INSEAD The Business School for the World®

Pre Release Version

Case Study

To Catch a Thief:

Explainable AI in Insurance Fraud Detection

07/2022-6752

This case study was written by Antoine Désir, Assistant Professor of Technology and Operations Management, Ville Satopää, Assistant Professor of Technology and Operations Management, both at INSEAD, Eric Sibony, CTO at Shift Technology, and Laura Heely, INSEAD MBA'17. It is intended to be used as a basis for class discussion rather than to illustrate either effective or ineffective handling of an administrative situation.

Extra teaching materials are available at https://publishing.insead.edu/case/to-catch-a-thief

White lies cost the insurance industry billions of dollars every year. Ironically, after investing heavily to automate workflow from policy subscription to claims processing, digitization has made fraud easier to commit and harder to catch. However, advances in artificial intelligence and machine learning (AI and ML) offer some hope to an industry drowning in data and paying out millions for fraudulent claims.

As a senior operations professional at Shift, an insurtech unicorn, you are tasked with refining the company's fraud detection algorithm, which is used by leading global insurers such as Generali France and Mitsui Sumitomo to fight fraudulent claims. Working with a team of data scientists and engineers, you are responsible for overseeing the logic powering the algorithm. The choices you make will have an impact on millions of policyholders serviced by your partners in terms of monthly premiums, claims outcomes, and overall experience. Equipped with a rich dataset of more than 10,000 claims, you can backtest your logic on historical data.

What does the optimal model look like? How will you market it to insurers?

A Crash Course on Insurance Fraud

Insurance fraud – acting to deceive an insurer for economic gain – is believed to occur in between 10 and 20% of insurance claims.[1] In the US, the world's largest insurance market, the Coalition Against Insurance Fraud estimates that the cost of fraud exceeds US$80 billion per year.[2]

Soft (or opportunistic) fraud is the term used when individuals exaggerate or lie in the claims or application process to submit a higher claim amount or pay a lower premium. Common examples include overstating damages in an automobile collision and neglecting to mention a health condition or vice such as smoking that increase insurance premiums. Experts report more frequent occurrences of soft fraud, albeit with a lower monetary value than professional fraud cases.

Hard (or professional) fraud occurs when someone deliberately plans or invents a covered loss to claim payment for damages. Premeditated fraud – often perpetuated by criminal organizations – represents millions of dollars in theft. Some of the more bizarre cases become tabloid fodder with staged deaths, faked amnesia, and intentional arson. Others are more sophisticated such as the white collar criminal sentenced to 845 years in prison for his role in a "series of numbingly complex mortgage and stock frauds" that cost National Heritage Life Insurance Company US$450 million.[3]

A sizable portion of insurance fraud stems from the fact that those who commit fraud do not think of themselves as dishonest. A survey by the Association of British Insurers found that roughly a third of people thought it was acceptable to inflate the worth of a lost or stolen item, or exaggerate claims for damages.[4] McKinsey & Company describes this view of

1 Shift company analysis
2 Coalition Against Insurance Fraud
3 The New York Times
4 RipeInsurance

insurance fraud as "peccadillos" (little sins) about which "many of the perpetrators do not even have a bad conscience."[5] However, these peccadillos add up.

Due to the pooled pricing and risk structure inherent to insurance (see **Exhibit 1**), insurance fraud hurts honest policyholders because it is recouped via increased premiums – to the tune of £50 per year in the UK[6] and up to US$700 per year in the US.[7] The logic is relatively simple: as claims paid rise, either premiums must rise or losses covered (reimbursed according to an insurance policy) must be minimized, both of which hurt the policyholder. Premiums are calculated based on the collective risk of the pool.

The insurance industry has made strides in tackling fraud with a combination of manual and automated interventions. **Exhibit 2** illustrates the steps in the fraud detection process undertaken by insurers, whereby suspected incidents are investigated by specialist teams. In the UK alone, £1.2 billion worth of confirmed and suspected general insurance[8] fraud cases were found in 2019, spread over nearly 107,000 incidents (a 5% increase in volume year-on-year).[9] With an insurance scam estimated to occur every minute in Britain, an estimated £2 billion of fraud slips through the net undetected.[10]

Anti-fraud techniques like automated business rules, data visualization, and manual red flags are somewhat effective for insurers in spotting known fraud patterns, but sophisticated fraudsters are 'gaming the system' at an alarming rate thanks to increasingly automated workflows.

