B, and Company C. Company A and Company B are prominent general insurance providers in India, established in 2001 with joint venture partners from Europe and the USA/Canada. Both companies have revenue of over $ 3 billion and over 15000 employees. The company's offerings encompass a wide range of insurance products, including motor, health, travel, home, and business insurance. In contrast, Company C is a prominent life insurance provider in India established in 2001 with a joint venture partner from Asia, with revenue of over $1 billion and over 10,000 employees. Data were coded iteratively, combining Dynamic Capability constructs with emergent themes from interviews and cases. Following Eisenhardt (1989), the analysis sought to identify causal mechanisms linking institutional pressures to organizational fraud governance responses.

Given the sensitive nature of fraud research, strict confidentiality protocols were observed. Company names were anonymized where required, and respondent identities were protected. Importantly, no external funding—including from case companies—was accepted, to ensure neutrality in research design and interpretation (Yin, 2014). This independence strengthens the credibility of findings in a field where proximity to organizations may risk interpretive bias.

5. Theoretical Framework: Dynamic Capabilities

Dynamic capabilities (DC) provide a robust theoretical lens for understanding how firms sustain competitive advantage in turbulent environments. Teece (1997) conceptualized DCs as a firm's ability to integrate, build, and reconfigure internal and external competencies to adapt to rapid change. Eisenhardt and Martin (2000) expanded this view by showing how capabilities differ in stable versus uncertain environments, highlighting their iterative and flexible role under unpredictability. Winter (2003) further differentiated dynamic from operational capabilities, suggesting that adaptability originates from processes of learning and innovation rather than routine execution.

Despite rich theorization, the practical application of dynamic capabilities in specialized areas such as fraud control remains underexplored (Teece, 2007; Wang & Ahmed, 2007; Agarwal, 2025b), emphasizing absorptive, adaptive, and innovative capacities as core to dynamic capability. Yet, how these capacities interact with real-time digital threats—such as phishing or identity fraud—remains unclear. For example, a bank confronted with a phishing attempt must absorb the external signal, adapt its systems in real time, and innovate preventive mechanisms to counter evolving risks.

Absorptive capacity is the firm's ability to recognize, assimilate, and apply external knowledge. It enables organizations to learn from outside signals—such as competitor practices, regulatory changes, or customer behavior—and convert that knowledge into actionable insights. In fraud control, this could mean scanning external fraud databases, monitoring phishing attempts in other markets, or leveraging regulatory advisories to strengthen internal fraud detection systems.

Adaptive capacity reflects the firm's ability to reconfigure internal processes and resources in response to environmental changes. It is the agility to adjust strategies, structures, and systems when confronted with new threats or opportunities. In fraud management, adaptive capacity might be seen in how an insurer quickly modifies claim verification rules after detecting a surge in fabricated hospital bills, or how a bank recalibrates its risk models in response to new patterns of cyber fraud.

Innovative capacity is the firm's ability to develop new products, services, or processes by recombining resources creatively. This goes beyond reacting to change—it involves shaping the environment through novel solutions. In fraud governance, this could mean creating an AI-driven fraud detection system, launching a mobile self-survey app for vehicle insurance, or collaborating across the industry to design blockchain-based claim verification platforms.

6. Findings

The study reveals that all insurance companies employ a multi-layered fraud management framework built around five interlinked strategies—reactive, proactive, preventive, curative, and deterrence. Reactive strategies ensure timely investigation and resolution once fraud is reported, while proactive strategies use data analysis, risk triggers, and field investigations to detect vulnerabilities early. Proactive strategies emphasize early detection by using data analytics, suspicious triggers, and field investigations to identify and neutralize fraud risks before they escalate. Preventive strategies strengthen onboarding, enforce due diligence, and deploy technology to block fraud opportunities before they occur. Curative strategies, in contrast, rectify systemic weaknesses that have already caused financial or reputational harm, redesigning processes to prevent recurrence. Finally, deterrence strategies focus on sanctions, regulatory escalation, and industry-wide collaboration to ensure long-term accountability and reputational consequences for fraudsters. Together, these strategies not only reduced fraud-related losses but also **e**nhanced trust, compliance, and competitive advantage across the insurance sector.

