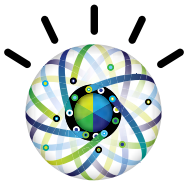


The smarter way to fight fraud

Authors

Adam Bellchambers
Business Development Executive, UK Insurance, IBM

Rick Hoehne
Global Insurance Industry leader for Business Analytics and Optimisation, IBM

At first, it looks like any other motor accident at a road junction, and the total insurance payout amounts to thousands of pounds. Later, it is discovered that both cars were part of a carefully staged collision orchestrated by known players in insurance fraud. Recovering the money will not be easy. In the war against fraud, the criminals are winning.

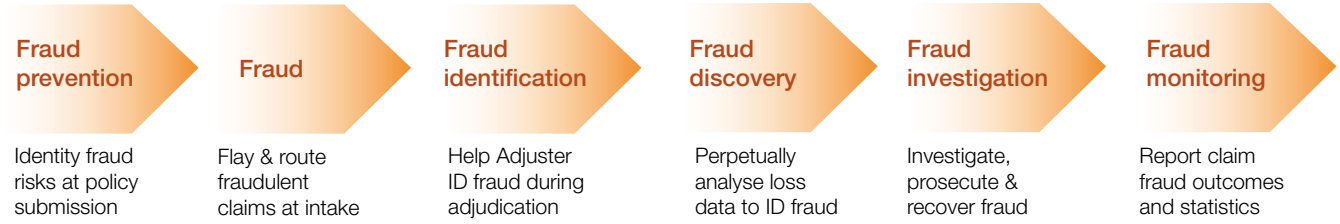
Fraudulent acts against insurance companies are on the rise, and most go undetected. Fraud comes in many forms, from organised crime rings taking advantage of no-fault clauses in policies, to the distressed house owner who sees no other way to pay off the loan, to organised crime rings targeting large retail chains.

For too long, the insurance industry has accepted fraud as a cost of doing business. Historically, finding claim fraud required a significant amount of staff hours that could not be justified based on the returns. However, with combined ratios climbing well above 100, operational costs already cut to the bone, and zero percent interest rates all but eliminating investment income, insurers can no longer accept this cost.

Fortunately, advances in technology and the affordability thereof, coupled with the increasing impact fraud is having on combined ratios, have changed the cost equation. Finding and, more importantly, preventing fraud is now not only feasible, but necessary. Insurers can now implement technology previously available only to deep pocket crime-fighting organisations. Indeed, in discussions with many of our non-life, and particularly motor clients, they name fraud detection as a top investment priority in 2012.

Smarter insurance companies must begin to rethink their claim fraud strategies and attack this problem from a holistic perspective – preventing where possible, detecting when it occurs, and efficiently investigating and prosecuting where necessary.

Change is already underway. The UK's Insurance Fraud Enforcement Department (IFED) opened its doors on 3 January 2012 and "will combat a criminal threat estimated to be costing the UK economy £3 billion per year – adding on average £50 to each insurance policy. The IFED is an operationally independent unit – run by the City of London Police and supported by the Association of British Insurers (ABI) – dedicated to tackling insurance fraud across the UK ... A major priority for IFED will be targeting the organised crime groups at the heart of much of today's insurance fraud."[1]



Targeting fraud across the lifecycle

Fraud prevention is especially effective at two key points: underwriting and claims intake. Fraud can be prevented if the identities, the entities, or the behaviours of the perpetrators buying the policy can be identified. Entity analytics and predictive analytics make this possible.

At underwriting

If the named insured, and/or the vehicle have been involved in previous claims, technology can identify which policies are being purchased for the purpose of conducting a staged accident. In near real time, the script used by underwriters and new business specialists can be changed to let fraudsters know they are exposed. It may not be enough to prosecute, but it might drive them to other insurers with less sophisticated means of detecting fraud. Ideally, in the case of an aggregator sourced business, this level of scrutiny should be applied at the time of interfacing with the aggregator.