With troves of data at their fingertips, artificial intelligence (AI) offers insurers a neat solution. While its application to insurance fraud detection has been slow, a slew of state-of-the-art AI technologies are now being deployed such as anomaly detection, network analysis, web crawling and analysis tools for images, videos and speech (see **Exhibit 3**). However, with limited visibility into how AI and machine learning technologies work, some insurers are concerned that hidden biases may be skewing the results (see **Exhibit 4**). Examples of AI gone wrong, such as the Dutch child benefits scandal in which 20,000 parents were wrongly labelled fraudsters, give insurers pause before replacing humans with machines.

Shift Technology

Shift was founded in Paris in 2013 to tackle insurance fraud using powerful AI solutions to root out fraudulent behavior and automate claims processing. The brainchild of founders Jérémy Jawish, Eric Sibony and David Durrleman, Shift offers a cutting-edge technology

5 McKinsey & Company
6 UK Government
7 Federal Bureau of Investigations
8 General insurance refers to insurance policies outside of life insurance, for example property and casualty insurance, health insurance, and travel insurance.
9 Association of British Insurers
10 UK Government Insurance Fraud Task Force

solution via SaaS.[11] Their AI-native toolkit covers claims fraud detection, claims automation, underwriting software, subrogation[12] detection, and financial crime detection.

University friends Jawish and Sibony came up with the idea during internships at a multinational insurance company on a fraud-detection team. During the five-month stint, they realized that, despite the fact that insurers were sitting on hundreds of years' worth of data and actuarial expertise, the industry was not equipped to analyze the data it captured. Innovation, they believed, had to come from the outside. Joining forces with technical co-founder David Durrleman, they put their heads together to build a more powerful fraud-detection model using AI.

Despite prior experience in insurance and financial services, they were fresh out of university at the time they started Shift. Jawish describes the reaction when first pitching AI solutions to large insurance incumbents:

> *"It wasn't the trend in the insurance market. It was hard at first. Everyone said they weren't going to look at a bunch of kids."* [13]

Shift's solution suite was developed expressly to help those incumbents detect fraudulent behavior. It pioneered a new branch of intelligence tools called Explainable AI, which provided the rationale for insurers on top of the analytical tools. Early results were promising. Compared to an average industry hit rate (or conversion rate) of 35%, Shift's 75% was dramatically more accurate.

How did they do it? The fraud detection algorithm worked by identifying statistical patterns across a range of internal and external datasets and comparing them with individual claims filed. These datasets include policy information, claims reports, satellite imagery, historical fraud scenarios, weather conditions, as well as policyholder photos, videos and social media. Additional AI and ML techniques such as "privileged learning"[14] and natural language processing[15] (NLP) helped Shift contextualize and understand claims in real time. In turn, Shift's data and behavioral analysis could be used by insurers to set up rules and processes that flag suspicious claims for review by Special Investigative Units (SIUs) (see **Exhibits 5** and **6)**.

With automated claims handling and AI-based decision automation, Shift provided tangible benefits in terms of business profitability and customer experience. Notably, claims

11 SaaS, or Software as a Service, refers to a model of licensing and delivering centrally hosted software on a subscription basis.

12 Subrogation describes a right held by insurers to legally pursue a third party that caused an insurance loss to the insured. Subrogation helps insurance carriers recover the amount of the claim paid by the insurance carrier to the insured for the loss. For example, in the case of a car crash, subrogation allows an insurer to recoup costs (car repairs, medical expenses, etc.) from the at-fault driver's insurance company.

13 TheInnovator

14 "Privileged learning" paradigms, also referred to as "learning using privileged information" and "LUPI" describe machine learning techniques in which contextual (or privileged) information is shared by a so-called Intelligent Teacher to an algorithm Student during the training stage to accelerate the speed of learning.

