SHIFT

SHIFT TECHNOLOGY
# FRAUD INSIGHTS

VOL. 1: APRIL 2020

Welcome to the inaugural edition of Shift Technology Fraud Insights. The work we do — using artificial intelligence (AI) and advanced data science to spot suspicious behavior in the insurance claims process — puts us in an unique position to spot the global fraud trends impacting the insurance industry. Unlike "case of the month" analysis, where a single, or one-off fraud event is broken down, each quarter we'll spotlight schemes affecting larger swaths of the insurance industry. We'll show how they're evolving or migrating, the impact they're having, and how they were identified in the first place. While there's no arguing that a splashy, exciting case can be fun to review, we strongly believe that shedding light on these more widespread scenarios can help insurers around the world better mitigate the risk of fraudulent claims and protect honest policyholders.

In this edition, we'll take a closer look at provider fraud — more specifically, fraudulent activities perpetrated by unscrupulous mechanics and body shop operators. And although — just like the majority of policyholders — the majority of mechanics and body shop operators are honest, some will see the insurance companies as an easy way to make some additional profit on the side. What's interesting about provider fraud is that it's incredibly hard to spot unless you have a sense of the "big picture" of how individual claims may be connected. In this edition of Shift Technology Fraud Insights, we'll explore four examples of provider fraud that offer a view into how some body shops are trying to cheat the system.
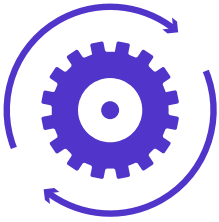
This is a scheme Shift originally identified in France in 2016 and has since migrated to Spain and Italy during the following years.

We're now typically seeing between 10-20 suspected body shops per country per year perpetrating these kinds of schemes, resulting in approximately 800 claims in each geography.

It requires complicity between the body shop and the insured to be successful. In most cases, it's the body shop employee/owner who takes the initiative to suggest participation to their client. From this individual fraudulent activity, we do see that in approximately 50% of cases the scheme becomes repeated, others are recruited to participate and the behavior evolves to form more traditional fraud rings.

The fraud looks like this:

An undamaged automobile is brought into the shop for regular maintenance or other mechanical repair. This scheme typically does not involve physical damage to the car as the impetus for a visit to the garage.

↓

The garage has damaged parts available that match the make, model, year, and color of the automobile just brought in and a proposition is made. Essentially, "I can cover the cost of the repair you came in for if you work with me a little."

↓

While the car is in the shop for the original mechanical repair, the damaged parts are installed and a claim is filed. In some cases, approximately 30%, the shop employee will offer to file the claim on behalf of the policy holder.

↓

The insurer assigns a loss adjuster to the case who can clearly see, for example, significant damage to the right front quarter panel and associated parts. The damage looks legitimate.

↓

The claim is paid and the provider and insured part ways.

It all seems pretty simple. So why is this kind of provider fraud so hard to spot. It all goes back to being able to "see" the patterns that can help claims professionals identify the suspicious behaviors in what, on the surface, may look like legitimate claims.

Unfortunately, it's nearly impossible for an individual — whether claims handler, loss adjuster, or other claims professional — to identify the connections that make up the larger pattern.

This is where AI and data science come into play. Take, for example, the loss adjustor's role. It's incredibly rare for a single loss adjuster to be assigned to a single body shop or garage. If that were the case, this type of fraud likely wouldn't exist. It would become pretty clear, fairly rapidly, that the shop did an inordinate amount of repairs on the same make, model, year and color vehicle, all with exactly the same damage. But single shop, single adjuster simply isn't the reality. Loss adjusters are nomads.

And while they may visit the same garage multiple times per year, they will not necessarily be assigned to enough of the illegitimate claims to see the pattern. Yet, with AI, the pattern emerges quite quickly. Not only can you see that within a single shop a significant number of the exact same repairs (make, model, year, color, and part) are being made, but also that these same repairs happen at a significantly higher rate than for similar shops in the same area.

Interestingly, there are some countries, such as India, that have taken a more proactive approach to stopping this kind of fraud. Local regulations are in place that prohibit damaged parts from being stored by the body shop. All damaged parts removed during a vehicle repair must be destroyed by the shop before the claim can be closed and reimbursed.

Until those requirements become universal globally, we'll want a means to spot this kind of fraud when it happens.

Many body shops or garages look to supplement their income by buying and selling used cars. Others may keep vehicles on hand to serve as loaners customers can use while their car is being repaired. Having ready vehicles on hand has led some owners to use them to drive additional income in a more dishonest manner. Shift identifies approximately 250-300 suspected cases per year of this scheme across the geographies in which we serve clients."

