FC Business Intelligence

The Role of Data and Analytics in Insurance Fraud Detection

FC Business Intelligence

The Role of Data and Analytics in Insurance Fraud Detection

With contributions from:

Taşkın Kayıkcıoğlu, AGM, CIO and Member of the Executive Committee, Groupama

Ben Fletcher, Director, Insurance Fraud Bureau

Roland Woerner, Global Head of Counter Fraud, General Insurance, Zurich Insurance Group

Steve Jackson, Head of Financial Crime, Covéa Insurance

Richard Collard, WW Business Development, Fraud Analytics, IBM

Disclaimer

The information and opinions in this document were prepared by FC Business Intelligence Ltd and its partners. FC Business Intelligence Ltd has no obligation to tell you when opinions or information in this document change. FC Business Intelligence Ltd makes every effort to use reliable, comprehensive information, but we make no representation that it is accurate or complete. In no event shall FC Business Intelligence Ltd and its partners be liable for any damages, losses, expenses, loss of data, loss of opportunity or profit caused by the use of the material or contents of this document.

7-9 Fashion Street, London, E1 6PX

www.analytics-for-insurance.com/

Author
Geoff Whiting

Editor
Helen Raff
helen@fc-bi.com

The Role of Data and Analytics in Insurance Fraud Detection

Overview

The rise of analytics presents a world of almost limitless potential for industries such as insurance where companies have long held a foundation of information. The industry at large has had a slow adoption of new Big Data analytics because of cost concerns, and regulation may be the limiting pressure of the future.

In the past, fraud detection was relegated to claims agents who had to rely on few facts and a large amount of intuition. New data analysis has introduced tools to make fraud review and detection possible in other areas such as underwriting, policy renewals, and in periodic checks that fit right in with modelling.

The role this data plays in today's market varies by insurer as each weighs the cost of improving upon information systems versus the losses caused by current fraud. This often comes down the question of: is fraud creating a poor enough customer experience that infrastructure investments will improve fraud detection and improve honest customer claims processes?

Protection of personal information is paramount, but fraud pattern recognition requires a large amount of data from underwriting, claims, law enforcement and even other insurers. Each new piece of legislation has only made the protection hurdle higher when integrating these sources.

Once this data is collected and properly utilised, insurers must consider if it is accurate. Modelling often relies on past behaviours for fraud predictions, but criminal practices change quickly enough to make some of this analysis worthless. Assessing data quality has become a struggle.

While analysis has proven a difficult task to master, today's insurers are seeing many benefits. Fraud detection has improved and systems are now robust enough to provide analytics in real-time. Some insurers have gained the ability to scan for fraud before a policy or claim is approved, pushing Big Data from a siloed fraud unit all the way to agents in the field.

The future of fraud detection, however, cannot be via a pure analytics approach. The human element in assessing risk will remain a vital piece of proper detection. Data can hasten the detection of fraudulent activity and patterns, but people will always be required to turn reports into actionable intelligence.

Setting the Stage of Today's Market

The illegal activities that encompass fraud are first and foremost a detriment to the financial stability of each insurer, but the harm caused is much more far-reaching.

These deliberate acts have a long-term impact on all operations of an insurer. Fraud losses and risks can lead to price increases for loyal customers as well as introduce additional time and review before insurers pay legitimate claims. This increased scrutiny of honest customers is only visible when they feel most vulnerable and are in the greatest need of the insurer's services.

Pressing customers in such a vulnerable position can create significant harm to reputation and trust, risking increased policy turnover.

Fraud detection units and internal auditors typically manage most of the data and systems used to store and process fraud detection. As automated processes become more in-demand, IT has a bigger role to play within the fraud unit. The availability of real-time services will further the importance of IT in budgets and decision making.

Regardless of an IT or fraud background, team members must be well-trained to understand the modern threat. As many units are still growing to scale, team members are pulling double-duty as both IT experts and fraud analysts.

The Face of Today's Fraud

In Europe, fraud is largely gang-related, so the focus is typically on third-party instead of first-party fraud.

Fraudsters pursue the path of least resistance and this eventually shifts to areas where there is less fraud detection. Analytics engines that aren't applied across an entire organisation may indicate where fraud will shift to, such as pet care divisions for some insurers.

Ghost-broking is also a growing area of fraud and tends to stick to one type of insurance product. Analytics engines can help identify some of these areas and establish patterns to help the market identify concerns before paying a claim and potentially before a claim is filed or policy issued.

