Insurance Frauds and Prevention

Measuring insurance fraud has always been and was an elusive goal. Trying to understand fraud numbers is a constant work in progress. It is widely estimated that fraud can account for up to 20% of an insurance company's claims costs on average. But to better understand insurance leaks, let's dig deeper into real-life examples of the four most common insurance frauds and how to prevent them.

# What is an Insurance Fraud?

Insurance Fraud is considered to be an illegal activity conducted by the purchaser or seller of insurance policies. Insurance fraud by issuers includes selling policies from nonexistent companies, failing to submit premiums, and canceling policies to earn more commission. On the other hand, buyer fraud consists of exaggerated claims, medical history falsification, policy date changes, travel fraud, fake death or kidnapping, and murder.

# What is the motivation behind Insurance Fraud?

Many people who commit fraud do so out of desperation because they are in dire financial straits. But that's not the only motivation for insurance fraud. It also includes greed, addiction, entitlement, and so on.

* Organized crime syndicates are willing to pay premiums for up to three months. I know the insurance payout markup could be more than thrice what he paid.
* Before a customer can cancel an insurance policy, they view the insurance as a ransom purchase and submit false or fraudulent claims as they need to profit from all the premiums they have paid over the years.
* Debt collectors target scammers and the only way to pay off your debt is to file a fraudulent claim.
* Customers cannot get additional loans or credit from banks or financial institutions, and the only way to get cash is to submit a fraudulent claim.

# How Insurance Fraud is committed?

Organized crime is a category of international, national, or regional groups of highly centralized corporations that criminals operate to engage in illegal activities, most commonly with money and money. It is purely intended to earn profits unethically.

In recent years, we have become accustomed to accident-preparedness communities that collect and purchase vehicles that have been involved in accidents, insure them, and stage accidents, thefts, or robberies with the intent of recovering the insurance value. These losses occur within days of initiation. Then there would be little evidence of the vehicle's existence and no time for inspection. The members of the syndicate were initially the insured of the policy, but they used the economically deprived to draw them into this vicious cycle and make it harder for insurance companies to close the loop on this criminal ring. It has been found that additionally, these criminals commit identity theft by sending personal information to unsuspecting individuals to close the policy. It also randomly selects vehicle information by copying details from vehicles that do not yet have proof of ownership on the sales floor. In addition, we also use information about vehicles involved in previously uninsured accidents. The claim was also filed within his first week of initiation, leaving no time to see why the registered owner and policyholder information did not match. Members of the consortium pick up rental cars by the time they realize something is wrong and the matter is referred for further investigation. A release fee was also paid for the release of the vehicle to an unauthorized towing contractor. The tow company and invoice turned out to be fictitious and the vehicle cannot be found by the tow company.

In some cases, the syndicate cannot use the vehicle information because the vehicles with the tow company have been abandoned by their previous owners and these vehicles have not been deregistered or disposed of as required by law. It's getting easier. By the time the investigation uncovers all this information, the rental car may have been rented to an unsuspecting individual who paid a membership fee to a member of the syndicate, or the vehicle may have been stolen. Real-time analytics and triggers can prevent similar events like this from progressing to the stage where rental vehicles are issued and potential claims are paid, with no financial loss to the insurer.

Take another example of luxury watches and the reason why it is important to share unique specifications such as serial numbers internationally.

Many people these days buy and wear quality watches due to rising crime rates around the world. Armed robberies of these insured luxury watches are on the rise and are precisely carried out by organized crime gangs in the same manner. The insured in almost all cases will find themselves being tracked while visiting public areas such as local grocery stores, shopping malls, gas stations, and restaurants. Spotters are looking for customers wearing these luxury watches. The customer (in this case, the insured) is tracked down, and when they arrive at their destination, they are robbed and their watches were stolen. The goal is always the clock. These armed robbers rarely steal other items unless the opportunity presents itself. Criminals are often brazen and footage of them with identifiable faces is available. When such an incident occurs, the insured will usually report the armed robbery to the police, who will circulate the stolen watch based on the serial number. The serial number and brand of the watch are then entered into the police database. He had one such incident in April 2019. After examining a customer's watch that was put up for sale at a Chinese auction house in October 2019, investigators were able to block the sale of the watch. The watch was worth R600,000 ($36,000) when it was lost. This is made possible by ensuring that the watches are also distributed internationally through the Manufactory Jewelers. However, such common scenarios offer fraudsters the opportunity to insure fake watches and staged losses to advance the possibility of expedited settlement and recovery of the watch. Since most international and proprietary branded watches have serial numbers and may be distributed by the manufacturers of those watches, they cannot be sold at auction. Collecting and compiling data will help identify and investigate these cases. Only pictures of the watch may be provided as evidence and these are taken from the internet. Activating an image scanning tool can help you figure this out and investigate very quickly.

