

Stamping out fraud

While the insurance industry has had some successes in the fight against fraud, this crime has not always received the attention it deserves from insurance firms. Liz Booth explains that sharing information and technology can help reduce insurance-related crime

Fraud is a growing problem for the financial services sector, both in terms of exaggerated claims and in organised crime - and with the latest Association of British Insurers (ABI) study putting the cost of insurance fraud at an estimated £1.6bn, it would be a dream come true if a one-size-fits-all technical solution could be found.

Technology is playing a growing part in tackling fraud, and many insurers have invested in a range of options but so far the magic wand has yet to be waved.

Bobby Gracey, head of counter fraud solutions at loss adjuster Crawford and Company, finds it interesting that the fraud figures continue to rise, despite the massive investment made collectively by the industry in trying to reduce the risk.

"As an industry, we are getting more sophisticated about management information," he says, "but the mistake businesses have made is that when they buy a system, they need to ensure it fits with their own operational requirements."

Without a proper fit, he believes any money spent on a system will be wasted. Instead, he is a great believer in the 'human touch', and Crawfords invests large amounts of time and money training its staff to spot anomalies across all areas of the business.

He adds: "Systems will only point out a problem, they will not provide a solution. We work in a people industry, and it is people who are needed to solve this."

Common stereotypes

Crawfords has also undertaken its own research using information garnered over the years from its clients, which Mr Gracey says has thrown up some stereotypes. For example, fraud is more prevalent between May and July, and fraudsters are also less likely to give claims handlers their mobile telephone number, preferring to keep a distance between themselves and the insurer.

However, these are huge generalisations, and the issue of false positives is a challenge for the industry - people cannot be labelled as a potential fraudster just because they make a claim at a certain time of year. Scott Clayton, claims fraud and investigations manager at Zurich, also believes that the key lies in training people to be aware of the issue. He says that one of the biggest problems in the use of technology is that, within the ABI figures, it is clear that there are two types of fraudster - organised criminals and opportunists.

Mr Clayton welcomes the initiatives of the Insurance Fraud Bureau (IFB), which celebrates its first anniversary, saying it has done much to challenge organised gangs. This is because insurers are able to share information anonymously, helping investigators identify types of frauds and the criminals behind the operation. Data is then shared between members to help prevent such scams happening again. "However, detecting exaggerated claims mostly relies on gut instinct," he adds.

Although the danger is that fraudsters are becoming more cunning. David Hicks, head of insurance forensic at KPMG, says that finding a fraudster is like looking for a needle in a haystack. He believes that technology helps to reduce the amount of 'hay' and, therefore, increase the proportion of 'needles' left for people on the ground to find.

He says: "Two organisations may be linked and carrying out the same fraud but be separated by 10 people. Technology can help find this link, and then insurers can be warned so that they can stop the second gang."

Unified approach

Mr Hicks believes that a unified approach would be useful but that firms can operate independently and do much to reduce their risk. "The industry recognises that it is a collective issue, and the IFB has been very successful - but it is not just an insurance issue. Sharing knowledge across financial services could be employed. If someone has a propensity to commit credit card fraud, then they are likely to have a propensity to commit insurance fraud as well," he says.

Mihir Pandya, fraud manager at Allianz Insurance, is a huge supporter of the work of the IFB in terms of tackling the problem of organised gangs. He explains that data sharing can work in this way because the source remains anonymous, and the whole industry can benefit from the information.

Mr Pandya says the company has trailed several products and has found that "technology can only work behind a very strong team". He believes the odds of technology helping to find a first-time fraudster are as good as if the claims handler "tosses a coin", although technology can help narrow the field, which then enables investigators to operate more effectively.

Many technology providers have developed their software for other businesses, and then have found it useful in the battle against fraud. For example, ACL developed its software as an audit tool and has been supplying its products to insurers for several years.

However, Liz Maloney, ACL's regional director for Europe, the Middle East and Africa, explains that it has recently been used to collect information that can then guide claims handlers. As its customers become more concerned about the problem, ACL has started to host special interest group meetings. The last meeting, held in February, gave insurers an opportunity to discuss their problems.

Ms Maloney explains that the meeting covered collaboration, and there was clearly a willingness to support the IFB initiative and to share information. She says there was also a realisation that while there is sharing of information at a corporate level, this is not always filtering down to managers on the ground.

David Carrick, chief executive officer at Memex, adds that many solutions lie within organisations themselves. "Fraud prevention tends to be department focused, and firms are not making use of the information around the home organisation. Many of these insurers are global, and they have information in other parts of the world. There can be language issues and also legislative restrictions about where information is held but they could be making more use of it," he says.

Mr Carrick cites a recent case in which enforcement officers had given a company information, and it took a further two weeks for the company to check its own records to see if it was relevant. "This is simply too long," he says. "In that time, the company could well be a victim of a preventable fraud. Technology can help speed up those checks, and then spread the information throughout the organisation."

Tip of the iceberg

However, Mr Carrick believes the ABI figures are the tip of the iceberg. "You only hear a small proportion of what goes on," he says, although he welcomes the increasing numbers of former law enforcement agents who are now being employed by the insurance industry. "Insurers are about providing a quote and policy and then paying out claims when needed. Tackling fraud is about investigation."

Mr Carrick explains that technology can play its part: "Insurers need confidence in the quality of the data available, as it will help reduce the false positives. Some organisations have been quite naive and almost expect the system to flag-up the fact that 'this is a bad person'."

To make the most of the technology available, Mr Carrick says that the data used needs to be reliable and firms need to invest in skilled analysts. Only then will the information gathered give an insurer's claims team the best opportunity to spot frauds before it pays out.