At claims notification

The same technology can examine who is who; who is related to whom; and who is doing what in terms of the names of individuals and businesses involved in the claim. Armed with insight about the individuals and intent, one could change the questions being asked of the risk or claimant to determine if they are fraudulent. If the claimant knows that you suspect them, this may be enough to discourage them from proceeding. If it is a legitimate risk or claim, the claimant will consider these questions part of the normal process.

Fraudsters are very good at masking their identities from underwriters. However, the technology can examine hundreds of elements across millions of records to provide alerts, and predictive analytics can look at hundreds of rules and conditions that might indicate fraud – both in near real time.

As an example, Bill Smith may be reporting a claim. BJ Smith was a witness in a separate, similar claim last month, and John Smith was a passenger in a claim three months ago. Each has similar but slightly different addresses and phone numbers, and the same date of birth. By examining these entities, it can be reasonably determined that they are in fact the same individual. The intake specialist might miss this information, but entity analytics will not.

The alert is fed into a predictive engine along with other data to determine if sufficient evidence exists to challenge the person reporting the claim with a few more details. The claims notification specialist can determine whether this is the same Bill Smith involved in a previous claim, or if they would like to update to a single address. Organised fraudsters are sensitive to unusual responses and would be likely to drop the claim and go to easier marks, rather than take the risk that they have been identified.

These two activities alone can dramatically reduce the fraud that is submitted before it even gets to the adjuster, and once it becomes known, can remove the insurer from an organised fraud ring's hit list.

Across the claim experience

A smarter claim fraud program does not stop here. If the claim does reach the claims handler, tools can be attached to existing claims administration systems that assist in analysing a wide array of data sources – both internal and external – including social media and public data, to determine if anything is out of the ordinary. These can be run in the background, reducing the claim handler's workload and providing alerts if an anomalous activity is detected.

Insurers should regularly churn their data looking for patterns and associations in the data. As the insurer becomes more equipped at finding fraud, they will develop a richer set of rules and known networks which will help them identify fraud that has already been reported. This not only helps find additional fraud, but it provides a better set of rules for searches to prevent fraud.

As fraud is identified, modern visualisation and investigation technology can help reduce the time it takes investigators to piece together the elements of a fraud ring – often in an afternoon instead of requiring 18 months of painstaking analysis.

The last element of a smarter claims fraud program is in the reporting, monitoring, and visualisation of claim fraud data. A powerful tool is geo-spatial mapping, where, for example, the ratio of bodily insurance to non-bodily injury claims can be laid out to identify where a fraud ring might be operating. Once identified, the claims can be examined to identify a network of interconnected entities and begin to identify the behaviour rules and individuals involved to alert insurers if they buy new policies or report new claims.

Conclusion

In today's challenged market, insurers can no longer accept the 10 percent of their incurred losses leaked through fraud as a cost of doing business. No longer should the primary defence against fraud be limited to educating the claims handlers on what to look for and staffing a special investigation unit. While these are still necessary activities, they are not sufficient to reduce the significant cost of fraud.

The time has come to leverage technology that is available and affordable to implement a comprehensive smarter claims fraud program that not only identifies fraud, but predicts, and ultimately prevents, fraud from occurring in the first place.

Having sufficient data to prosecute is not always required to prevent fraud. Sometimes just letting perpetrators know that you are aware of them can cause them to shift their attention to easier targets and insurers who do not have the same level of sophistication.

For more information about the authors and IBM's point of view on a holistic claim program, please contact Adam Bellchambers at *adam_bellchambers@uk.ibm.com*.

Adam Bellchambers is IBM's Business Development Executive for their UK Insurance business. Adam has spent his entire career working in and serving the insurance industry.

Rick Hoehne is IBM's Global Insurance Industry leader for Business Analytics and Optimisation. A 25-year veteran in the insurance industry, Rick is a member of IBM's Industry Academy.

---

1 City of London Police, UK's first insurance fraud unit launches today, January 2012: http://www.cityoflondon.police.uk/CityPolice/Media/News/IFEDlaunchestoday3012012.htm

IBM United Kingdom Limited
76-78 Upper Ground
South Bank
London SE1 9PZ

Produced in the United Kingdom

Please Recycle

GBW03182-USEN-00