# Using analytics to detect and address ghost-broking

**Jeremy Owenson,** Senior Vice President
Insurance, WNS Global Services

Insurance fraud costs companies and the insured tens of millions of dollars. In general, it takes several forms

- Consumers take out policies either for money laundering purposes or for obtaining money through either cash back deals or direct debit fraud
- Claims represent an opportunity for either design or opportunistic fraud
- Where insurance is compulsory, such as car insurance, customers may misrepresent their details to obtain a cheaper quote. This is called ‘fronting’.

In auto insurance alone, the focus of this article, fraud is staggering. As per National Crime Insurance Board estimates, auto fraud in the U.S. costs companies an estimated USD 30 billion per annum.

Most motorists buy auto insurance products from agents. Whether or not consumers can verify the credentials of these agents is perhaps debatable.

Increasingly, however, auto insurance is being offered online and many unauthorized agents have used this route to set up fraudulent policies by using false details in order to ensure lower premiums. They then charge the consumer a fee for their service. This new form of fraud is ‘ghost broking.’

Ghost broking typically works this way. A car owner who doesn't want to pay the premium approaches a ghost broker who arranges for a quote by changing key details in order to ensure that the end-user pays lower premiums. For instance, the insured individual's date of birth might be written as 1958 instead of 1985, making the driver a 'safe' 51 instead of a 'dangerous' 24. Or, parents might be listed as the primary drivers of their children's vehicles to avoid young driver premiums.

Because ghost broking is costly for both the insurance industry and the public, insurance companies have begun to adopt various mechanisms that can detect and fight this kind of fraud. These include

- Scrutinizing suspicious claims and referrals by deploying statistical analysis
- Cross-referencing information such as date of birth, marital status, and date of issue of driving license with industry databases
- Examining policy records and quote records to determine especially if one particular address was being consistently used to obtain quotes. Computer IP addresses are also checked to determine if the same computer is being used to post multiple quotes.

These suspect claims and referrals are then referred to a skilled team of investigators for further analysis.

At WNS, the Research and Analytics team was asked by a top auto insurer to review policy and quote data to identify potential ghost broking activities. The team was tasked with identifying polices obtained through ghost broking, gathering information on such agents and finally obtaining accurate policy information to underwrite premiums optimally. The team then

- Studied the motor insurer database
- Collated a ghost broking database
- Cross-referenced policy details with those obtained by ghost broking
- Checked excess exceed claims
- Issued letters to policy holders for clarification and for determining correct premium

- Amended policies after receiving accurate information
- Addressed telephonic queries including complaint calls
- Studied live maps of the policyholder's 'claimed' address
- Referred suspicious cases to a police investigation unit.

The WNS analysis resulted in a number of suspect policies being identified. This lead to a large proportion being cancelled or lapsing.

By deploying R&A, the WNS team was able to demonstrate that ghost-broking can be detected and addressed. If an insurer does not have expertise to tackle this emerging fraud, putting in place an outsourcing plan with a firm that has prior experience can be a cost-effective solution.

To learn more, please write to us at **info@wns.com**