6.1 Reactive Strategies

Reactive approaches remain central to fraud governance, where insurers detect irregularities only after suspicious claims are reported or audited.

Chief Risk Officer of Company A discussed that the company did not like to follow reactive strategies, as it is post-mortem rather than pre-mortem.

"*In motor claims, we hate to discover fraud during post-payment audits. Matching engine numbers and vehicle images at settlement has exposed several falsified claims at the early stage of risk management."*

Company A officials found that reactive strategies are part of compliance and pressure from the top, rather than deriving any advantage for the company.

The audit team of Company B reviewed documents on a regular basis. Every audit follows some procedures for validation. Regarding the claims department, a few checks and balances are maintained related to receiving the premium for the claim, the validity of the vehicle, and the validity of the owner's driving license. Some comparisons are also made, such as the vehicle picture at the time of taking insurance should match the vehicle picture at the time of the claim, the identity of the insured should match the claimant's identity in the claim file, and the engine and chassis number of the motor vehicle should match at the policy issuance and claim payment stages. Even though claims departments follow underwriting guidelines, companies carry out independent audits by using several tools, such as digital image mapping. If any of these parameters are mismatched, a trigger is highlighted for fraud after payment of the claim.

Fraud is often reported through five channels: email, hotlines, whistle-blowers, claims, and the internal audit team. After receiving a red flag, the Fraud Control team appoints an investigator. The company has hired several investigators based on their expertise and availability at different locations. Investigators investigate, collect evidence, and submit a report to the management. In general, an investigator is paid fixed fees for regular claims, while for high-value claims, the experienced and expert investigator's fee may reach a significantly higher level.

The investigation is carried out in three steps. First, the investigator reviews the files and reads the literature of existing reports, pictures, and case histories. Second, a physical investigation is carried out, which is followed by a report submission with evidence and recommendations in the final step.

After completing a close file review, an investigator develops notes for differences in the insured vehicle photo at the garage and at the time of insurance. The pre-diagnosis showcases the possibility of fraud. The investigation team then met with the employees of the garage. In the garage, the record register shows no evidence of the insured's vehicle repair on the mentioned date. A Statement was collected from the garage owner, and a copy of the garage record register was taken as evidence. A formal investigation report containing all facts was prepared and submitted for action by the surveyor and the owner of the insured vehicle. The Fraud Control Department received a total of 3247 suspected fraud cases related to eight departments in 2021. Finally, 1299 fraud cases were detected with evidence by the Investigation team.

The assessment revealed that the motor and health line of business is facing maximum fraud so far. A post-fraud assessment report based on evidence collected is prepared to report to auditors, regulators, and senior management. Some examples from the findings are: Driver swapping, fabricated documents, and damage before insurance in Motor claims were the main reasons for rising fraud. Pre-existing illness, patient impersonation, and Fabrication of claim documents were the major causes of Health Fraud.

To deal with these problems, an investigator is deputed to ensure the genuineness of the claims documents and information provided at the time of claims reporting, whether the patient admitted to the hospital is someone who is insured, etc. Reactive strategies are supported in improving losses in the company and preventing fraudulent claims from payment, but they offer no competitive advantage.

Company C rather truly believed in reactive strategies. The CRO of the company mentioned:

"A significant portion of our life insurance portfolio is concentrated in ULIPs, with higher commissions incentivizing agents. This has led to multiple policies being sold to the same customer, often without a clear understanding of their actual financial needs. Our approach often reacts to issues after they arise rather than anticipating them, addressing risks only when customer complaints or compliance flags emerge."

Company C did not find that controlling fraud can result in any type of competitive advantage.