Let's look at this fraud scenario more closely:

Using their loan/used car inventory, the shop recruits drivers — often friends or family — to stage relatively minor accidents with easy to fix damage.

↓

The driver who caused the accident strongly recommends that the victims have their cars repaired in the shop where the "aggressor" car was in inventory.

Yet again, it's not a complicated plot, but it's not always easy to spot without applying artificial intelligence and data science. And much like the "Undamaged/unnecessary repair" scheme, identifying this type of suspected fraud is all about seeing the right connections between individuals and actions.

For example, is there evidence that the individuals involved may know each other or may even be related? Or do these same individuals appear frequently in claims involving accidents where the two cars involved are repaired by the same body shop?"

These are two things that would be difficult to piece together by individuals or even teams of claims handlers working together. And if we apply analytics to the shop itself, do we find any outliers in the number of repairs the shop has historically done, or when compared to similar shops in the area? These are all good indicators that something suspicious may be going on.

Falsifying Windshield Repairs

As insurers expand the adoption of claims automation, straight through processing, and "low touch" and "no touch" claims, body shop employees are increasingly responsible for assessing the veracity of claims. And while the goal of the carrier may be to expedite claims by not sending a loss appraiser to review "simple" claims — such as a damaged windshield, they may be opening the door to increased levels of fraud. For example, Shift's own research indicates that fraudulent claims activity increases by up to 300 percent when automation is introduced into the process. As such, It should come as no surprise that body shop operators and employees may be tempted to abuse the trust they were given by the carriers."

So, how are body shops billing insurers for fake windshield claims? Let's check it out:

Shift is identifying an increasing trend — approximately 3X over the last two years — of body shops simply using policyholder data to report a completely fake claim. This can be done with or without the policyholder's agreement.

↓

Shops are unnecessarily replacing windshields that could be repaired. And since the margin is higher on parts than on labor, it's more profitable.

As with other types of fraud, this can be incredibly difficult to spot using traditional detection methods. Analytics can identify if a shop is conducting a significantly greater number of full replacements vs. repairs, especially when compared against local industry norms.

Analytics can also help to spot whether or not the shop is charging considerably more than peers for the same service.

Unfortunately, we're beginning to see this trend expanding to other covers, which only makes sense. As we highlighted previously, as soon as a claims journey is automated and/or a carrier-employed loss adjuster is removed from the process, new opportunities to easily falsify claims information are created.

This type of fraud may also go overlooked as the body shops with the ability — and permission — to assess damages are often part of the insurer's affiliated network. Thus, it's critically important for an insurer to routinely assess their existing body shop network from both a cost and fraud perspective. For example, are their average repair prices in line with industry averages and is there evidence that fraudulent repairs are being made.

Body Shop Shuffle

Fraudsters do get caught. And when they do, they're often forced to close up shop and may even be prohibited from doing business for a period of time. The bad news, however, is that it can be relatively easy to simply open a new body shop or garage with a "strawman" owner acting as a front. For example, maybe the business is registered in the name of a friend or relative who receives a kickback for lending their name to the paperwork. Now the fraudster is up and running again, and most likely kicking off new fraud schemes. And while this may not be new, the industry does have new ways to combat the "body shop shuffle" thanks to AI.

We've explored how AI can help paint a picture by uncovering connections that an individual would never be able to see on their own. In the case of unscrupulous owners opening up shop under a new name, there are a couple different ways AI can help insurers identify the new potential for provider fraud.

Entity resolution is all about breaking down the information associated with several presumably different individuals to determine if they may all be the same person. When entity resolution is paired with myriad external data sources, it becomes much easier to see the links which exist between the "owner on paper" and the real owner of the shop.

The ability for AI to identify and "build" fraud networks which show the interconnection between several body shops and their clients is incredibly powerful. Do multiple shops share multiple clients? If so, and if there has been an identified fraud scheme, we can deduce those shared clients from the body shops are probably part of it. We can also safely infer that If the same social group is suddenly going to another, recently opened body shop, that we may be dealing with a shop "owned" by a front and is worthy of further investigation.

Insurance fraud is ever evolving. For insurers to stay ahead, they must understand the latest fraud trends impacting their business, and how to most effectively spot and mitigate them.

SHIFT

About Shift Technology

Shift Technology delivers the only AI-native fraud detection and claims automation solutions built specifically for the global insurance industry. Our SaaS solutions identify individual and network fraud with double the accuracy of competing offerings, and provide contextual guidance to help insurers achieve faster, more accurate claim resolutions. Shift has analyzed billions of claims to date, and is the Frost & Sullivan 2020 Best Practices Award Winner for Global Claims Solutions for the Insurance Industry.

Learn more at **www.shift-technology.com**