15 NLP is a branch of artificial intelligence that is concerned with deciphering and understanding human (or natural) language.

automation had the dual advantage of increased claims-handling productivity and reduced leakage (money lost through claims management inefficiencies), each of which improved profitability through reduced costs. The cherry on the cake was that machine learning enabled the algorithm to improve with every new claim analyzed.

Amplifying an insurer's existing systems, Shift enabled a high-volume, low-touch claims process that was fast, fair, and appealed to policyholders. Its direct claim settlement solution aimed to meet evolving policyholder expectations through an API (application programming interface) that allowed Shift's technology to be seamlessly adopted by the insurer's own systems and branding.

In May 2021, following a US$220 million Series D funding round led by Advent International, Shift achieved 'unicorn' status (a valuation in excess of US$1 billion). The team planned to use the capital injection to fund expansion in its core market, property and casualty (P&C) insurance, expand further into health and travel sectors, and grow the company's burgeoning US presence. Fueled with additional capital and experienced investors, Shift hoped to win the projected US$7.9 billion global market for insurance fraud technology.[16]

But it was not alone. The competitive landscape, including virtual claims management technology such as Guidewire and BriteCore, was heating up with well-funded insurtech start-ups building in-house fraud-detection systems (like Lemonade's AI lie detector) and direct competitors from China like Ping An. Success would therefore depend on continuing to improve its fraud-detection prowess and convincing more insurance companies to sign up to use Shift technology.

Decisions: Improving the Algorithm

As a senior member of Shift's Operations team, your job is to maintain and improve the fraud detection algorithm with the help of dozens of data scientists and engineers. Which objectives are most important for your model? What should you prioritize?

1. **Increasing the detection rate:** Undetected frauds, which appear as false negatives in the algorithm, are estimated to be costing insurers millions of dollars *per day*. Should you seek to increase the detection rate of suspicious claims? How?
2. **Improving the hit rate**: Insurance fraud detection teams have set budgets for investigations. Time and money spent by fraud investigation teams scrutinizing false positives cannot be spent fighting real fraud. How can you improve the algorithm's hit rate?
3. **Limiting bias:** Not all fishy behavior implies fraud and false positives may have unintended consequences for policyholders such as punishing poorer individuals who use lower-resolution cameras. What tools does Shift have to limit bias in the algorithm?

16 ReportLinker

4. **Evolving over time**: Since the advent of digitization in insurance, criminal fraudsters are becoming ever more sophisticated. How can Shift's fraud-detection tools keep up?
5. **Ensuring usage:** Ultimately, the SIU decides which cases to investigate, no matter what score Shift applies to a claim. What mechanisms can help convince insurers to use Shift?

Decisions: Go-to-market Strategy

On the heels of a few cunning suggestions to improve the fraud-detection algorithm, the team has asked you to propose a go-to-market strategy, evaluating the following considerations:

1. How can Shift widen its competitive moat? What do you view as its defensible USPs (unique selling points) as it expands internationally?
2. With some evidence of insurtech platforms creating their own in-house fraud-detection solutions, should Shift worry about their insurance partners copying its technology?
3. Tech companies and local regulators have recently enacted new privacy policies and rules which allow people to control usage of their data. With heavy reliance on external datasets, should Shift be worried?