6.2 Proactive Strategies

Proactive strategies focus on anticipating fraud risks before they materialize, using foresight, technology, and systemic collaboration to strengthen resilience. Unlike reactive approaches that address fraud after it occurs, proactive measures emphasize early warning systems, predictive analytics, and innovative practices that minimize vulnerabilities. These strategies often involve building industry alliances, embedding technological solutions, and reallocating investigative resources based on risk signals. By moving from compliance-driven responses to forward-looking risk anticipation, companies not only mitigate potential fraud but also secure competitive advantage through efficiency, trust, and leadership in fraud governance.

In Company A, proactive strategies extended beyond routine compliance to industry-level initiatives. By anticipating fraud risks and collaborating with regulators, councils, and international partners, the company sought to strengthen systemic resilience while differentiating itself from competitors.

"By collaborating with regulatory bodies and industry councils, we proactively shaped fraud governance beyond compliance. Initiatives such as embedding QR codes in motor policies, developing certification programs for fraud investigators, and building a shared database with global partners allowed us to sense emerging risks, seize opportunities to strengthen industry-wide

resilience, and reconfigure our internal systems. This proactive stance not only mitigated fraud but also positioned us with a clear competitive edge in trust, credibility, and market leadership."

Company B demonstrated agility in proactive risk management by leveraging technology during external disruptions. The shift to digital tools for fraud checks during the pandemic showcased its ability to sense risks, seize available resources, and reconfigure traditional processes. This approach not only ensured business continuity but also reduced operational costs.

"During COVID, we launched virtual fraud checks through video calls and social media reviews. It ensured continuity when field investigations were not possible."

By adopting virtual fraud detection, the company reduced investigation costs, minimized claim settlement delays, and achieved a competitive advantage by curbing losses while maintaining customer trust.

Company C applied a proactive lens by tracking geographic patterns of fraud emergence. Through hotspot mapping, it anticipated fraud-prone areas and pre-empted collusive fraud rings before claims reached the payment stage. This strategic foresight helped the company to restructure its investigative focus and optimize resource allocation.

"Fraud cases kept emerging from the same districts in one state of the country. Mapping these hotspots allowed us to pre-empt fraud rings before claims were processed."

Such measures not only reduced the financial burden of fraudulent payouts but also lowered the cost of investigations, thereby offering a competitive edge through both efficiency and stronger fraud control.

6.3 Curative Strategies

Curative strategies are designed to rectify systemic weaknesses that have already caused harm, such as financial losses, policy lapses, or reputational setbacks. Unlike preventive or proactive approaches that anticipate risks, curative measures focus on damage control—addressing existing loopholes, correcting operational inefficiencies, and restoring stakeholder trust. These strategies often involve targeted reforms, process redesigns, and stricter enforcement mechanisms to ensure that past mistakes do not recur.

For Company A, curative strategies became critical once systemic weaknesses in policy cancellations surfaced. Fraudulent misuse of temporary receipts by agents had already caused large-scale cancellations and financial damage. The company sensed the loophole through root cause analysis, seized the opportunity to redesign controls, and reconfigured policy issuance processes.

"We discovered agents were misusing temporary receipts, leading to large-scale policy cancellations. Auto-cancellation after eight days helped us close the loophole."

These measures helped bring cancellations under control, reduce diversion-related losses, and improve governance over agents, thereby strengthening competitive advantage by restoring financial discipline and market trust.

Company B faced widespread premium diversion that eroded profitability, requiring strong curative measures. The Fraud Control team realized that detection alone was insufficient and treated the issue like a systemic disease. By diagnosing the scale of the problem and implementing reforms to eliminate fraudulent policy cancellations, the company sensed deep-rooted weaknesses, seized corrective reforms, and reconfigured its internal processes to improve oversight.

"Premium diversion was hurting our bottom line. Curative reforms were essential—we had to treat the issue like a disease after it spread."