# How can technology help?

Consider an example of a stolen car and how technology can help recover stolen vehicles. Car theft is more common than we believe. In many cases, the tracking device is disabled, so the insurance company will attempt to recover the vehicle and eventually pay the claim. But it doesn't have to be. This real-life example shows another solution and results for the claim. Mr. X reported that his car was stolen from his residence in the Bluff district of Mumbai, India. As he heads to his job, he finds his car missing. The night before the theft, he had parked his car in the yard behind an access-controlled gate. When his wife got up the next morning, she found the access gate open. Further investigation discovered that the vehicle had been stolen and had no visible damage to the gate or engine. Mr. X immediately reported the theft to the police and notified a tracking company to locate and retrieve his car. Mr. X was told that a tracking device attached to his vehicle had been recovered and that his vehicle was still missing. All hopes of a rescue had already been dampened, as no one believed the vehicle would be rescued. The job now was to ascertain the damage and formulate payment for the damage, but the investigator responsible for the damage quickly intervened. She knows the vehicle has her iDrive system active and she has asked to track the vehicle. Investigators soon received good news. His iDrive system in the car was still active and the vehicle was being tracked to a specific location in South Africa. The car was recovered with the help of the police. Police also arrested three suspects and seized property believed to have been stolen. There was a suspicion that the vehicle was stolen using the vehicle's duplicate key because the insured was unable to present it at the time of assessment. This raised suspicions that the insured may have been involved in preparing his car for theft. This turned out to be the case, and further network connections were established from the information provided by the arrested suspect. This uncovered other similar staged losses and insurance claims involving these individuals. By cross-referencing known personally identifiable information, we were able to make important connections that aided the process of uncovering the entire network of people and property involved in this organized crime syndicate. Fraud detection solutions and systems should be able to connect these dots.

Submitting the correct documents will not pay the claim. Another common insurance scam is submitting claims in redacted documents, as in the real-life example below. The SIU department was brought in with a stolen laptop and the claim was filed within a month of inception. This claim was triggered by a fraud detection solution. After interviewing customers, some discrepancies regarding losses were identified. He only reported that the laptop was lost and did not report the theft to the police. The loss is said to have occurred in another state and also during a family visit, though contact details could not be provided. The customer was asked to show proof of ownership of the laptop and was presented with the invoice and payment method from her iStore where she purchased the laptop. The customer confirmed that this was done through a bank card and also provided a bank statement to confirm that he purchased this item. A thorough investigation confirmed that the bank statement details provided by the customer did not match the account and had been tampered with. Metadata revealed changes in the content of the document. Shortly thereafter, the insured claimed to have miraculously recovered the laptop and no longer wanted to claim it. I asked for a confirmation of the same invoice as given but the details belonged to a different customer. When we compared the proof of ownership documents with other insurance companies, we found that the documents were scanned in the same way and had the same markings. Also, although the address and profile are different, it turns out that the customer's contact number and email address are the same. After receiving and analyzing all this information, it was confirmed that it was identity theft and that this claim was sufficient to arrest the customer for fraud.

# Prevention against Fraud

After seeing all these carefully planned examples of fraud, you might want to know how to protect your loyal customers and prevent billing fraud. The answer is technology. Proactively detecting fraud and improving analytics before claims are paid is currently one of the top fraud prevention priorities for insurers. As an industry, insurers have become accustomed to detecting fraud at the claim stage or when the claim has already been resolved. Today, analytics and fraudulent claims rules play a key role in identifying potentially fraudulent policies and counterfeit claims. Additionally, data plays a key role in the design of these fraud triggers. Data is extracted, recognized, and branched to identify and analyze behavioral patterns. Without the quality and quantity of data, creating triggers for these frauds and performing proper analysis to further improve already created rules becomes an almost impossible task. As well as a more rigorous evaluation of useful data points, it's important to partner with platforms that enable information growth. The solution is an end-to-end platform with advanced AI-powered analytics that continues to evolve. It helps detect fraud at various stages long before a claim is paid.