SHIFT

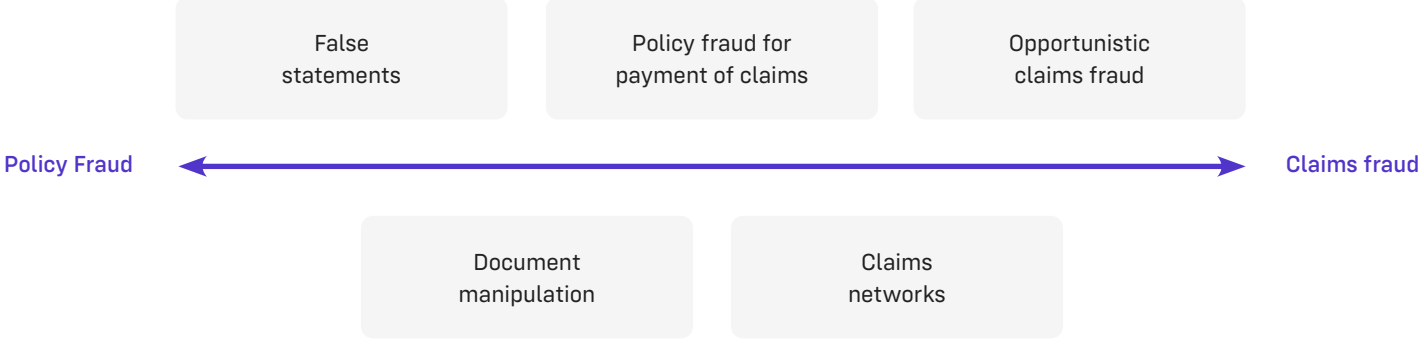
Policy Fraud Trends: How Advanced AI is Helping Insurers Fight Digital Risk

Introduction

On the heels of a difficult few years filled with inflation, changing legislation, and uncertainty, insurers across the UK are looking to adjust their business strategy to tackle costs while still satisfying customers. At the same time, a new set of challenges related to digital fraud are threatening to derail any progress towards a better customer experience. From cyber security to generative AI, insurers have never felt more pressure on the digital front from bad actors attempting fraud with increasingly sophisticated tools.

The Fraud Landscape

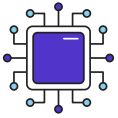
Advanced maturity insurers across the country have become adept at finding claims fraud networks and opportunistic claims fraud, achieving incremental £2.2-5M in fraud stopped for every 200,000 claims analysed.* However, the rise in digital policy fraud represents a unique challenge to underwriters. Policy specific fraud, such as manipulation of bank statements or false declarations, may be intended for lower costs or criminal fronts, rather than fraudulent claims. At scale, the cost to insurers in missed premiums can be severe. At the same time, policy fraud targeting payouts from fraudulent claims are difficult to detect, precisely because they are designed to appear as ideal policyholders, or may even be ideal policyholders whose accounts have been hacked.



*Source: **Shift Technology Insurance Perspectives**

A Suite of AI Capabilities for Underwriting Risk Detection

The good news is, Advanced AI strategies are successfully fighting back against hidden risk and fraud in policies. And while new innovations, such as generative AI, are receiving rightly deserved attention, it ultimately takes a whole suite of AI capabilities to successfully uncover these many new forms of policy fraud and risk. AI is used first to prepare the data for fraud detection. This is where capabilities like entity resolution, where AI assesses possible connections across datasets, can act as a first foundation for fraud and risk detection. Once data has been unified across internal and external data sources, AI methods such as supervised learning and unsupervised learning excel at connecting data to fraud trends. In addition to these methods, for effective document fraud analysis is critical to the UK insurance market, where bank statements and other supplied documents are susceptible to manipulation or falsification. Finally, advanced network detection models excel at finding connections across policies, providers, people, and properties. The point is, AI is not just one maths equation, it's several capabilities deployed together to stop policy fraud.



Generative AI

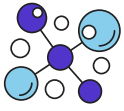
Generative AI is a branch of artificial intelligence that focuses on creating new data, content, or outputs based on patterns and insights learned from existing datasets

Machine Learning (ML)

A subset of AI that enables machines to learn from data without explicit programming. It allows systems to improve their performance over time through experience

Network Analysis

The process in which data is collected and analysed to identify individual connections to a broader network

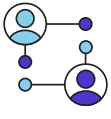


Supervised Learning

A type of machine learning where the algorithm is trained on labelled data, and it learns to make predictions based on this input-output mapping

Unsupervised Learning

A type of machine learning where the algorithm learns patterns and structures from unlabeled data without explicit guidance



Entity Resolution (or Reconstruction)

The identification and consolidation of separate entities in a data source that actually represent the same real-world entity

Reinforcement Learning

A type of machine learning where an agent learns by interacting with an environment

Document Analysis

A type of analysis that gathers metadata, image, and text information to extra insights from documents for use in machine learning

False Declaration Networks

✓ Network Detection ✓ Supervised Learning

Fraud Method

False declarations are nothing new for insurers, but the cost of inflation has pushed more in the UK to consider these types of fraud. These small false declarations, whether about the vehicle location, the primary driver, or commercial vehicle use, leads to lost premiums and higher claims costs. But what happens when this method of false declaration is built into a business model for lower premiums?