This approach reduced losses, restored premium flows, and lowered the long-term costs of fraud investigation, allowing the company to regain operational efficiency and customer trust.

Company C encountered unusually high policy cancellations—12%, well above the industry average—driven by gaps in agent-level monitoring and weak KYC verification. By tightening checks at the agent level, improving KYC validation, and advocating for systemic reforms like mandatory digital death records, the company sensed underlying control failures, seized corrective actions, and reconfigured fraud governance practices.

"Policy cancellations rose to 12%, far above the industry average. Strengthening agent-level checks brought cancellations back under control."

These measures curtailed policy lapses, reduced revenue leakages, and ensured compliance, providing a competitive advantage through improved service turnaround time, reduced mismanagement, and cost savings in fraud handling.

4. Preventive Strategies

Preventive strategies are designed to stop fraud before it occurs by blocking opportunities through stricter due diligence, robust data validation, and technology-driven controls**.** Unlike curative approaches that repair damage after the fact, preventive measures focus on early detection, deterrence, and building systemic safeguards**.** These strategies often involve pruning out high-risk intermediaries, tightening onboarding processes, verifying customer and asset details against official databases, and using digital tools for real-time risk assessment.

For Company A, preventive strategies became central to reducing small-ticket fraud in motor insurance. Rising numbers of pre-existing damage claims from remote regions revealed weaknesses in traditional verification processes. Physical surveys were often impractical and costly, leading to fraudulent claims slipping through. By sensing this gap, the company introduced a mobile self-survey app that enabled customers to record vehicle conditions at the time of issuance. The firm seized technology as a control tool and reconfigured fraud prevention through digital innovation.

"Our self-survey mobile app allows policyholders to record vehicle condition at issuance. This reduced small-ticket motor fraud significantly."

This initiative reduced fraudulent claims, streamlined investigations, and earned recognition through an Innovation and Emerging Technology Award, while enhancing customer experience and lowering operational costs.

By leveraging a self-survey mobile app, the company gained a competitive edge through lower investigation costs, faster policy issuance, and improved customer satisfaction.

Company B faced increasing fraud from misrepresentation in online sales—particularly where two-wheeler premiums were collected for commercial four-wheelers. These practices caused losses in the millions and highlighted a major verification gap. The company sensed the systemic risk, seized regulatory alignment, and reconfigured processes by mandating cross-verification of vehicle details with the Transport Authority database.

"We now verify every vehicle registration number with the Transport Authority database. It eliminated thousands of fraudulent motor policies."

This approach eliminated fraudulent policies at the source, safeguarded premium flows, and improved trust in digital sales channels, strengthening both governance and competitive positioning.

Through mandatory vehicle verification with the Transport Authority database, the company strengthened digital sales integrity, reducing fraud losses and enhancing trust in its online channels.

Company C identified agents and hospitals as recurring nodes of fraud, responsible for premium diversion, bogus documentation, and inflated claims. Although blacklisting repeat offenders reduced exposure, the company realized the need to prevent re-entry of fraudulent actors. It sensed the limitation of reactive blacklisting, seized the opportunity to redesign controls, and reconfigured onboarding through mandatory due diligence checks. *"Blacklisting hospitals and agents is no longer enough. We introduced due diligence at onboarding to stop repeat offenders from re-entering the system."*

These measures pruned systemic vulnerabilities, reduced dependence on high-risk intermediaries, and strengthened compliance frameworks, giving the company a preventive edge in fraud management.

By embedding due diligence at onboarding, the company built stronger compliance frameworks, minimized reliance on risky intermediaries, and secured long-term operational resilience.

6.5 Deterrence Strategies

Deterrence strategies focus on sanctions, collaboration, and reputation costs to ensure that fraudsters face lasting consequences beyond immediate financial recovery. Unlike preventive or curative measures that address fraud within a company's boundaries, deterrence relies on industry-wide cooperation, regulatory enforcement, and legal action. By escalating proven cases, sharing blacklists, and collaborating with enforcement agencies, insurers not only reduce fraud but also send a clear message that fraudulent behavior will have long-term professional, financial, and reputational repercussions. These strategies significantly reduced losses, strengthened governance, and created a renewed image of credibility among stakeholders.

