WHITE PAPER

HARNESSING THE POWER OF ARTIFICIAL INTELLIGENCE IN FRAUD DETECTION

A Proactive Approach to Insurance Fraud Prevention and Detection

Abstract

Insurance fraud detection is an area that needs focus and investment in terms of finance and technology. This is important to prevent the rising financial burden on insurance companies and their customers. Fraudulent activities cost the industry billions of dollars leading to higher premiums for policyholders in addition to financial and reputational costs for insurers.

This white paper explores the current scenario and the use of artificial intelligence for detection and prevention of insurance fraud. It further highlights the capabilities of some leading technology solutions available and explains why insurance companies must adopt the power of AI for fraud prevention and control.

Infosys®
Navigate your next

CONTENTS

INTRODUCTION

Insurance fraud is a massive problem that plagues the insurance industry worldwide. Every carrier must constantly be on guard against fraudsters trying to game the system and subvert the claims process. It is now critical for insurers to find and stop fraud by such mala fide elements among their customers and in the claims process.

In the current technology landscape where digital transactions and interactions have become the norm, there has been a sharp rise in cases of insurance-related fraud. From financial institutions to e-commerce platforms, organizations struggle to keep pace with the ever-evolving tactics swindlers employ. Natural disasters and epidemics are perfect settings for fraudsters to pursue high-volume claims. Every year, policyholders and insurance companies suffer tremendous losses due to false claims.

New tools are being developed to help fight fraud, but insurance companies and other industry stakeholders need to be open to change. Simply reacting after fraud occurs is no longer enough – the goal must be to implement predictive solutions that can sniff out suspicious behavior proactively. Through a combination of insurer education, deploying the right tools, and innovative fraud detection solutions, insurers can stay ahead of these threats.

By adopting the latest fraud-fighting technologies and supporting programs to educate people about fraud, insurers can play a crucial role in preventing insurance fraud.

INSURANCE FRAUD NEWS

The following news items drive home the need for urgent technology-aided steps to prevent and control fraud in the insurance industry.

1 Insurance fraud surges: AI to the rescue

Insurance fraud costs consumers in America at least US $80 billion (about US $250 per person) every year, according to The Coalition Against Insurance Fraud (CAIF). CAIF also estimates that workers' compensation insurance fraud alone costs insurers and employers US $30 billion (about US $92 per person) a year. The FBI reports that non-health insurance part of the overall problem amounts to US $40 billion (about US $120 per person) annually. Ultimately, the massive scope of the problem can mean the average American family will pay an extra US $400 and US $700 per year in premiums.

READ MORE

2 Teradata and FICO Partner to Reduce Fraud, Improve Business Outcomes

Teradata, a connected multi-cloud data platform company, and FICO, a leading global analytics software provider, announced the plan to bring to market integrated advanced analytic solutions for real-time payments fraud, insurance claims, and supply chain optimization.

READ MORE

3 Arkansas Supreme Court rules state agency must provide information relating to algorithms implemented

On June 9th, 2022, the Arkansas Supreme Court issued a decision ordering the Arkansas Division of Workforce Services to provide information relating to an algorithm it implemented during the pandemic to process unemployment claims. Legal Aid of Arkansas learned that the agency implemented an algorithm leading to thousands of claims being wrongfully flagged, leading to delays from six months to over one year for benefits.

READ MORE

TYPES OF INSURANCE FRAUD

Insurance fraud covers a wide range of deceptive acts, from harmless overstatements to elaborate illegal schemes purposely designed to cheat unsuspecting victims. Common fraudulent activities in the insurance industry include:

Staged auto accidents

Dishonest persons or groups stage motor vehicle collisions to exploit innocent drivers and wrongfully obtain insurance payouts. The scammers cause intentional accidents, then file exaggerated bodily injury claims and falsified property damage reports against the lawful drivers' policies. Beyond the monetary losses for insurers, staged accidents create tremendous stress, delays, and expenses for the parties affected.

Exaggerated claims

Insured individuals sometimes pad their legitimate claims to recover funds above what was actually lost. This padding ranges from slightly embellished descriptions of damaged goods to entirely fictional events. Such exaggerated claims impose unnecessary expenses upon insurers and contribute to rate increases for honest policyholders.