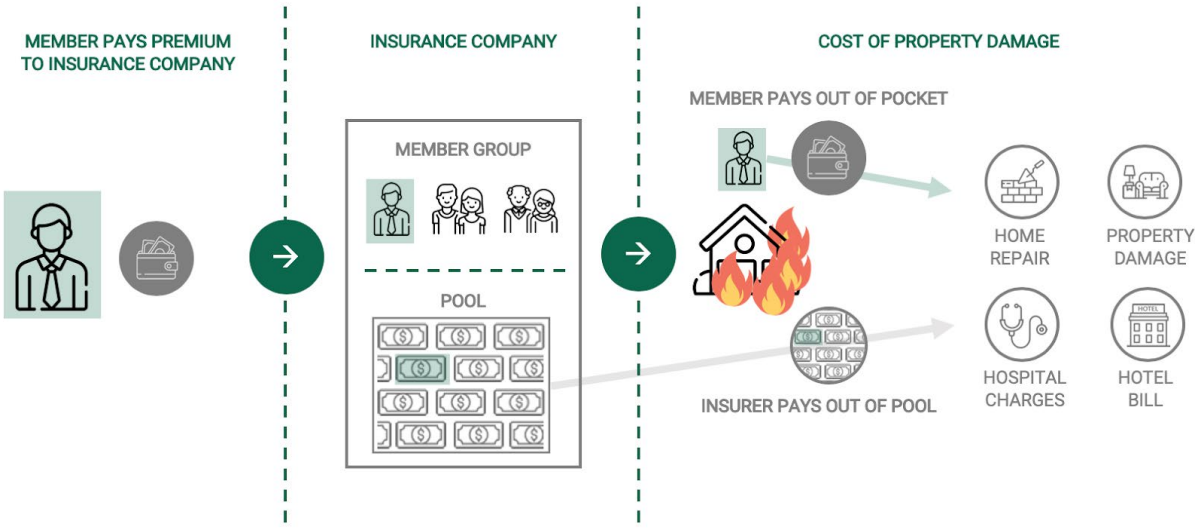
Exhibit 1

How Insurance Works

The concept of insurance emerged to help provide security and protection against risk. Clients (individual or business) agree to a policy and pay a regular premium to an insurer to protect against financial damages associated with an insured loss (i.e., fire, accident, theft). In practice, it enables businesses to operate in a cost-effective manner by transferring certain risks associated with their activities to third parties. For individuals and families, insurance is vital, as it provides financial security for common and costly events like illness, property damage, or death of a loved one.

Insurance companies pool risk across their client base to provide protection at a reasonable cost to individual policyholders. They pool the premiums collected, which are used to settle policyholder claims and cover operating costs.

Figure 1. Illustration of insurance pool in Property and Casualty insurance



Source: Authors

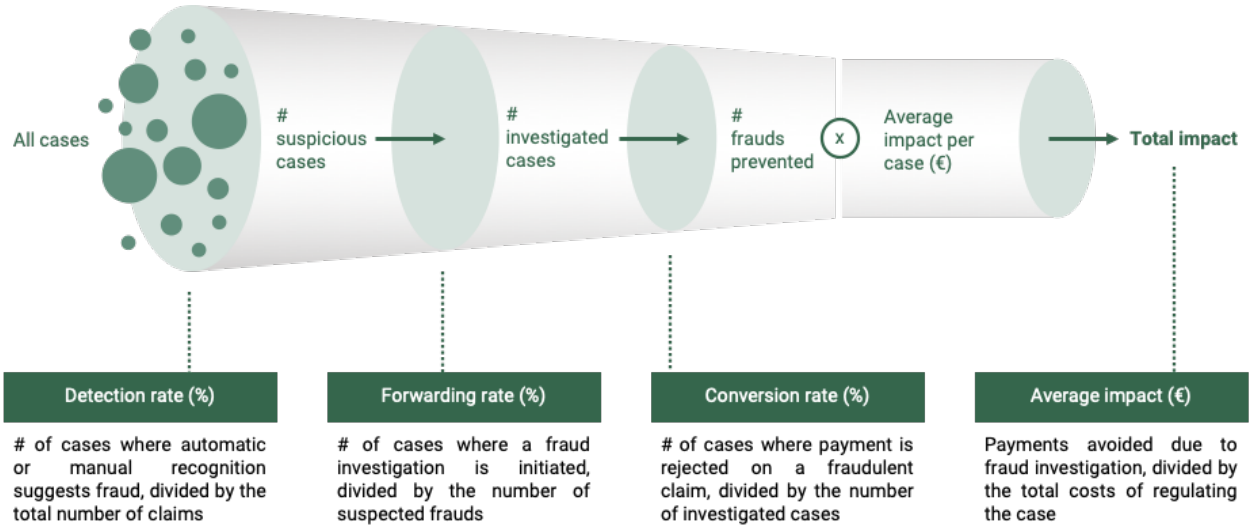
From a policyholder's perspective, three basic components of insurance are the premium, policy limit, and deductible.

