Rethinking the business case for anti-fraud programs in insurance

Building a better working world

Insurance fraud is not only widespread, it is also quite varied in terms of the forms it takes.

Executive summary

Historically, claims and related insurance fraud has been considered a relatively minor issue that did not deserve a place on the strategic agenda of senior executives. The expense of investigating suspicious activity and the risk of being sued for denying claims made many insurers all the more reluctant to pursue anything beyond the most egregious instances of claims fraud.

Today, however, a range of factors has forced real evolution in this perspective. For one thing, the industry better recognizes the scope and scale of the problem. US insurers lose approximately $80 billion to fraud every year, according to the Coalition Against Insurance Fraud (CAIF). Startlingly, that figure does not include Medicare or Medicaid fraud. Industry groups have estimated that up to 10% of property and casualty claims are fraudulent. Whatever the precise proportion, there is an increasing recognition that insurance fraud is a serious problem and deserves the kind of attention many companies are applying to other risks in the industry, such as cybercrime or business continuity.

As a result, insurers are looking closely at their anti-fraud investments and the potential business value they can generate. The potential value includes not only significant cost reductions, but also process improvements resulting from increased automation, better data, more efficient investigations and more extensive use of fraud analytics tools. Well-managed fraud programs can lead to faster handling times for legitimate claims and can enhance the overall customer experience. In other words, there are real financial and operational benefits to be realized from a clear anti-fraud strategy and well-coordinated, cross-functional programs.

Ultimately, anti-fraud capabilities must be less about punishing wrongdoers and more about protecting legitimate claimants and policyholders. Insurers have a commitment to accurately and fully pay what is owed on valid claims — and not a penny more. In that sense, anti-fraud programs speak directly to the heart of the mission of many insurers and indeed the core role of the industry as a whole.

Forward-looking insurers are taking a holistic, business-oriented view of their anti-fraud programs and are seeking business and technology-driven improvements in a range of areas. Predictive analytics and advanced tools, such as voice biometrics, are part of the plan, but so too are specialized interviewing and investigative techniques, as well as end-to-end process improvements.

This paper explores the impact and extent of claims, underwriting and application fraud today; highlights the business case for improved anti-fraud capabilities; and describes a series of necessary steps to create a highly effective and efficient fraud operating model that moves detection efforts as far upstream as possible and leverages advanced analytics to generate significant benefits for the business, as well as policyholders.

Identifying the many types of insurance fraud

Insurance fraud is not only widespread, it is also quite varied in terms of the forms it takes. The most common types include:

- Opportunistic or soft fraud: misrepresented or exaggerated data (e.g., water damage in the basement of a home resulting in claims for new televisions, furniture or other items that were not legitimately part of the damage).
- Hard fraud: often committed by organized criminal gangs; this may include people buying policies with the intent to submit bogus claims or the submission of auto bodily injury claims (e.g., where the number of claimants exceeds the number of passengers who were actually in the vehicle at the time of the accident).
- Application fraud, underwriting fraud and premium fraud: significant threats involving the misrepresentation of information (e.g., smokers claiming to be non-smokers or a business owner claiming to have more clerical workers than employees working in higher-risk roles) to obtain coverage at a lower premium rate.

It is important to note that there is much overlap in these types of activities, and fraudulent parties may use multiple types within the same scheme. For instance, application fraud potentially results in premium fraud or goes hand in hand with subsequent claims fraud.

Some lines of business are at higher risk for fraud than others. For instance, auto-related fraud and bodily injury claims in auto accidents are quite common and involve staged accidents, induced accidents, ghost accidents, crash-and-buy (insurance policies purchased after the crash) and "ghost brokers" who trick young drivers online. The rapid development and adoption of driver assistance and safety features in vehicles are turning cars into mobile data sources, giving insurers a powerful weapon in the anti-fraud battle (provided they have the analytical skills and tools to process and examine such data).

According to the National Insurance Crime Bureau (NICB) and CAIF, the other most common questionable claims are faked or exaggerated injuries (e.g., suspicious slips and falls), questionable theft (e.g., of a vehicle), prior damage, fictitious loss or suspicious theft. "Mysterious disappearance" – e.g., items stolen from a hotel room or other situations where there is little or no documentation of an incident — is a growing area of concern relative to personal and property lines. Insurers must also be on the lookout for medical providers, lawyers and other service providers billing for services not rendered or charging for more expensive services than were actually provided.

Assessing the impact of fraud

According to NICB, many of these popular "flavors" of fraud are becoming more common. In fact, 55% of insurers are seeing a rise in workers' compensation fraud rings, and 61% are seeing a rise in auto fraud rings.

The resulting impacts are plaguing insurers around the globe with higher costs, lower customer confidence in the market and a subpar customer experience for legitimate claimants. Industry groups have estimated the financial impact:

- Eighty billion dollars annually in the US.
- Forty-five percent of carriers surveyed said claims fraud is 5% to 10% of claims costs, with 32% of carriers indicating it was as high as 20%.
- NICB estimates that 10% of all property and casualty claims are fraudulent.
- ALFA (Agence pour la lutte contre la fraude à l'assurance), France's fraud bureau, estimates that 15% of claims paid, representing between 4% and 8% of premium collected, are fraudulent, which equates to €2.5 billion.