Workers' compensation schemes

Companies occasionally misrepresent employee statuses or job duties to avoid paying appropriate premiums, putting both injured workers and honest firms at a disadvantage. In extreme cases, workers may fabricate incidents involving nonexistent injuries or even fatalities to collect undue settlements.

Premium diversion

Premium diversion occurs when insurance agents misrepresent premium payments meant for insurance companies. Instead of sending the money to the insurer so that people and businesses are covered in case of accidents or disasters, corrupt agents keep the cash for themselves. This leaves policyholders exposed and helpless if something goes wrong because they do not have proper insurance coverage. Widespread premium diversion causes distrust among consumers and instability in the insurance market since it harms the reputation of insurers.

Ghost brokers

Illicit operators sell counterfeit insurance certificates online, targeting consumers seeking affordable coverage options. Ghost brokers secure fake documents bearing stolen logos and credentials belonging to reputable carriers. Victims discover too late that their policies offer no real protection if catastrophe strikes.

Fraudsters are infinitely creative in finding new ways to cheat the system and trick insurance companies out of money.

As soon as insurers crack down on one kind of scam, the dishonest perpetrators modify their tactics or devise new fraud strategies. Relying on traditional investigation methods is no longer enough. Insurers must implement advanced technology-based fraud detection systems that can identify suspicious behaviors and emerging threat patterns before the money goes out the door.

IMPACT OF FRAUD ON INSURERS AND POLICYHOLDERS

The effects of insurance fraud ripple throughout the ecosystem, adversely impacting all participants connected to the chain of commerce.

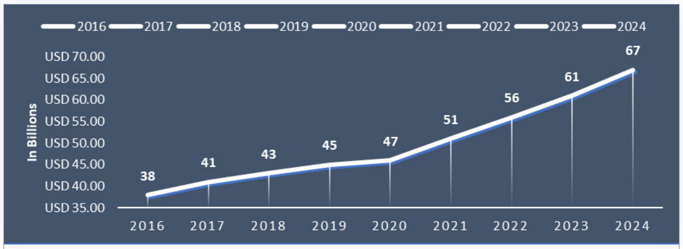
Specifically, insurers and policyholders face negative consequences such as weakened finances or stability and compromised integrity. For insurers, the immediate impact manifests in terms of monetary losses arising from erroneous claim payments, administrative overheads related to fraud investigation and prosecution, legal fees defending against civil litigation, and artificially inflated claim reserves. Over time, persistent fraud worsens the pressure on pricing models, compelling actuaries to increase premiums to offset mounting losses. Furthermore, widespread dishonesty threatens insurer solvency, jeopardizes investor confidence, and raises concerns regarding long-term sustainability.

Fraudulent claims indirectly impact policyholders as well. Insurers absorb the expenses incurred due to fraudulent claims and pass this on to policyholders by increasing the insurance premiums. Similarly, decreasing levels of trust caused by rampant deception prompt stricter underwriting scrutiny, making it difficult for deserving candidates to obtain coverage. Finally, prolonged engagement with fraudulently inclined customers may lead to suboptimal outcomes following valid claims, as reputationally damaged insurers struggle to meet obligations amidst deteriorating capitalization.

KEY STATISTICS RELATED TO COST OF FRAUD AND SOFTWARE UTILIZATION

According to statistical data, the property and casualty (P&C) cost of fraud reached US $47 billion in 2020, and is projected to escalate significantly, reaching a whopping US $72 billion by the end of 2025.

Graph 1 illustrates an alarming upward trend, with the cost increasing year-on-year, rising from US $38 billion in 2016 to an estimated US $67 billion by 2024. This data emphasizes the need for insurance companies to adopt advanced fraud detection and prevention solutions to combat the issue and mitigate the enormous financial losses associated with fraudulent activities.