A Shift customer recently detected a false declaration network, where a residence in a higher-end neighbourhood was presented as the location of multiple vehicles. In truth, the residence was abandoned, and the vehicles were all related to a business in an entirely different neighbourhood being used as work vehicles, incurring multiple claims.

False declaration data samples

More than 10 vehicles insured at a false address

3 key links: Telephone, IBAN, last names

16 Social ties: Family, colleagues, neighbours

Impact to Insurers

While the main purpose of these false declarations is rate evasion rather than claims payouts, Insurers in the UK have to face the cost in claims. This can range up to £3,000 for commercial vehicle claims, nearly twice the cost of a typical personal motor claim. The modified neighbourhood network mentioned above had filed claims on their many commercial vehicles over 5 years, costing the insurer nearly £21K.

Advanced AI Approach

Several advanced AI methods come together to detect false declarations, including unsupervised learning and network detection. Looking across policies, AI can quickly identify links in contact information or underlying IBAN information, as well as external data like business records. In this case, the external data connection revealed the commercial use of policies authorised for personal use only, empowering the insurer to take action.

£21K

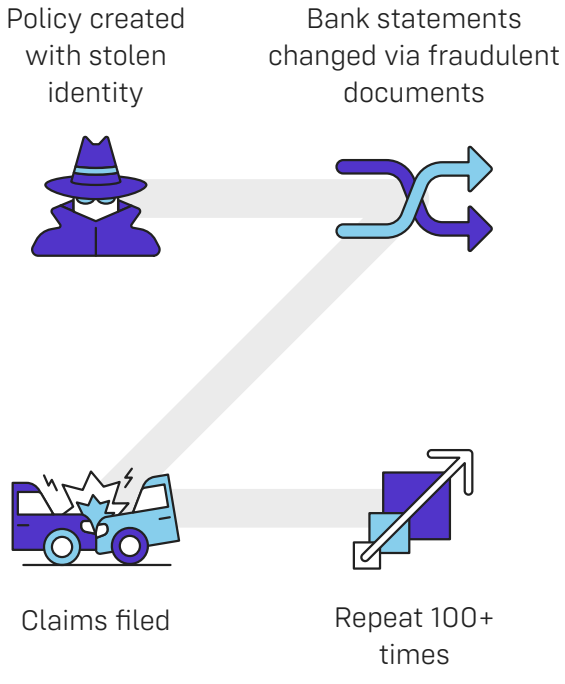
Estimation of claims costs from a single false declaration network

Policy Fraud Networks

✓ Entity Resolution ✓ Unsupervised learning

Fraud Method

The relative anonymity of online insurance applications has opened up a new path for large scale fraud through the use of stolen identities and fraudulent documents. A recent example identified by Shift included 146 new policies generated over the course of 6 months. On the surface, the policies looked quite desirable: Higher value vehicles from drivers with a clean record. Behind the scenes, these policies were all being generated through stolen identities and outright false - but consistent - policy information included in bank details and statements. WIth nothing out of the ordinary, these policies were bound, and perhaps even valued as good business.



Impact to Insurers

For the impacted insurer, dozens of corresponding minor 3rd party claims were then filed, costing the insurer not enough to be concerned about the individual claim, and keeping the fraudulent policies under the radar. However, when added up, the total cost of claims were estimated at £127K, costing the insurer far more than the collected premiums.

95 claims

in a 6 month period

Advanced AI Approach

AI is particularly adept at uncovering suspicious patterns which are otherwise "normal" and "consistent." For these types of policy networks, entity resolution is important because it detects similarities between policies, including policy details and locations where those policies have been incepted. Additionally, document fraud detection can intake and compare images or pdfs across policies to identify when images are similar or when they've been modified.

Once the network is identified through AI, the insurer is able to take action, by automatically investigating claims associated with the network, routing policies for non-renewal, and reviewing applications suspected to be part of a network.