- A **premium** is the price of an insurance policy, typically expressed as a monthly cost. Typically, premiums are determined based on the coverage requested and the risk profile of the policyholder (assessed by underwriters of the insurance company).
- The **policy limit** sets the maximum amount an insurer will pay for a covered loss. As a general rule, higher policy limits are associated with higher premiums.
- The **deductible** refers to a specific amount that the policyholder must pay out-of-pocket before the insurer settles the claim. Higher deductibles usually are associated with lower premiums.

Exhibit 2

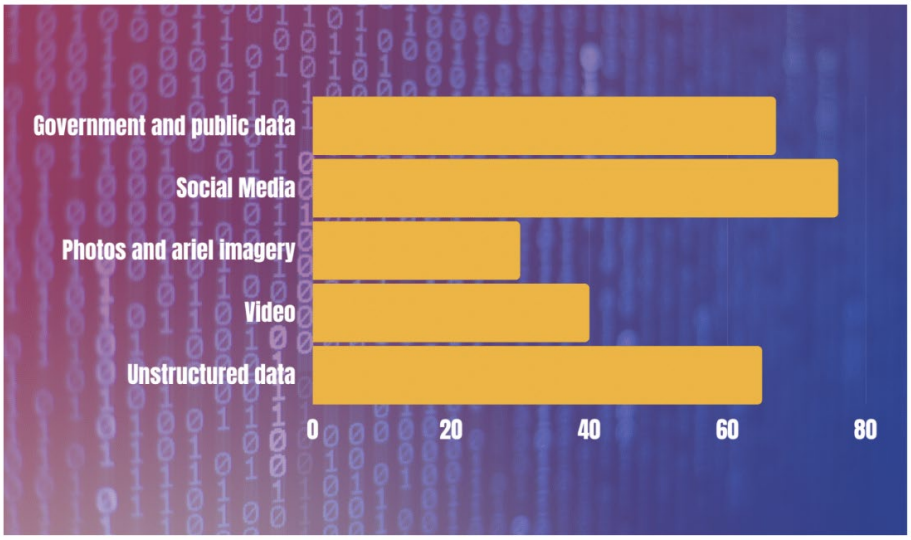
Insurance Fraud Detection

Figure 1. Fraud detection funnel



Source: Adapted from McKinsey & Company

Figure 2. Data sources used by insurers to fight fraud detection in addition to claims and policy data



Source: Coalition Against Insurance Fraud

Exhibit 3

Select AI Technologies in the Insurance Industry

Anomaly detection: The user defines a baseline for key performance indicators (KPIs) associated with tasks or events, then sets a threshold. When a threshold for a particular measure is exceeded the event is reported. Outliers or anomalies are used to identify existing or previously unknown patterns.

Network analysis: Organized fraud involving multiple linked claims and entities is pervasive and continues to expand. To address organized fraud rings, insurers are looking to capitalize on emerging highly sophisticated capabilities to analyse social networks and identify connections and patterns. Network link analysis has proven effective in identifying organized fraud activities by modelling relationships between entities in both the claims and new business acquisition processes. While link analysis is not new to fraud investigators, AI's ability to analyse massive amounts of data and "connect the dots" takes analysis to levels never seen before.

Natural language processing (NLP): NLP is a branch of artificial intelligence that helps computers understand, interpret, and manipulate human language. It draws from many disciplines, including computer science and computational linguistics, and seeks to fill the gap between human communication and computer understanding.

Machine learning for scoring (neural networks, random forests, etc): This technology uses mathematical algorithms that learn from data without relying on rules-based programming. With every iteration the algorithms become smarter and deliver more accurate results. Machine learning (ML) is split into supervised and unsupervised learning. Unsupervised ML is very effective in detecting suspicious activities when users don't know what specific data may indicate fraud.

Speech recognition: Sentiment analysis algorithms can be used during customer communications to analyse speech and voice patterns. Combined with spotting keywords, identification corresponding to certain sentiments, speech recognition can provide strong indicators of potential fraudulent behaviour that most humans would never be cognisant of during the conversation.

Image & vision analysis: Image analysis allows the computer to determine if the subject of the photo is indeed the insured object (for example, a broken television, flooded basement, cracked headlight), or if it is something completely unrelated. It can also verify that a photo has not been used in previous claims, downloaded from the internet, or manipulated in various ways.