Graph 1 | P&C cost of fraud over the years

Fraud Prevention Status in Organizations

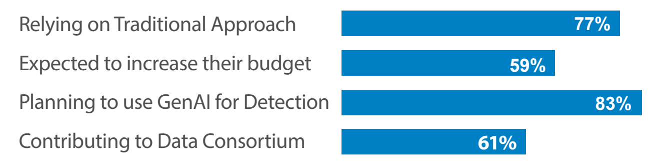


Figure 1 | Approach towards fraud prevention strategy across insurance organizations

The P&C cost of fraud data provides insights into the adoption and priorities of fraud prevention measures across insurance organizations as shown in Figure 1.

77%

of organizations are relying on a traditional approach.

59%

of organizations expect to increase their budget for fraud detection augmented by artificial intelligence (AI).

83%

of organizations are planning to use generative AI (GenAI) for detection purposes. A significant rise is expected in the adoption of GenAI augmented software, computer vision, robotics, and behavioral biometrics (over 50%) for anti-fraud efforts.

61%

of organizations are contributing to a data consortium for synergetic benefits of fraud data.

A significant portion of applications (5% to 6% of underwriting applications, mid-term adjustments or MTAs, and renewals) contain fraudulent elements. However, digital forensics/e-discovery software is used by 29% of organizations for fraud detection.

Cost Factors in Adopting AI Technology

Fraud detection measures, including the adoption of advanced technologies, skilled personnel, and comprehensive fraud detection solutions, require substantial financial investments. The high percentage of organizations facing budget limitations indicates the challenges faced in keeping up with the evolving fraud detection landscape and addressing potential vulnerabilities effectively.

Figure 2 illustrates the huge gap between insurers who have adopted modern technology versus traditional organizations constrained by budgets in the fight against fraud.

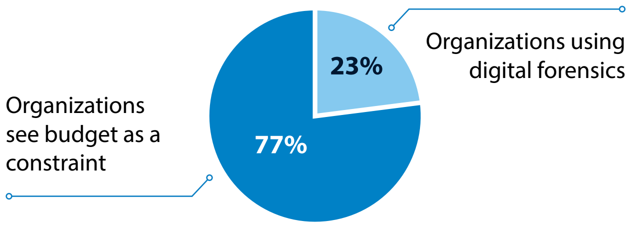


Figure 2 | Percentage of organizations using digital forensics for fraud detection

About 23% of organizations are already utilizing digital forensic tools and techniques. Digital forensics involves the acquisition, examination, and analysis of digital data to identify potential fraud, gather evidence for investigations, or uncover traces of fraudulent activities.

However, 77% of organizations consider budget constraints a significant factor influencing their fraud detection strategies and resource allocation.

While several insurers are leveraging digital forensic capabilities, a large majority (82%) are grappling with budgetary constraints that hinder their ability to implement robust detection measures. However, more than 50% of organizations plan to increase their anti-fraud budgets in the next two years. Today, it is a mix of organizations that utilize external solutions (35%), homegrown systems (28%), or no solution (28%).

Striking the right balance between investing in essential fraud detection tools and managing budgetary constraints remains a critical consideration for organizations striving to protect their digital assets and mitigate financial risks.

CURRENT APPROACHES IN FRAUD DETECTION

While some insurance companies are increasingly adopting advanced technologies to combat fraud, many still rely on traditional techniques that have been the backbone of fraud prevention for decades.

These methods involve human expertise, rules-based systems, and analysis of historical data patterns. Traditional fraud detection mechanisms include manual investigations by experienced claims adjusters, rules engines that flag claims meeting certain criteria, and statistical analysis that identifies suspicious trends over time. When implemented effectively alongside modern solutions, conventional methods provide insurers with multiple layers of protection.

Manual investigations

Experienced claims adjusters investigate suspected instances of fraud. The adjuster will gather evidence through interviews with policyholders, witnesses, medical providers, and others involved in the claim. They may also conduct site visits to inspect property damage or injury sites. If the adjuster identifies red flags, such as conflicting statements or missing documentation, they may launch a full investigation into the claim.

Rules-based systems

Rules-based systems automatically flag suspicious claims based on specific criteria. For example, a system might flag claims that contain inconsistent or contradictory information, exceed expected payout amounts, or come from areas or geographic regions with high rates of fraud. Rules-based systems can be tailored to individual lines of business, such as auto, health, life, or homeowners' insurance.