Given these startling numbers, it is no surprise that improved decision support (especially related to fraud management) is a top priority for the finance function through 2020, according to EY's 2014 global survey of senior finance executives in the insurance industry.

While the cost impacts may be eye-opening to insurance finance executives, it is worth noting how customers may be impacted in other ways. Today, up to 70% of detection is conducted via manual means, which may cause all claims – even legitimate ones – to be paid more slowly. These delays can hurt customer satisfaction. Similarly, product development and personalization efforts and the application process may be unnecessarily slow for those insurers lacking clear insight into the attributes of the products most associated with fraud.

The business case for anti-fraud

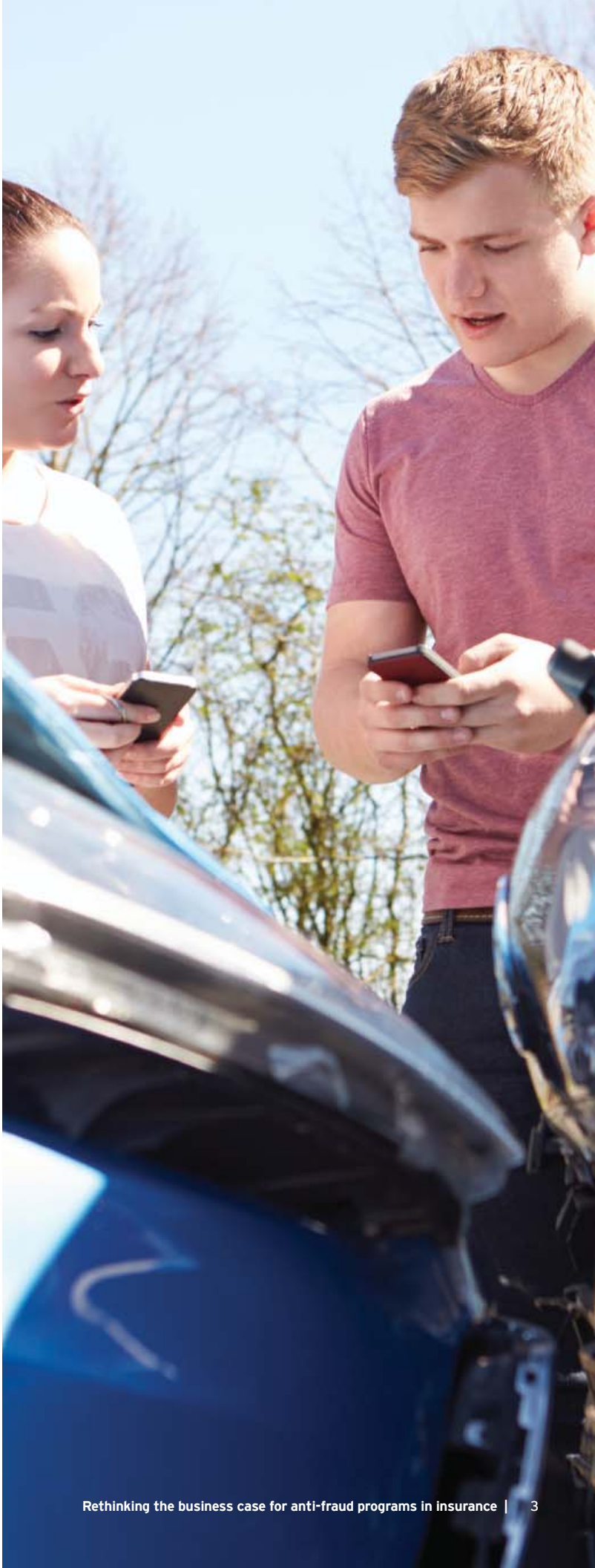
The business case for enhanced anti-fraud capabilities is both clear and highly compelling. Our experience suggests that up to 4% of total claims spend can be saved from an optimized anti-fraud program (i.e., $500 million in claims means up to $20 million in potential reductions). Loss reduction is a top priority for many insurers, given cost and market pressures affecting every area of the enterprise and a few percentage points can make a difference in any insurance organization.

The business case looks most attractive for those insurers that take a truly end-to-end and cross-functional view of fraudulent activities. Insurers that view fraud as an issue to be solved collaboratively among claims, underwriting, technology, special investigative teams and other units are more likely to build out a stronger anti-fraud program and realize greater business value. They are also less likely to be accused of bad faith because they have an objective and systematic way of identifying applications and claims that need further scrutiny.