"The success of an individual fraudulent claim depends on the fraudster's ability to present that as a genuine, unique occurrence. Obviously frauds have common traits, and these can be determined through data sharing and analytics," said Ben Fletcher, Director of the Insurance Fraud Bureau.

The What and When of Data Availability

Most insurers have a huge repository of existing data in terms of historic claims and policy information plus a steady stream of new claims and application data. Insurers work with law enforcement to share some information; however EU law as well as country laws significantly limit what information can be shared among insurers.

Much of this data is typically used to validate what's being told by the claimant and what is being processed. Insurers not only look for red flags in terms of conflicts but they also look for connections to organised crime.

Insurers today look for fraud in new policies and then review information when there are policy changes. Touch points that cause a review include coverage shifts by insurers, new claims, changes by the policy holder, and during policy renewal.

"Sometimes not all needed data is available and the quality of the existing data is partly poor. We have to find the right balance in reducing data volumes and gathering the best data for effective analysis," said Roland Woerner, Global Head of Counter Fraud at Zurich Insurance Group.

However, the market is improving. Unstructured data has become an opportunity instead of a problem. Many insurers have the ability to change unstructured information into structured data and actively mine this for the opportunities available therein.

"The challenge with some data is that some brokers are not always willing to give all of the information that insurers' fraud detection units would like, such as contact information. Email addresses and phone numbers can be essential to identifying links to fraudulent activity," said Steve Jackson, Head of Financial Crime for Covea Insurance.

Existing Operations and Obstacles

To a large extent, Big Data analysis is being driven by IT imperatives and not mainline business operations. Analytics are often introduced on a project basis and, if benefit is shown, then analytics platforms are expanded to more divisions.

Insurers may implement these techniques in marketing or other customer service areas first, but fraud detection units benefit from the tools and analysis just as much. The main point for the introduction of analytics in a business sense is determining its present value and building the case for a consistent return. It becomes a people plus power equation.

"For claims fraud prevention and detection, an insurer needs a highly professional organisation, and the best people capabilities supported by excellent data analytics," said Woerner.

These professionals can help companies make full use of core systems and external sources such as the common fraud database provided by Insurance Information Centre. To avoid data concerns, "required fields should be matched and accuracy of the fields examined step by step," said Taşkın Kayıkcıoğlu, AGM, CIO and Member of the Executive Committee at Groupama.

Fraud Systems from Silos to Ever-Present

In the past, systems were unable to speak together and often were siloed because integration technology wasn't available. Today, every insurer will be slightly different as they move to new services, so some insurers have legacy problems while many others have robust systems that can pull data from multiple sources.

Unfortunately, even insurers who have made significant investments are still operating with some silos because of concerns over improper information sharing within departments.

For many customers, the information they provide can only be used by the department responsible for their policy. This means an auto policy division cannot access much information collected by a homeowner's insurance division. While data sometimes may be collected and processed en masse, insurers must make sure that results and other information are not passed along improperly or without consent.

"Many legacy systems lack detail and this is compounded by the fact that some departments still work in silos. This means that disparate pieces of useful information about an entity are rarely pooled; but if they could be, we would create a single accurate impression. Many analytics solutions use mapping layers, which helps fraud departments pull in multiple data streams, either internally or externally, into a consolidated view. Of course, this does nothing to ensure that data is no longer siloed by other departments," said Jackson.

The Holistic Fiefdom

Claims investigation units typically hold the data for fraud detection, so they have a necessity for systems integration. Unfortunately, many organisations still have a fiefdom and this precludes a more holistic view of the complete fraud threat that exists today.

Data-focused insurers are struggling to unify information around the touchpoints of claims and underwriting. This operational convergence is of the utmost importance.

The conversation still comes back to three main questions that insurers must answer for their business models:

- What are the costs of advancing data analytics to the organisation?
- Are fraud losses today creating a significant burden for current or future operations?
- Is fraud creating bad press or making the customer experience poor?

As a whole, insurers believe they have a control on the industry and its fraud, even with the slow pace of adopting new technologies. Insurers who adopt a sense of urgency around data diligence are finding it to be a significant point of distinction for their customers and their bottom line.

"It comes down to: how little can they spend to give the impression of excellent customer service and maintain capabilities," said Richard Collard, WW Business Development IBM i2 Fraud Analytics. "Insurers too often take a Band-Aid approach to an infrastructural concern."

It may take pressure from state regulators for the industry to adopt new services on a broad level.

Model Citizens and Model Concerns

"I think today we're looking at a change in behaviour and the propensity to commit fraud," said Collard.