Company A used deterrence as a way to enforce accountability in the healthcare network. By escalating proven fraud cases to regulators, the company triggered license cancellations for repeat-offender doctors. This action not only removed persistent fraudsters but also created a ripple effect across the industry, discouraging others from similar practices.

"We escalated proven cases to regulators, leading to license cancellations for repeat-offender doctors. That had a ripple effect across the industry."

The company's firm stance reinforced trust with customers and partners, showing that fraudulent practices would face serious consequences backed by regulatory action.

Company B strengthened deterrence through collective industry collaboration. The Insurance Council's shared blacklist system ensured that once an agent was flagged for fraud, they were barred from working with any insurer in the industry. By supporting and adopting this framework, the company not only blocked repeat offenders but also signaled a zero-tolerance approach to fraudulent behavior.

"The Insurance Council's shared blacklist has transformed deterrence. Once flagged, an agent cannot work with any insurer."

This initiative helped reduce systemic risks, enhanced transparency, and built customer confidence by showing that fraud was not just managed but actively eradicated through collective measures.

Company C confronted the challenge of collusion fraud, where fraudulent activities often spanned across multiple insurers. Recognizing that individual company efforts were insufficient, it spearheaded industry-wide collaboration by organizing a Chief Risk Officer (CRO) Forum for data sharing and joint deterrence measures.

"For collusion fraud, industry-wide data sharing is the only solution. Collaborative deterrence is stronger than individual company action. We are organizing the Chief Risk Officer Forum."

By promoting collaboration across companies and regulators, the firm reinforced a culture of shared responsibility, significantly reducing losses and enhancing its reputation as an industry leader in fraud governance.

7. Discussion

The findings revealed that all companies, Company A, Company B, and Company C, relied on all three types of capacities: absorptive, innovative, and adaptive.

For Company A, reactive strategies such as blacklisting fraudulent agents showcased absorptive capacity, as the firm learned from past losses and integrated external signals of misconduct into its internal governance. Its preventive strategies, such as due diligence during agent hiring and vehicle verification via government databases, highlighted adaptive capacity by reconfiguring operational routines to block future risks. Moving further, proactive initiatives like collaborating with regulators and embedding QR codes in motor policies demonstrated innovative capacity, as the company went beyond firm boundaries to shape systemic fraud governance. Similarly, its curative measures of redesigning policy issuance processes after temporary receipt misuse reflected adaptive learning from systemic weaknesses. Finally, deterrence strategies, including escalation to regulators for license cancellation, reinforced both absorptive and innovative capacities by leveraging external institutions to strengthen long-term fraud deterrence.

Company B's reactive strategies were anchored in absorptive capacity, as the firm identified the scope of premium diversion through internal audits and investigations, enabling it to sense systemic weaknesses. Its preventive measures, such as reinforcing oversight and reducing loopholes in policy cancellations, signaled adaptive capacity, since these changes required redesigning workflows under pressing conditions. During the pandemic, proactive virtual fraud detection tools highlighted innovative capacity, as the firm experimented with digital solutions to maintain continuity while cutting costs. In terms of curative reforms, the company's framing of fraud as a "disease" reflected deep absorptive learning and adaptive restructuring to manage systemic risks. Lastly, its adoption of the Insurance Council's shared blacklist for deterrence underscored innovative capacity, demonstrating how collaborative deterrence reconfigured industry practices beyond the organizational boundary.

