neural technologies

## WHITEPAPER

# Insurance Fraud in the Digital Age

## Why advanced data analytics and the exploitation of Big Data are key tools in counter fraud control

### Neural Technologies

The global insurance industry is the world's largest business sector with annual worldwide revenues of $4.6 trillion and a portfolio of $25 trillion in assets under management, according to Berkeley Lab. In the UK alone the insurance industry accounts for 7% of all global premiums and it is thus the largest in Europe and the third largest in the world.

Insurance fraud is also a worldwide phenomenon and the UK's National Fraud Authority in its Annual Fraud Indicator 2012[1], puts the cost of insurance fraud in the UK at £2.1 billion. The report also states that organised insurance fraud, targeting particular products, is becoming more commonplace. These organised frauds are described as complex and difficult to investigate and they often involve collusion by professionals (for example, legal, medical and claims practitioners in the case of fraudulent personal injury claims) some of whom who may feature regularly.

**The insurance fraud landscape**

Exposure to most insurance fraud falls into four categories:

- False claims
- Exaggerated claims
- Multiple claims
- Inflation of asset value

A great deal of insurance fraud involves opportunistic responses to unexpected events such as accident, fire or flood, as well as deliberate damage to property in order to support a claim, but organised claims fraud is a growing part of the whole.

In 2011, Legal & General's Steve Phillips, Head of Fraud Services, commented in that firm's annual Fraudstoppers Report that, "One of the biggest challenges facing insurance companies, and affecting consumers, is home insurance fraud. It has long been a concern of myself and many of my peers working in the industry that insurance fraud is not regarded in the same light as theft. Amazingly many people don't associate exaggerating home insurance claims or falsifying claims as fraud. The term fraud seems to be reserved for major swindles or billion pound corporate frauds."

Legal & General's report also cites the work of the Association of British Insurers which reported that Insurers are detecting more fraudulent insurance claims than ever with over 2,000 dishonest insurance claims worth more than £16 million being reported weekly during 2010. The value of these claims, at £840 million, had risen by 14% on the previous year.

It seems clear then that there is a growing level of concern about insurance frauds ranging from opportunistic individual frauds to highly organised cases perpetrated by people with considerable expertise and knowledge of the workings of the industry. This presents firms with a very broad set of challenges.

1 Source: www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/annual-fraud-indicator-2012?view=Binary

# FACT SHEET: INSURANCE FRAUD IN THE DIGITAL AGE

## The Robin Hood Syndrome

False and exaggerated claims have always been driven in part by public perceptions that it is acceptable to take something extra back from a big corporate organisation like an insurer. Legal & General, for example, found that 29% of people surveyed in the UK feel it is reasonable to exaggerate a home insurance claim, for example by adding extra items or increasing the value of the claim. As we go increasingly online and as face-to-face contact between providers and policy holders declines, this rationalisation of theft can only become more significant as a driver for fraud and, of course, the vast size of the industry doesn't help matters.

'Up-raiding' is another fraudulent practice that involves making false claims in order to upgrade home appliances and other electronic equipment such as mobile phones and tablets. Men are twice as likely to do this as women and there is clearly a link between this finding and the observation that excessive force is a frequent indicator of fraud as many gadgets are more durable than consumers anticipate when they first set out to damage them.

Some retailer policies exacerbate this risk. For example, the latest Kindle Paperwhite is sold along with an Instant Replacement Care Plan that states, "Unlimited replacements for breakdown and mishaps (exclusions may apply)". While the exclusion clause provides some protection to the insurer, the wording of the policy, which is often exacerbated by the comments of sales staff, certainly gives the consumer the impression that a blind eye will be turned in the event of 'mishaps' that put them in line for the next generation of the device.

This tension between fraud control and marketing is nothing new and in the device market it is a challenge that telecoms operators have been faced with for decades. Indeed, the telecoms industry has been managing complex consumer and organised frauds through the analysis of big data for many years and, it may be argued, probably possesses the most advanced systems and the deepest expertise on this front of any industry.

## Proactive fraud control

The industry already employs advanced proactive controls designed to detect potential fraudsters during the applications process. While these techniques are continuously evolving, and some of the latest are understandably confidential, the following highlights provide a good sense of the overall approach.

- Referencing of applicant details against industry-wide Watch Lists such as that maintained by the Insurance Fraud Bureau, as well as internal company watch lists and intelligence databases, is conducted systematically in order to identify known fraudsters at an early stage in the application process.
- Checking patterns in stored data to establish whether applicants have made numerous quote requests over a prolonged period of time can also help to detect people with criminal intent, although not all people who fit the profile will in fact be fraudsters.
- Checking of current applicant details against previous applications for changes, such as a reduced number of driver penalty points, a different job title or an altered date of birth can also highlight risky accounts.
- Graphing (also known as 'link analysis') and fuzzy matching to spot small changes in spelling or other details are employed to produce matches or maps of data connections that might indicate deception or collusion.
- Weighting of selected fields in applicant data records is also employed as a means of reducing false positives (false alarms). Any field that would normally have a big influence on the premium quoted is weighted more heavily, as it is in such fields that fraudsters are most likely to enter false or deliberately misleading information.