Behaviour changes represent a challenge to insurers because behaviour modelling currently trains and bases predictions on past, identified fraud practices. Many of these models have not been relevant in recent years because the prediction data they're using is simply too old.

The established belief that models must train for future behaviour based on past experience took a significant hit during the financial crisis. However, it has been beneficial for insurers and other industries to see this hole.

"There are always challenges around data quality. It's a perennial problem," said Jackson.

Insurers and their fraud teams are starting to regain ground and learn what new behaviours look like to respond to fraud. Predictive analytics is playing a stronger role as is entity analytics, the understanding of who an individual is and if they are who they claim to be. Analytics engines can now run these checks and raise concerns during the on-boarding process.

"The single biggest challenge is putting in the appropriate controls and team to ensure that you find the fraud but that you don't disrupt the customer experience in the process," said Fletcher.

Beyond speed, the safety and security of the information itself is paramount.

Data Safety and Disclosure

"Everything we do is through a secure connection. I wouldn't say we're paranoid but we're very conscious about data security. Anything that leaves us goes through a secure connection," said Jackson.

A separate fraud department exists in today's insurer and this unit typically holds all of the data being used for detection. Data from multiple sources, such as claims and underwriting, are syndicated and sent to the fraud team that then does its analysis on-site.

Holding the data in a separate location allows the fraud team to enhance, modify, and update data safely and securely. This also helps a fraud team keep data only on internal systems and away from Web-based risks. Insurers take a significant blow to credibility when any data is lost or stolen.

While the data is being managed by fraud detection, it is up to individual agents throughout a policy's lifecycle to ensure that policy holders give their consent for data to be analysed. This has led to overt disclosure that data will be monitored for fraud and that any discoveries will be shared with authorities.

"Transparency is important for credibility of anti-fraud activities. It's one of our fundamental priorities to keep our honest costumers informed and it's part of our fraud prevention approach," said Woerner.

The industry is hoping to expand this type of sharing to new data as it is collected. For fraud detection, "image recognition and voice analytics will be used in near future. For example, one photo can be used for multi-claims, it should be prevented technically," said Kayıkcıoğlu.

Overt disclosure has also had a chilling effect on some fraudulent activity.

"Now, there's a strong chance that they're not going to commit fraud unless they're organised criminals – then they don't care," said Jackson.

Does Fraud Detection Get in the Way of Other Business?

Fraud units have three main goals:

- Detect fraud and pull potential fraudulent claims for in-depth review.
- Return non-fraudulent claims back into the claims cycle so honest customers are not upset.
- Perform the first two operations as seamlessly in the business cycle as possible.

Many insurers are now capable of performing analysis with Big Data to quickly flag or validate claims. The automation process focuses on this speed and, overall, the industry is at a place where it can claim that very little gets in the way.

"On the whole we don't face any real problems with interrupting the cycle on a genuine claim," said Jackson. "Nothing gets in the way of the claim when we can help it."

"Taking an attentive approach to fraud and associated costs means we are able to protect our honest customers and continue to provide them with the best possible insurance cover now and in the future," said Woerner.

New innovation is helping to speed up the fraud processing of data and other services. Some providers can even process information and provide an initial analysis while a person is in an office signing up for a policy. Agents can often get a real-time approval or denial from an initial claims unit review.

Is Real-Time a Necessity?

When discussing Big Data and analytics in a broad sense, there is typically a business-case emphasis on real-time functionality. In the insurance world, real-time processes are the preferred approach for operations, but they are not a necessity for analysis once potential fraud is determined.

In the application screening process and pre-sales decisions, real-time analysis is desirable for most policies. Here, insurers are struggling to balance speed with thoroughness. The ultimate goal is to avoid the need to look for fraud after an insurer has made a sale.

However, this is mainly a propensity modelling concern, not a complete search for fraud. This modelling is used to determine the likelihood of a new policy holder to commit a fraudulent act, and it can be done in real-time.

Routine checks don't have any need for lightning-fast speed, reducing the computing requirement and overall cost of analytics programs. Again, insurers are likely deploying propensity models as new information is uncovered or databases are updated.

In claims, insurers again want service to be as close to real-time as possible to maintain the best level of customer service. Here and in policy origination, if fraud or a potential for fraud is detected, the need for real-time decision making is reduced.

Insurers want to take their time when reviewing cases for fraud, so it is okay if the process becomes longer and more involved after a red flag is discovered. "We've found quite a bit of fraud based on this kind of approach," said Jackson.

Police Under the Insurance Umbrella

Insurers are taking a more prominent role in community monitoring by working with police to fund specific units for fraud enforcement.