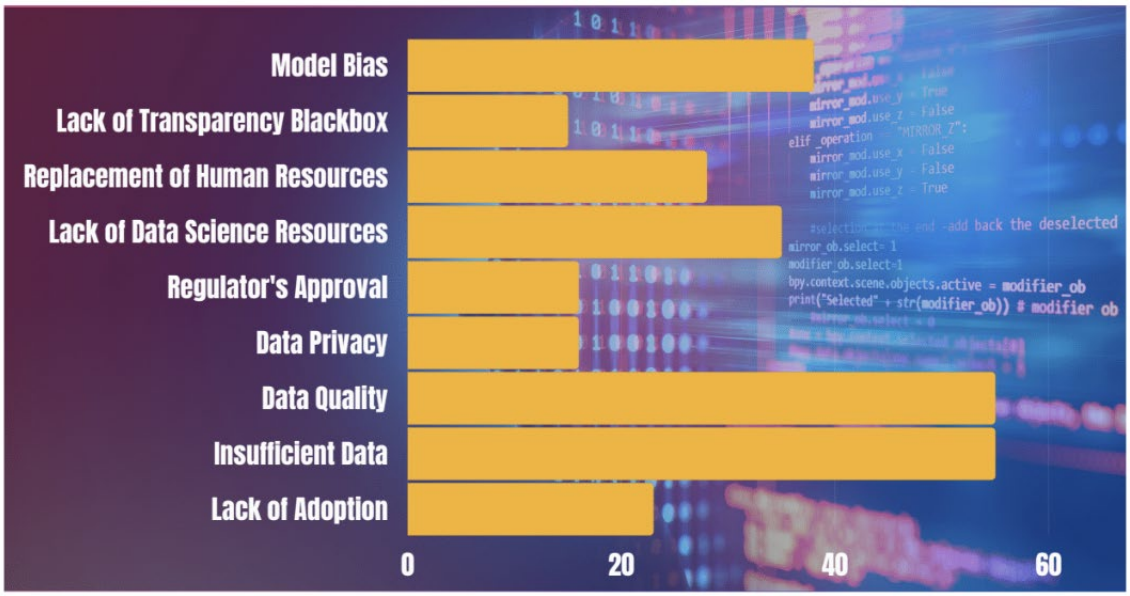
Web crawling: A new area of text mining focuses on the ability to analyse the huge amount of data available within the realm of social media platforms. Investigators are now searching publicly accessible Facebook, Twitter, Snapchat, Instagram, LinkedIn, Craigslist and other social media sites for evidence of non-meritorious claims. While the social media angle is rather advanced, some insurance companies are using software to effectively mine and analyse this unstructured text data in meaningful ways.

Source: Coalition Against Insurance Fraud

Exhibit 4

Insurance Industry Perceptions of AI in Fraud Detection

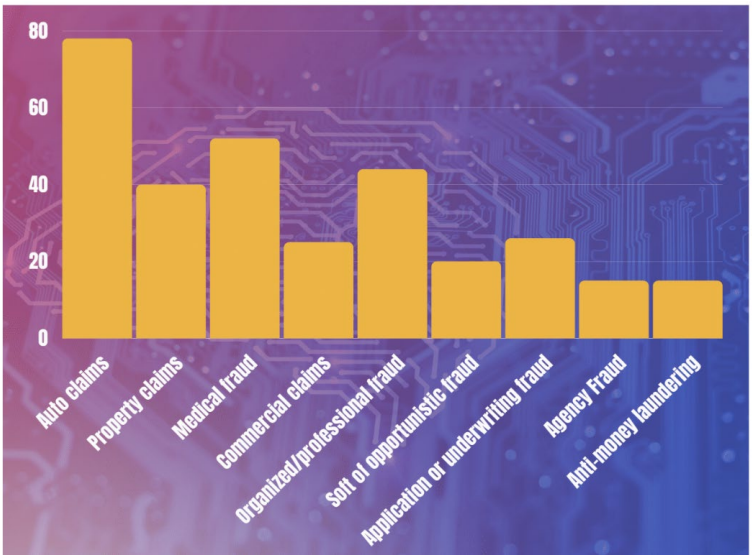
Figure 1. Primary concerns of insurers when considering using AI



Source: Coalition Against Insurance Fraud

Survey participants were invited by the Coalition Against Insurance Fraud to name their top three concerns regarding the use of AI in their business.