Historical data analysis

Historical data is used to identify common patterns associated with fraudulent claims. For example, an insurer might notice that certain types of claims such as workers' compensation tend to spike during particular seasons or months. Alternatively, an insurer might find that certain geographic regions have higher rates of fraud than others. By understanding these patterns, insurers can develop targeted strategies to prevent future fraud.

Statistical data analysis

Basic and custom algorithms are used to identify subtle indicators of fraud that might otherwise go unnoticed. For example, an algorithm might be able to detect anomalous billing patterns among healthcare providers or spot irregularities in policyholder demographics. By combining various data points, including policyholder characteristics, claim history, and industry benchmarks, insurers can create robust predictive models capable of identifying emerging fraud risks.

Data matching

Data matching techniques are used to cross-reference policyholder information against internal and external data consortium databases. For example, an insurer might check for duplicate policies issued under different names or verify address changes against public records. Additionally, insurers can screen applicants against watchlists maintained by regulatory agencies, law enforcement, or industry groups to prevent coverage for known fraudsters.

GAPS IN EXISTING APPROACHES

Traditional methods have several limitations that can be easily overcome using modern technologies.

Inability to detect real-time fraud

Time-consuming traditional methods face limitations in identifying external fraud and real-time fraudulent transactions.

Manual processes

Fraud detection methods used in the past are manual and therefore time-consuming, expensive, imprecise, and impractical.

Limited scalability

Traditional methods struggle to trawl through huge volumes of data leading to potential oversight of fraudulent activities. This was particularly prevalent during the COVID-19 pandemic when the claims volume was very high.

Inflexibility

Existing fraud detection methods rely on static rule-based systems that look for specific patterns of behavior. These systems cannot be changed easily to adapt to new types of fraud.

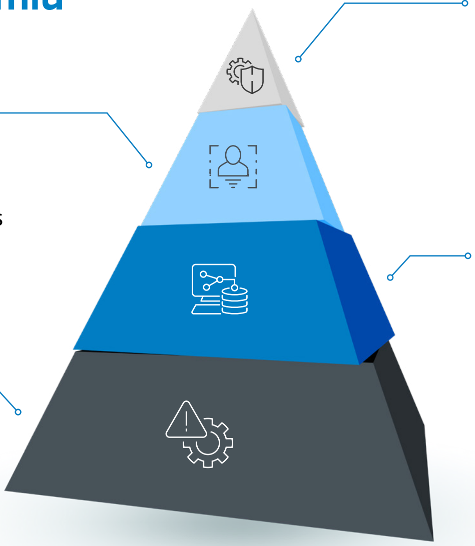
High false positives

Systems used in the past tend to generate a high number of false positives, which can be time-consuming and costly to investigate and clear.

GENERATIVE AI: A GAME CHANGER

Automation and the use of generative AI is a game changer for fraud detection in the insurance industry. GenAI provides prevention and control across several layers as shown in Figure 3.

GenAI Potential Pyramid



Proactive Fraud Prevention

Generative AI models can be designed to produce realistic scenarios of potential fraudulent claims, helping insurers anticipate and proactively identify emerging fraud schemes.

Deepfake Detection

As fraudsters leverage deepfakes to manipulate evidence, GenAI can be used to identify and flag inconsistencies in submitted documents, images, or videos.

Synthetic Data generation

Realistic but synthetic datasets can be generated for training and testing fraud detection models, addressing data scarcity issues, and improving model performance.

Potential in fraud detection

This layer holds immense promise for further enhancing insurance fraud detection in several ways.

Figure 3 | Layers of capability in fraud detection using GenAI

FRAUD PREVENTION USING AI

The role of AI in fraud detection has become increasingly critical in today's rapidly evolving digital landscape.

Software giants such as SAS, FICO, Experian, and LexisNexis have harnessed AI to fortify their product offerings and combat fraud challenges faced by the insurance industry. Leveraging cutting-edge AI technologies such as deep learning, machine learning (ML), and natural language processing (NLP), these companies empower their clients with enhanced analytic capabilities, driving informed decision-making and delivering superior fraud protection solutions.