Last year, the Association of British Insurers announced plans to invest £11.7 million over three years to help fund an expansion of the Insurance Fraud Enforcement Department within the City of London Police.

Additionally, groups like the IFB help UK insurers to detect fraud rings and have reduced some informational barriers. Information must flow directly to the IFB and not to other insurers, which some insurers say dampens the ability of their in-house teams. However, this type of system-flow could be a benefit to the industry as a whole.

Current fraud police units also have limited data-sharing back to the insurers. Much of their work is predicated on information provided by the insurance companies, but English laws prevent a proper back-flow of information to help all insurers learn new warning signs.

Information resting solely in the hands of law enforcement keeps a strong impetus out of the market. If all of this information were made accessible to insurers, they would naturally write systems and software to share and collect what was available. This sharing would be one of the strongest driving forces behind creating a common language for insurers' systems.

It's All Binary to Me

A system run by law enforcement is inherently rigid and the industry would need to conform to access data it makes available. This could create a significant third-party market for software development and/or a rash of in-house development that would potentially work across insurers.

"Understanding a common language will be an Esperanto for fraud investigation, which can only be a good thing," said Collard. As the language provided better channels to discovering new fraud, insurers would focus on aligning more of their processes with this new language. "Success breeds success."

The Acquisition Model

Many major insurers in the European Union have made significant size growth by leveraging mergers and acquisitions. This creates a unique problem for the adoption of big data initiatives by creating multiple databases that an insurer has access to.

On its face, having multiple datasets seems like a boon. In fact, using multiple datasets is an established best practice of fraud detection. However, the problem is that these datasets are not guaranteed to have a similar architecture and may not integrate properly.

Since these systems are typically not the focus of an acquisition, they are often used in tandem instead of combined. This holds the insurer back by creating multiple views of the customer.

"On this basis, it's very difficult to create the 'Holy Grail' that is a single view of the customer," said Collard.

To address these issues, insurers must make fraud detection and analytics part of their core business rules and development. "We combined all (business) rules in the company and put mathematical modelling on this data, and got the necessary accuracy to find fraudulent cases with a 72% success ratio for 20% of all claims," said Kayıkcıoğlu.

Understanding Legacy Systems

Requirements of today's data analytics often include an upgrade on some systems, but fraud detection units have largely maintained an IT budget that has allowed them to stay up-to-date.

The real concern in terms of systems is the use of a third-party service or software because privacy protections and concerns lay at the feet of an insurer. Not having absolute control causes worry at the very least and a significant liability at the worst. Third-party systems also lack enough customisation to make insurers feel absolutely comfortable.

"One would've hoped that the EU would have standardised approaches to data protection to actually share data. It's actually gone the other way for us. It has created a far greater protection of individual's rights. This drives insurers and other institutions to continue to work in silos and that's where the fraudsters pick us off," said Collard.

The Future

Why Is Today's Fraud Detection Different?

Fraud detection has changed in its location relative to the insured. Insurers are now able to run predictive and entity analytics during multiple touch points, essentially as each new piece of information is added.

This not only improves detection capabilities in the event of fraud, but it also allows an insurer to assess a fraud-risk. Some have begun providing risky policy holders with high-priced policies in order to drive them to other service providers.

The insurer today has moved away from a purely reactionary stance to a proactive effort to keep bad business off of its books. Insurers are seeing the financial benefit of enacting large efforts to keep fraudulent activity completely out of the business cycle by identifying it during signup.

"The move from reactively looking at data and intelligence at a practitioner level, to using analytical tools to proactively look for trends and patterns at an industry level has been the single biggest step forward from the IFB's point of view," said Fletcher.

Beyond this shift, much of current evolution is around communication and it presents a clear opportunity for moving forward. The future is about collaboration with brokers and other outside parties as much as with other insurers.

"We need to be a lot more open about this information so we can do the proper analytics. The fact that we haven't got information isn't an obstacle because most of it can be found with a little bit of research. But, if it's something that the policy holder is trying to conceal – such as publicly available phone numbers being different from what they've given their broker – then it's a potentially missed link or signal for fraud," said Jackson.

Blending the Art and Science

While analytics engines may get much of the coverage, the successful fraud detection unit of tomorrow features a very well-educated staff.

"The more data we capture and the more detail we capture, the better we can refine these models. But, there's only so far we can go with probability," said Jackson.

Fraud professionals are being asked to step up to the plate like never before. They have access to more data and increasingly strong ways to manipulate it. Staff will need to be trained in these systems as well as new fraud tactics.