Company C's reactive response to unusually high policy cancellations was rooted in absorptive capacity, as it internalized insights from cancellation trends to diagnose the root cause—weak KYC and agent monitoring. Its preventive measures, like stricter onboarding and self-recording apps for vehicles, reflected adaptive capacity, enabling the company to realign operational processes with fraud control objectives. On the proactive front, fraud hotspot mapping illustrated absorptive and adaptive capabilities, allowing the firm to anticipate emerging fraud rings and redirect investigative resources. In terms of curative actions, Company C's effort to restore trust by improving KYC and lobbying for systemic reforms demonstrated adaptive and innovative capacity. Finally, its deterrence strategy of organizing CRO forums exemplified innovative capacity, as it sought to co-create an industry-wide governance mechanism that extended deterrence beyond company boundaries.

8. Conclusion

This study set out to address the research question: How do insurance firms in emerging market create new capacities to control fraud? By examining reactive, preventive, curative, proactive, and deterrence strategies across three firms, the research provides insights into how organizations sense, seize, and transform their fraud management practices in response to complex and evolving risks.

The findings suggest that firms consistently combine absorptive, adaptive, and innovative capacities to shape their fraud control frameworks. For instance, reactive measures rely heavily on absorptive capacity, preventive and curative actions highlight adaptive reconfiguration, and proactive as well as deterrence strategies often showcase innovative capacity through systemic or industry-wide interventions. However, what remains less understood is the temporal sequencing of these strategies—whether firms deploy them in a linear progression (from reactive to deterrence) or in overlapping cycles depending on contextual triggers. Moreover, while the micro-foundations of sensing, seizing, and transforming are evident, the measurement of their effectiveness in financial and reputational terms is still underexplored.

Theoretically, this study extends the dynamic capabilities literature by linking absorptive, adaptive, and innovative capacities directly to fraud control in financial services—a context often overlooked in capability scholarship, which tends to emphasize innovation and competitive positioning rather than risk governance. By mapping five distinct fraud strategies onto the DC framework, this research highlights how resilience is not only about innovation but also about learning from past failures, adapting operational systems, and engaging in collaborative deterrence. It therefore positions fraud management as a fertile domain for advancing organizational theory.

For practitioners, the study underscores that fraud control cannot be managed as isolated compliance exercises. Instead, firms should cultivate capability portfolios: absorptive capacity to learn from past fraud, adaptive capacity to redesign operational processes, and innovative capacity to anticipate and pre-empt emerging risks. Collaboration with regulators, councils, and industry peers emerges as a practical necessity for deterrence, while digital tools such as self-survey apps and virtual fraud checks demonstrate cost-efficient ways to manage fraud in high-volume, low-margin contexts.

At the theoretical level, the study demonstrates that dynamic capabilities are not confined to innovation-driven markets but are equally relevant to high-risk, regulated sectors. By illustrating how fraud control is a dynamic, capability-driven process, the research broadens the scope of DC theory to include risk governance and compliance. The mapping of five fraud strategies to three capacities provides a structured framework for future comparative studies in financial services and beyond.