By integrating AI seamlessly into existing platforms, service providers enable insurers to benefit from heightened precision and automation in fraud identification as well as reduced response times and costs. Incorporating AI into fraud detection processes enables employees to enjoy fulfilling roles focused on strategy development, while insurers profit from reduced fraud exposure and optimized operational efficiency.

Here are a few ways in which AI is revolutionizing insurance fraud detection:

1 Automatic anomaly detection

With its ability to sift through massive volumes of data, AI can pinpoint unusual patterns or outliers that could signal potential fraud. This technique helps insurers stay ahead of evolving fraud tactics and maintain tighter control over loss ratios.

2 Synthetic data generation

Given the scarcity of authentic fraud data available for training purposes, AI can generate synthetic data that simulates actual fraud scenarios. Utilized alongside real data, these fabricated examples bolster machine learning model performance, resulting in improved fraud detection outcomes.

3 Pattern recognition

AI demonstrates exceptional proficiency in discerning intricate patterns within data. In P&C for instance, AI-powered image recognition enables faster and more precise assessment of damages. Further, AI trend analysis enhances claims prediction accuracy, fostering proactive fraud mitigation.

4 False positive reduction

As AI continues to refine its algorithms through iterative improvement and self-learning, it reduces false positive alerts, thus streamlining fraud detection processes. This saves valuable time and resources, allowing employees to focus on genuine fraud cases.

5 Real-time analysis

Capable of rapid data processing and evaluation, AI facilitates instantaneous decision-making in fast-paced settings involving high-volume claims. This empowers insurers to swiftly thwart fraud attempts before losses escalate.

6 Adaptive learning

Compared to conventional rule-based systems utilizing fixed guidelines and models, AI adapts dynamically to changing circumstances and novel fraud schemes. Through continuous learning from processed data, AI becomes increasingly adept at combating new threats.

BENEFITS OF IMPLEMENTING AI-BASED FRAUD DETECTION SOFTWARE

Adopting a sophisticated fraud detection software solution delivers a multitude of benefits to insurance providers beyond merely enhancing security. Benefits of implementing fraud detection software include:

1 Reduced operational costs

By automating manual processes and workflows using fraud detection software, businesses can save money while also reducing human error rates. This results in more efficient operations and lower overhead expenses.

2 Faster claims processing

With automated fraud detection measures in place, insurers can expedite claim approvals and rejections, leading to quicker resolution times and improved customer satisfaction.

3 Scalability

As businesses expand, the number of claims they process increases significantly. Unexpected events such as the COVID-19 pandemic can cause sudden surges in claim volumes. Scalable fraud detection solutions allow organizations to maintain their watchfulness towards threats even during periods of unprecedented demand without needing extra resources or personnel. The ability to scale up swiftly is crucial in ensuring continuous protection and minimizing losses incurred due to fraudulent activities amidst fluctuating claim volumes.

4 Regulatory compliance

Insurance companies must adhere to strict regulatory standards regarding privacy, security, and transparency. Utilizing sophisticated fraud detection software helps ensure regulatory compliance by monitoring transactions for suspicious activity and maintaining accurate records.

5 Competitive advantage

Employing state-of-the-art fraud detection techniques empowers insurers to effectively address emerging risks and respond quickly to changing threat landscapes brought about by technological advancements and shifting consumer behaviors. Companies leveraging innovative solutions distinguish themselves from less agile competitors still reliant on antiquated methodologies or manual interventions. Insurers embracing new technologies become attractive options for customers seeking robust security features and seamless user experience. Thus, progressive fraud detection strategies contribute directly to acquiring and retaining clients, fostering long-term success and sustainable growth.

6 Better underwriting outcomes

Accurate fraud detection improves risk assessment during underwriting, resulting in informed decisions about policy issuance and premium pricing. This leads to healthier profit margins and increased revenue generation opportunities.

7 Data-driven AI insights

Modern fraud detection platforms provide valuable analytic reports and visualizations that help in strategic planning, resource allocation, and performance tracking within an organization. Decision-makers gain access to actionable intelligence that enables them to make informed choices about product development, marketing efforts, and other critical areas impacting growth and sustainability.