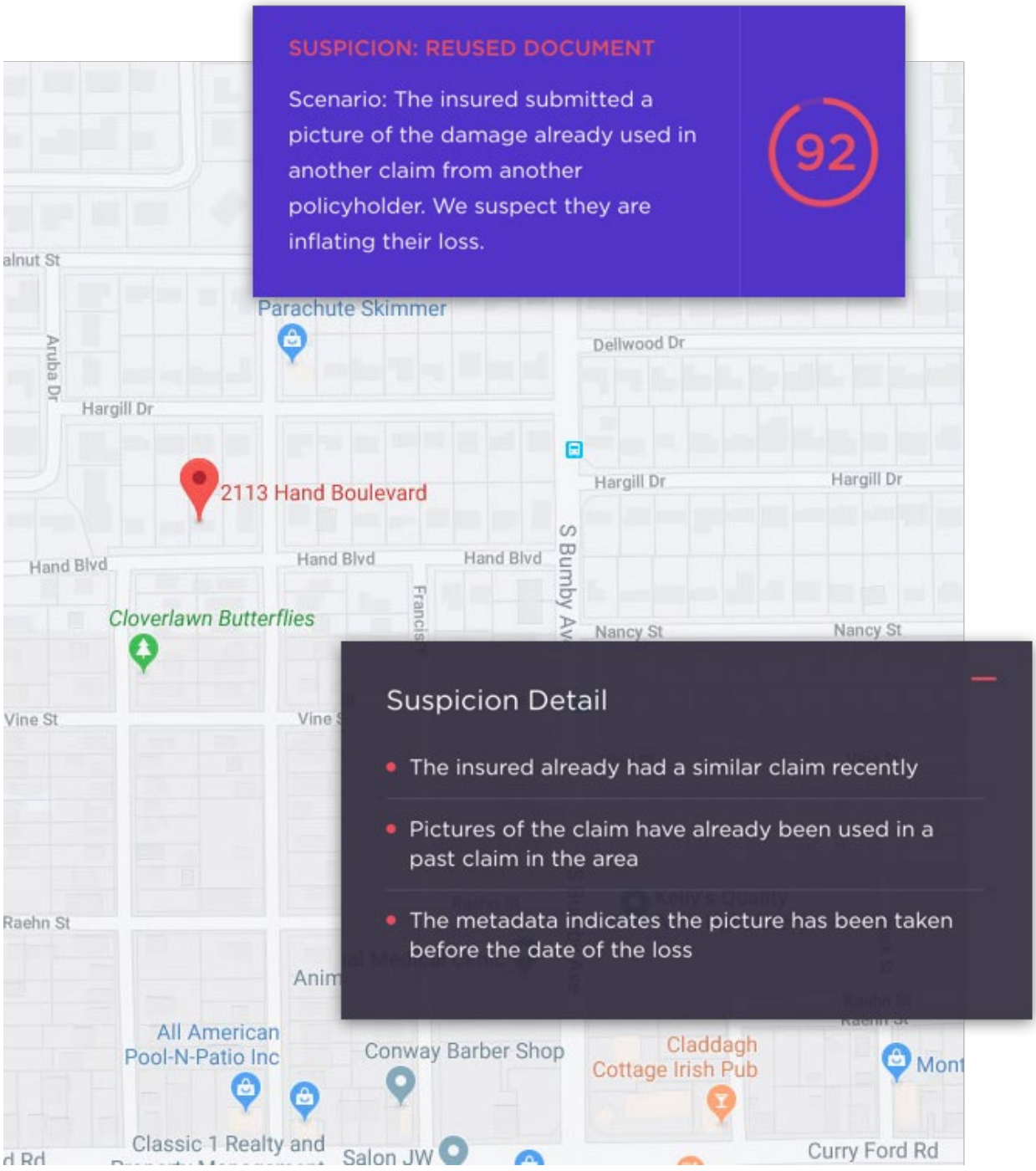
Figure 2. Areas highlighted by insurers for greatest impact in fraud detection