For each of these an applicant can be given a risk score according to the severity of the findings, leading to an accept/reject/defer decision.

# FACT SHEET: INSURANCE FRAUD IN THE DIGITAL AGE


## Fraud indicators or 'Red Flags'

Extensive 'rules-based analysis' is also employed to detect both potentially fraudulent applications and fraudulent claims later made by successful applicants. While known fraud indicators do not prove fraud, they are an essential tool for profiling and scoring claims in order to focus limited resources on those more likely to be fraudulent. A list of some key indicators includes:

**The Claimant(s)**

- Inaccurate/incorrect personal data
- Vague employment information
- Customer contact event logged shortly before the incident (e.g. to confirm cover)
- Evidence of financial difficulties
- Stated income does not match value of item(s) (e.g. living beyond their means or inflating value)
- Extensive claims history

**The Cover**

- New or recently renewed insurance cover
- Insured recently raised cover
- Profile of the device used to take out the policy:
    - IP Address
    - Operating system
    - Language settings
    - Device clock setting
- Website visit profile during purchase shows familiarity with process

**The Incident**

- Geo-location of the event
- Type of damage or personal injury
- Extent of damage is excessive given the cause stated
- Number of passengers in a vehicle (may indicate numerous false claimants)

**The Item**

- Age of item lost or damaged
- Known condition of item prior to claim (e.g. vehicle or vessel repair history)
- Relative age and value of vehicles involved in accident (e.g. one very old and one very new, high value)

**The Claim**

- Device profile used to log the claim
- Familiarity with the claims process
- Claims are preceded by a recent customer query about their cover
- Website visit profile during claim also shows familiarity with process
- Type of claim conforms to known or suspected fraud patterns
- Claim value is relatively high or low vs. average claim values for claims of that type
- Undocumented personal property included in the claim
- Claimant prefers lower settlement in lieu of producing additional evidence
- Numerous people with different surnames in a claimant's vehicle are:
    - Treated by the same doctor
    - Have the same injuries
    - Are represented by the same firms
- All the injuries reported are subjective – headaches, whiplash, soft tissue

**Other**

- Missing Police Reports
- Social network, name or address links between claimants and independent witnesses
- Contradictory online information (e.g. Social Media posts)

Much of this analysis relies on the human user, but a great deal can also be automated, or supported by various automation techniques. Link analysis, statistical analysis and geo-location mapping can all be employed to enhance the investigative process.

## Fraud Probability and Investigation Profitability

One core objective of technical approaches to fraud control in any high volume transaction environment (e.g. financial services, communications/data and eCommerce) is to reduce the gap between Fraud Probability and Investigation Profitability, thus leading to improvements in solution rates.

Fraud probability is expressed by scoring the Red Flags to produce risk scores at event, case, claim or account level to facilitate sorting by score. Investigation profitability puts a mathematically derived estimated financial value on each case based on its complexity. By combining the Probability and Profitability values it is possible to select a set of events or accounts that are more likely to be fraudulent, but which can be investigated cost-effectively.