Overall, implementing cutting-edge solutions provides a strategic edge, from more accurate underwriting and pricing to data-driven business intelligence that drives decision-making across an organization. Implementing robust fraud detection capabilities is a win-win that elevates an insurer's profitability while strengthening risk mitigation postures.

CAPABILITIES OF LEADING AI-BASED FRAUD DETECTION TOOLS

The landscape of insurance fraud detection is undergoing a transformative shift driven by advancements in AI.

Established tools such as SAS, LexisNexis, Experian, and FICO scores are harnessing the power of AI to provide a leap forward in identifying and preventing fraudulent activity.

Data analytics software with AI - SAS

Focus

Analyzes vast amounts of insurance claims data to identify patterns and anomalies suggesting fraud.

KEY FUNCTIONS

- Fraud pattern identification: Uncovers unusual claim frequencies, suspicious claim amounts, and connections between policyholders and providers
- Predictive modeling: Develops models to assess individual claim fraud risk based on various factors

Credit reporting and scoring with AI - Experian

Focus

Provides credit reports and scores reflecting an individual's creditworthiness

KEY FUNCTIONS

- Credit history analysis: Assesses if poor credit history might indicate a higher likelihood of fraud
- Debt verification: Helps identify potential cases of fabricated claims
- Income verification: In some cases, verifies the plausibility of claimed losses or medical expenses

Data aggregation and risk solution with AI - LexisNexis

Focus

Aggregates and analyzes public and private data on individuals and businesses

KEY FUNCTIONS

- Identity verification: Verifies the authenticity of policyholders and claimants
- Link analysis: Uncovers networks of fraudulent activity involving multiple parties

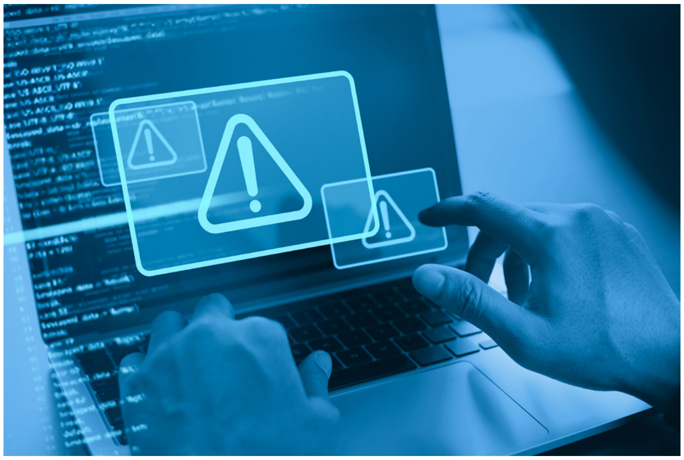
Credit reporting and scoring with AI - FICO

Focus

Develops credit scoring models that assess overall creditworthiness

KEY FUNCTIONS

- Creditworthiness assessment: Low scores can be a potential red flag for fraud, suggesting higher financial risk
- Behavioral analysis: Certain models incorporate factors such as frequent credit applications or sudden debt changes, potentially indicating fraud attempts



FUTURE TRENDS AND OUTLOOK

AI algorithms are constantly evolving, enabling them to analyze vast datasets and identify increasingly sophisticated patterns of fraudulent behavior using a combination of machine learning and deep learning.

Advanced ML algorithms can learn from historical data and predict potential fraud with greater accuracy by identifying anomalies and red flags that might escape traditional methods. Deep neural networks can process complex, unstructured data such as images, social media posts, and medical records, uncovering hidden connections and previously undetected fraud schemes. Software solutions powered by AI can carry out a multitude of checks such as:

Real-time fraud detection

AI systems can operate in real-time, analyzing claims data as it arrives, significantly reducing the time it takes to identify and flag suspicious activity. This allows for faster intervention and minimizes potential financial losses.

Behavioral analysis

AI can analyze policyholder behavior patterns across various touchpoints, including social media, online activity, and claims history. This holistic approach can reveal inconsistencies and suspicious behaviors that might indicate fraudulent intent.