References

1. Abbas Taherdoost, A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection, 10 Electronics 3065 (2021).
2. Ann Langley, Strategies for Theorizing from Process Data, 24 Acad. Mgmt. Rev. 691 (1999).
3. Deepa Mangala & Pooja Kumari, Corporate Fraud Prevention and Detection: Revisiting the Literature, 4 J. Com. & Acct. Rsch. 35 (2015).
4. David J. Teece, Dynamic Capabilities and Strategic Management, 18 Strategic Mgmt. J. 509 (1997).
5. David J. Teece, Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance, 28 Strategic Mgmt. J. 1319 (2007).
6. David T. Wolfe & Dana R. Hermanson, The Fraud Diamond: Considering the Four Elements of Fraud, 74 CPA J. 38 (2004).
7. Donald R. Cressey, The Criminal Violation of Financial Trust, 5 Am. Soc. Rev. 742 (1950).
8. Donald R. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement* (1953).
9. F.A. Riney, Two-Step Fraud Defense System: Prevention and Detection, 29 J. Corp. Acct. & Fin. 74 (2018).
10. Gary P. Wang & Shujun Ahmed, Dynamic Capabilities: A Review and Research Agenda, 29 Int'l J. Mgmt. Rev. 35 (2007).
11. J.F. Barger, Jr., Life, Death, and Medicare Fraud: The Corruption of Hospice and What the Private Public Partnership under the Federal False Claims Act Is Doing About It, 53 Am. Crim. L. Rev. 1 (2016).
12. Jan Viaene, Rudi Dedene & Bart Baesens, A Data Mining Application for Claim Fraud Detection in the Belgian Social Security, 34 Decision Support Sys. 1 (2007).
13. John W. Creswell & Cheryl N. Poth, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (3d ed. 2007).
14. John W. Creswell & Cheryl N. Poth, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed. 2018).
15. Joseph W. Marks, Expanding the Fraud Triangle: The Fraud Pentagon, 2 Acct. & Fin. Rsch. 15 (2009).
16. Karen L. Hooks, Steven E. Kaplan & Joseph J. Schultz, Jr., Enhancing Communication to Assist in Fraud Prevention and Detection, 13 Auditing: J. Prac. & Theory 86 (1994).
17. Kathleen M. Eisenhardt, Building Theories from Case Study Research, 14 Acad. Mgmt. Rev. 532 (1989).
18. Kathleen M. Eisenhardt & Jeffrey A. Martin, Dynamic Capabilities: What Are They?, 21 Strategic Mgmt. J. 1105 (2000).
19. Paul J. DiMaggio & Walter W. Powell, The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields, 48 Am. Soc. Rev. 147 (1983).

20. Richard A. Derrig, Insurance Fraud, 69 J. Risk & Ins. 271 (2002).
21. Robert K. Yin, *Case Study Research and Applications: Design and Methods* (6th ed. 2014).
22. Ruchi Agarwal & Sanjay Kallapur, Cognitive Risk Culture and Advanced Roles of Actors in Risk Governance: A Case Study, 19 J. Risk Fin. 327 (2018).
23. Ruchi Agarwal, Sanjay Kallapur & Sanjiv Dwivedi, Leveraging Digital Technologies to Control Fraud in a Resource-Constrained Institutional Environment: A Longitudinal Case Study, J. Acct. & Org. Change (2025).
24. Ruchi Agarwal, From Compliance to Culture: Organizational Communication as a Tool to Foster Effective Fraud Risk Management in Insurance Industry, 33 Int'l Ins. L. Rev. S4 (2025).
25. Ruchi Agarwal, Hybridization of Risk Cultures and Enterprise Risk Management in Insurance Sector, 33 Int'l Ins. L. Rev. S4 (2025).
26. Sidney G. Winter, Understanding Dynamic Capabilities, 24 Strategic Mgmt. J. 991 (2003).
27. Stanley White, Internal Auditing and the Three Lines of Defense Model, 12 Int'l J. Auditing 71 (1995).
28. Stavros Dellaportas, Corporate Fraud Prevention: The Fraud Triangle and Beyond, 20 J. Fin. Crime 287 (2013).
29. Steven L. Hillison, William S. Pacini & Michael R. Sinason, The Internal Auditor as Fraud-Buster, 14 Managerial Auditing J. 351 (1999). Institutional Authors (placed alphabetically after individual authors):
30. Comptroller & Auditor Gen. of India, *Reports on the Insurance Sector* (2006-07–2023-24).
31. Fin. Intelligence Unit–India, *Annual Reports* (2006-07–2023-24).
32. Ins. Regulatory & Dev. Auth. Of India, *Regulations, Circulars, and Guidelines* (1999–2023).
33. Sec. & Exch. Bd. Of India, *Orders and Regulations on Fraudulent and Unfair Trade Practices* (2003–2023).

Received: 27 Sep 2025 | Accepted: 10 Oct 2025 | Published: 23 Oct 2025