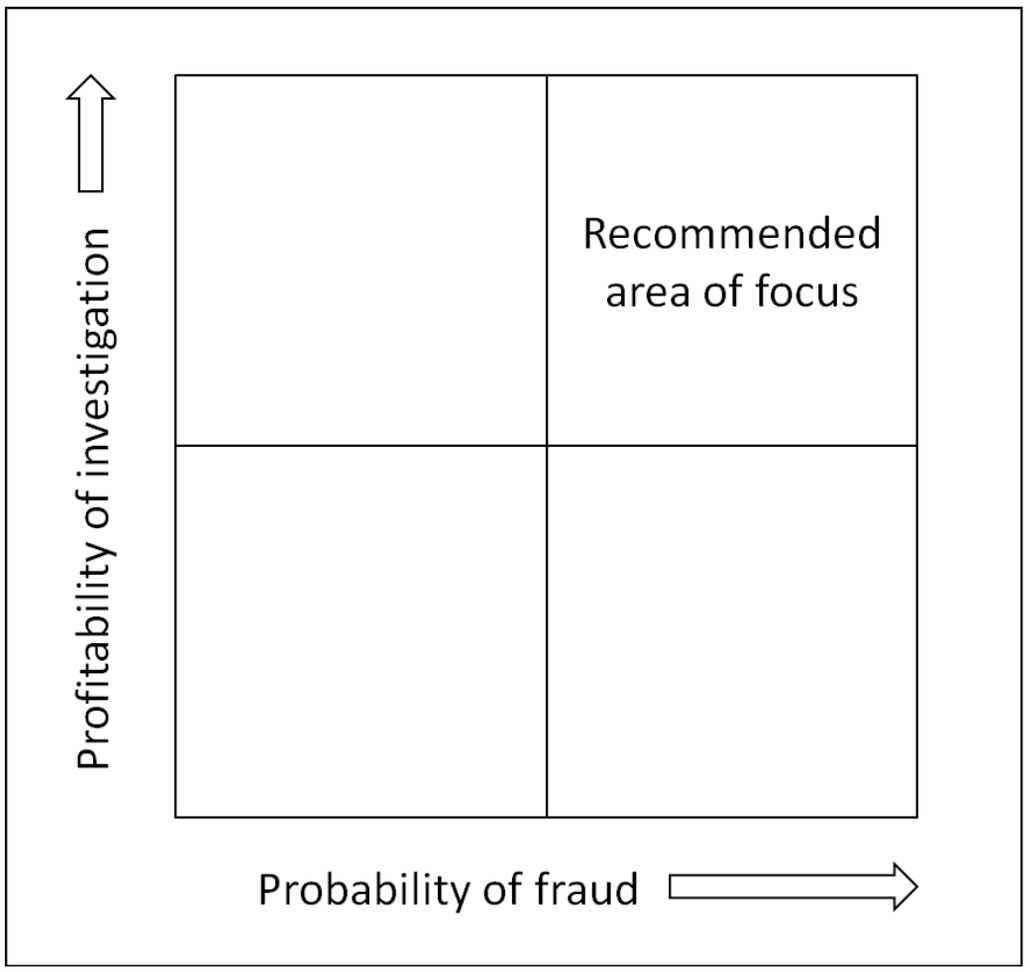


Diagram 1. Showing the conceptual relationship between Probability and Profitability.

**Risk Control**

Any strategy for managing fraud risks must take into account the operational realities of today, as well as the expected landscape of tomorrow; it must be both practical and flexible. The pace of change in the online world, with the ongoing transition to mobility, ubiquitous broadband access and the extension of identity management beyond the individual to the device used, throws up both challenges and opportunities for fraud managers. We apply six principles to the development and maintenance of a modern fraud control strategy:

1. Adapt fraud management strategies to keep up with the changing environment.
2. Ensure that fraud operations are closely aligned to regular assessments of Risk.
3. Ensure that changes in the operating model are matched by changes in the fraud control model.
4. Exploit new information sources, but with a focus on quality and ethics.
5. Make full use of available tools and analytics techniques.
6. Exploit the value of Big Data.
7. Invest in expert teams able to adapt to change, make full use of the tools provided and deal with an ever more complex set of fraud challenges.

Complexity is both a challenge and an opportunity. It makes the investigative process more challenging, but it can also provide many new links between data elements that allow appropriately equipped fraud investigators to map cases and networks in ways that would otherwise not have been possible.

## Data analytics and online investigation opportunities

There are opportunities for technical approaches to fraud detection and investigation as well as ongoing requirements for manual processes. It is important that firms recognise the need for both approaches and develop realistic expectations for the former.

The table below provides a few examples of where some of the main technical opportunities might lay within the typical firm. Actual implementations need to be guided by subject matter experts and, because they depend heavily on the type and format of data available, they will differ between installations and vendor systems.

| Red flag | Analytics | Link analysis | Geo location | Online enquiry |
|---|---|---|---|---|
| Claimants | Y | Y | | Y |
| Cover | Y | Y | | |
| Incident | Y | | Y | Y |
| Location | Y | | Y | Y |
| Items | Y | Y | | Y |

Table 1. How different lines of technical enquiry might apply to various facets of any suspected fraudulent insurance claim.

## Conclusion

It almost goes without saying that insurance fraud schemes extend to cover all industries and sectors, from transportation to telecoms, and from oil, gas and renewables to finance, the markets, trade and commerce. Nevertheless, the principles of data collection, processing, analysis and dissemination remain constant and, in an increasingly convergent globalised marketplace, automation and standardisation of approach have never been more important. Indeed, it seems self-evident that without advanced data analytics and the capacity to exploit Big Data, firms cannot hope to adequately confront the threat and secure their margins.

---

Extracted from the upcoming book 'e-Crime' being written jointly by Mark Johnson and Neira Jones and published by Gower Publishing.

www.trmg.biz/publications/books

Neural Technologies · Ideal House · Bedford Road · Petersfield · Hampshire · GU32 3QA · UK
T: +44 (0)1730 260256 · F: +44 (0)1730 260466 · E: info@neuralt.com · W: www.neuralt.com

neural technologies