Fraudulent Broking

✓ Network Analysis ✓ Document analysis

Fraud Method

While policy fraud often originates with individuals attempting to gain insurance for themselves or their network, a special class of policy fraud exists for agent-based fraud. Called "ghost broking", the schemes for fraudulent broking can relate to both licensed agents pocketing premiums without insuring policyholders OR unlicensed "agents" who sell fraudulent policies. In the case of unlicensed agents, the draw is for inexpensive insurance for individuals who might have to pay more due to claim history, location, or age. One recent public example in Italy highlights the methods by which fraudulent brokers profit*. Criminals acting as insurance agents purchased inexpensive policies on behalf of deceased individuals or stolen identities through false declaration. Then, they would "sell" the policy to unsuspecting consumers by forging vehicle sale documentation so that the new "policyholder's" vehicle would actually appear on the insurance policy, albeit for a person who didn't actually own the car. The "broker" pocketed the difference in premiums, and disappeared in the event of a claim, leaving the insurer to pay out the claim. In other geographies, including the UK, false brokers may similarly leverage this situation.

274 people involved

70 agencies impacted

*Source: **Fake Documents for Low-Cost Car Insurance: Massive Scam Discovered in Trieste**

Impact to Insurers

The police investigating that particular network estimated insurance losses at 700K€, with 274 people suspected of participating in the fraud. In Shift's own investigation of fraudulent broking networks, UK insurers have uncovered networks with as many as 400 policies suspected to be "ghost broked," with the potential for hundreds of thousands of loss in each network.

400+

Policies in single network detected by Shift in UK

Advanced AI Approach

Fraudulent broking can take many forms, which means that multiple AI methods work in tandem to uncover networks. Key to this work is supervised learning to seek out similar patterns in active policies, as well as network links and network detection, finding IBAN, contact information, or other patterns across policies. Equipped with these capabilities, Shift customers have moved up detection of network links into real-time for new applications, keeping new fraudulently booked applications from becoming policies.

Hacking network

✓ Unsupervised learning ✓ Entity Resolution

Fraud Method

While many attempts at policy fraud are at the point of application and sale, Insurers are also at risk for fraud losses incurred through cybersecurity breaches. In these fraud attempts, criminals gain access to customer accounts through phishing or other methods, change bank account information, and file minor claims such as windscreen damage. This form of fraud can also happen at a scaled level; in one such recent instance in France, an insurer's customer policy portal was breached, leading to multiple accounts switched to the same IBAN, and an ensuing flood of nearly 100 minor claims to capitalise on the breach.

Impact to Insurers

While the impact to this insurer was more than 100K€, the real concern is the risk to the insurer's brand. 58% of insurers see fraud as having a negative impact on customer experience, and undetected manipulation creates a perception that policyholder information is not securely protected.*

Advanced AI Approach

AI can be used at the time of endorsements or policy changes to detect these patterns, with both unsupervised learning recognising that a pattern of rapid, similar change is forming, while network linking recognises the repeated IBANs or other contact information. This way, insurers can actively pause claim payments even on seemingly minor claims, while internal information security teams can investigate and resolve the breach.

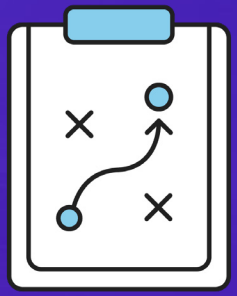
58%

of insurers indicate fraud has a negative impact on customer experience

*Forrester: "Insurers: Strike The Right Balance Between Fighting Fraud And CX"

Where insurers can start?

Considering these digital fraud trends, underwriters can start building their own unique plans for how they tackle new forms of policy fraud with the following considerations.



1. **Evaluate Risk Priorities**
   Assess which types of fraud trends are most important to address. A good risk gap analysis can help an insurer determine where to begin. For example, if the insurer's distribution model is agent based, the focus could be on agent patterns as well as false declarations. However, an insurer focused online may focus on document fraud detection for generative AI images, or network analysis.

2. **Consider Build vs. Buy**

   It's important to think through the pros and cons of building vs. buying when exploring the use of AI to solve digital policy fraud. Fraud continues to evolve, so a major consideration should be whether you have not just the initial ability to invest, but the ongoing resourcing needed to continually adjust and update AI, manage the advanced AI infrastructure needed to stay ahead, and support user teams as effectively as a specialised vendor.

3. **Ensure Data Security**

   Given the increased cyber security risks posed by fraud trends, validate that vendors and partners are maintaining the highest security certifications and protocols. This aligns with the reality that policy fraud includes cybersecurity risk for insurers themselves. Therefore, any AI fraud technology deployed must necessarily be designed to protect insurer customer data at an equal or higher level.

SHIFT

About Shift Technology

Shift Technology delivers AI-powered decisioning solutions to benefit the global insurance industry and its customers. Our products enable the world's leading insurers to improve combined ratios by optimising and automating critical decisions across the policy lifecycle. Shift solutions help mitigate fraud and risk, increase operational efficiency, and deliver superior customer experiences.

Learn more at **www.shift-technology.com/eb-gb**.