"A strong emphasis on technical excellence guides us on how we approach fraud prevention and look after the long term interests of Zurich and our customers," said Woerner.

Insurers want to automate the fraud process as much as possible to weed out as many proper claims and false positives as possible. At the end of the day, however, any flagged accounts still must be reviewed by a person.

A well-trained team can improve models by determining what normal behaviour is and what fraudulent behaviour is. It's the narrowing of the funnel from machine analytics on a large level to individual attention for final review.

"We will never remove this from the human domain," said Collard.

Where Is The Market Headed?

Use of analytics for fraud detection in insurance is essential to the future viability of the market.

For new technologies, there is a significant push in the underwriting process where rules and procedures can be applied before a policy is issued. "Technically, handwriting scanning, image processing and smart phone capabilities like geocoding and XDIF information can be used for advanced fraud solutions. We are working with some R&D centres for these purposes," said Kayıkcıoğlu.

However, there is no mad rush to adopt new third-party technologies or shift infrastructure. Recent market events have made this image much clearer than many would have thought at the turn of 2014.

Most notably, Heartbleed poked a large security hole in Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL). The consumer-facing Internet largely relied on SSL as a way to signify that a site and information were secure in the cloud.

The flaw going unnoticed for years has likely caused a major reduction in plans for insurers to move any part of operations to the cloud.

"We must protect data at all costs, no matter where it's handled," said Jackson.

The question has been: What is the potential benefit for economies that are predicated by adoption of the cloud or a cloud-based platform? When the answer focused on reduced margins and increased competition, cloud-based analytics were an easier case to make.

Now, insurers must weigh the risks of criminals' ability to exploit the generosity of insurers who keep data siloed versus the criminals' potential ability to access information if vulnerabilities arise from third-party processing power.

Where Should the Industry Look?

As austerity budgets continue in the UK and Europe, individuals, groups and gangs will look to the softest option to make ends meet.

Multiple insurers said their industry can learn a lot from credit card fraud detection. These companies have adopted and invented new technologies to detect and deter fraud because of a compelling business reason to act: regulators look heavily at money laundering.

"There is an overwhelming logic that says these technologies are absolutely relevant to what insurers should be doing" and even without regulatory imperatives, these businesses should recognise the benefits available to them, Collard said.

"Professional fraud analytics are crucial to bring fraud detection into the next level of excellence. At Zurich, fraud detection analytics are there to support our people and to assure the highest level of objectivity," said Woerner.

The Future of Third-Party Data

Third-party data may play a role in fraud detection but it will likely reside in systems run by the IFB, police, and other law enforcement for the near term. Major database providers don't yet speak the same language as insurers when it comes to privacy and value, so it'll take a shift from the IT industry to start the adoption of third-party data centres and fraud detection services.

In the UK, customer data is very strictly monitored. Similar protections are in place in France and Germany, and EU nations are likely to move toward stricter data controls in the future. Privacy concerns will naturally impact the data insurers use and own, so broad sharing will likely remain relegated to law enforcement unless there is a significant shift in political climate.

Many insurers and other industries still feel burned from outsourcing and offshoring their customer service to third-parties. Fraud detection systems become worthless when errors are introduced, so there is little likelihood of complex systems being outsourced to anyone, even native developers.

Closing Remarks

The potential of today's insurer lies in the realm of new data analysis, but its path is wholly determined by the human aspects present in insurance.

The largest hurdle faced by insurers remains legislative barriers to sharing and pursuing information. Where legislation allows, insurers are poised to collect and analyse new data and deliver better results. However, tighter controls over an individual's privacy may limit what analytics can do by stifling information pools.

The push toward Big Data and analytics for fraud is coming with a clarion call of automation and modelling. Unfortunately, a pure automation operation can create as big of an opportunity for fraud as already exists in the market by producing exploitable data pattern recognition.

Fraud detection still needs a human touch. Even the most advanced systems still deliver a data product, not a finalised piece of information. "People are still required to take this analysis and produce the final intelligence product that is useful to insurers," said Fletcher.

While data is at the core of the current revolution in insurance industry practices and advances, it must inherently remain an industry that relies on gut feelings and human insight. A proper mix of machine and human review can bring fraud detection to a new level, and an analytics backbone helps assure the highest level of objectivity.

Ultimately, insurers face a choice of absorbing the cost to adopt these new fraud detection capabilities today or of maintaining current operations in hopes that analytics will standardise and cheapen before increased competition presses margins too thin.