Collaboration and data sharing

AI-powered platforms can facilitate seamless data sharing between insurers, allowing them to leverage collective knowledge and identify emerging fraud trends more effectively. This collaborative approach strengthens the industry's defense against evolving fraud tactics.

Focus on explainability and transparency

As AI models become increasingly complex, ensuring explainability and transparency in their decision-making processes will be crucial. This will foster trust and allow human experts to understand the rationale behind AI-driven fraud detection, enabling them to refine the system and address potential biases.

CONCLUSION

In today's ever-evolving threat landscape, insurance fraud poses a persistent and potentially devastating risk to providers.

As fraudsters continuously adapt their tactics and schemes, insurers must stay vigilant and proactive in preventing fraud. To effectively combat increasingly sophisticated fraud schemes, insurers must adopt advanced artificial intelligence and machine learning technologies.

Leading fraud detection service providers such as SAS, LexisNexis, Experian, and FICO have already started leveraging generative AI to enhance their fraud detection products and services. These providers use advanced techniques such as deepfake detection, adaptive learning, real-time pattern recognition, and data-driven AI insights.

By partnering with proven AI fraud detection vendors, insurance providers can drive critical digital transformation seamlessly. Such a strategic investment will not only strengthen fraud deterrence but also foster innovation, operational excellence, and long-term business resilience in today's dynamic threat landscape.

In the high-stakes battle against insurance fraud, the winners will be players that embrace intelligent automation and predictive analytics. A digital transformation of this scale involving a thorough study of the insurer's current technology landscape and integration with AI tools and solutions requires collaboration with a partner that brings deep domain knowledge and technology expertise to the table. Infosys is a proven force multiplier that enhances fraud deterrence capabilities while driving innovation and long-term resilience for insurance companies.

REFERENCES

1. Background on: Insurance fraud
2. Insurance Fraud Detection Global Market Report
3. https://www.okta.com/identity-101/fraud-detection/
4. Fraud Prevention: Definition & How It Works
5. Real-time fraud detection
6. AI for Health Insurance Fraud Detection – Current Applications | Emerj Artificial Intelligence Research
7. Legal Aid of Arkansas Division of Workforce Services Case (arlegalaid.org)
8. 2021 State of Insurance Fraud Technology Study | SAS
9. Insurance Fraud Detection Market Growth Propelled By Rising (globenewswire.com)
10. Global Insurance Fraud Detection Market Size And Market Growth Opportunities (einpresswire.com)
11. Insurance Fraud Detection with Graph Analytics – Towards AI
12. An engine to simulate insurance fraud network data (arxiv.org)
13. How Is AI Used in Fraud Detection? | NVIDIA Blog
14. 5 Core KPIs in Insurance Fraud Detection and Why You Should be Tracking Them
15. Anti-Fraud Technology Benchmarking Report (acfe.com)
16. Global Artificial Intelligence (AI) in Insurance Market – Industry Trends and Forecast to 2030
17. Teradata and FICO Partner to Reduce Fraud, Improve Business Outcomes | Business Wire
18. The Impact of Insurance Fraud on the U.S. Economy
19. Insurance Fraud Report

Authors

Reviewer

Dilip Bhatt

Senior Technology Architect and Cloud Professional

Dilip is an enterprise and solution architect as well as a multi-cloud modernization strategist. He specializes in digital transformation, application rationalization, cloud migration, and modernization initiatives.

LinkedIn

Tina P

Digital Specialist Engineer

Tina is a machine learning and AI consultant with expertise in NLP, deep learning, and implementation of large language models (LLMs). She is a skilled developer proficient in Python, AWS, and cutting-edge GenAI frameworks. Tina develops and refines models (bridging the research-application gap) for diverse uses.

LinkedIn

Nagaraja Sarma Janga

Principal Technology Architect

Nagaraja is a seasoned solution architect of digital modernization/transformation programs with experience in cloud-native development, application modernization, and portfolio rationalization.

LinkedIn

For more information, contact askus@infosys.com

Infosys® Navigate your next