Source: Coalition Against Insurance Fraud

Exhibit 5

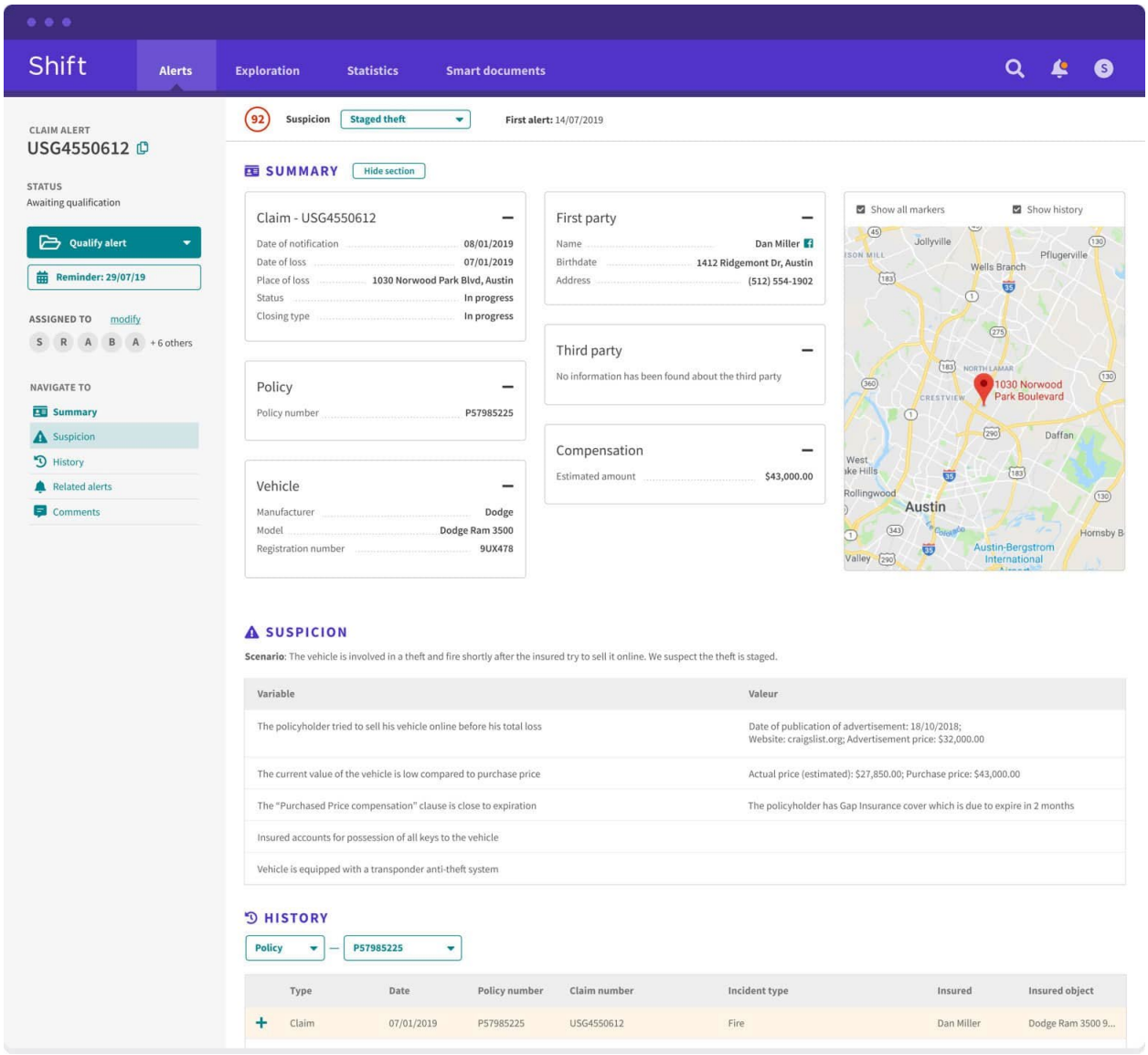
Shift Claims Fraud Detection



Source: Shift website

Exhibit 6

Shift Claims Alert: Suspicious Activity



Source: Shift website