Consider how anti-fraud capabilities map to a number of strategic imperatives across the enterprise. Improved anti-fraud processes and tools are one potential payoff for investments in advanced data management and analytics capabilities. Leveraging analytical tools will be essential as insurers move away from primarily manual fraud detection processes and look to improve detection by correlating data across applications, claims and third-party data sources. Given that vehicles are now producing large volumes of performance data, analytical knowledge has become an essential weapon in combatting fraudulent claims related to bodily injuries.

According to Gartner, "Fraud analytics tools have been evolving during the past five years, and their evolution has accelerated in the past 12 months. This is due to increased interest among insurers (especially those in North America and Europe) much as a result of the focus on big data and analytics, and the movement of big data to the top of the CEO's radar."

The business case for enhanced anti-fraud capabilities is both clear and highly compelling.



Looking specifically at claims, the implementation of new claims management platforms has given insurers better claims data. It has also greatly helped improve efficiency – and fraudulent case handling times can be reduced by up to 50% when a robust operating model and strong technology are in place. In fact, better insight into and increased confidence in the organization's ability to detect fraud often lead to an increase in the volume of claims that can be handled with minimal touch or straight-through processing.

As important as better data and predictive analytics are, they alone are not the answer, as a growing strain of conventional wisdom seems to suggest. Other capabilities must be incorporated if effective anti-fraud activities are going to occur earlier in the customer life cycle. How insurers use the data is ultimately more important than just having the data. For example, once insurers have clear visibility into the products and lines of business at risk of fraud, front-line claims handlers and call center representatives can be trained with specialized interviewing skills to ask appropriate questions when they see a suspicious report. In some cases, even gentle pushback on these submissions can lead to the withdrawal of false claims, which may be the best outcome of all for insurers; at minimum, these agents can refer suspect reports to special investigative units with relevant priorities based on the combination of size and suspiciousness of the claim. Such techniques have already demonstrated their value at early adopting insurers.

There are also gains to be realized by more integrated operations that closely link and synchronize actuarial and product development functions to claims and investigations in a kind of closed loop. For example, product design should very much reflect that some policy features and structures are more likely targets of fraudulent activities. These products, as well as specific attributes, should be well known across the company and can streamline both the product development process and the identification of suspicious claims. They can also help rationalize the product portfolio with anti-fraud components largely built in.

How insurers use the data is ultimately more important than just having the data.

A roadmap for strengthening anti-fraud programs

An optimal fraud capability model is multidimensional, involving strategic, organizational, process, and technology and data components.

Strategic: To successfully reduce the financial and operational impacts of fraud, senior leadership must set the right tone from the top. That means conveying the seriousness of fraud as a business issue that needs to be on the minds of senior managers (not just claims leaders). As anti-fraud strategies and plans take shape, C-level leaders may also need to break down organizational boundaries to ensure the key functions are working collaboratively to address the problem.

Organizational: There is a clear need for skilled resources, training on the front lines, and well- defined roles, responsibilities and accountability. Sourcing models (including outsourcing) must also be considered; if outside service providers support processes that are affected by fraudulent claims, their people must also be engaged in the fight against fraud. Multiple layers of defense – underwriters, claims adjusters, screeners and investigators all working toward common fraud prevention goals – will maximize the company's ability to service legitimate policyholders and claimants when they really need it. Implementing such a model may necessitate some adjustments to the organizational chart, or at least better coordination across functional lines. Lastly, many insurers have special investigative units in place, but they may not be optimally integrated with their counterparts in claims or other areas, and they may need updated training or new toolsets to help them achieve core objectives.

Process: Embedding detection further upstream is the hallmark of mature anti-fraud models and is likely to be a future-state objective for most insurers. There is a range of inputs for insurers to consider on this front. Product development, actuarial and underwriting processes can all prevent likely fraudulent parties from obtaining policies, as can an enhanced process for first notification of loss (FNOL). Fraud scoring for all claims and automated and manual referral processes must also be strengthened, with better workflows for detection, triage, investigation and closure. Systematic tracking of fraud trends and metrics should be incorporated into a comprehensive set of feedback loops and tactics to drive prevention and deterrence.

Technology and data: Better data and predictive analytics will help insurers fight fraud, but there is considerable risk in thinking these factors alone comprise a sufficient anti-fraud strategy or program. These tools help leverage new claims and underwriting platforms and can automate initial detection steps and focus skilled resources on the cases that need further scrutiny; for example, analysis of unstructured text can be used for a more comprehensive review of notes from adjustors and investigators, social media scanning, network link analysis, known fraudulent party databases and other relevant industry data. Designing policies and FNOL to ensure the capture and use of high-quality data and overcome siloing to gain a holistic view of claimants, policyholders and third parties across the business all serve to enable the effective use of analytics.

To be clear, analytics is essential to an optimized program. For many insurers, advanced analytics tools have become new, improved and not-so-secret weapons in battling fraud. However, it is essential for companies to know where they stand on the data, analytics and operational maturity curves so that they know where to focus efforts and investments in terms of strengthening anti-fraud capabilities for their specific business. An agile control framework will leverage quality data, integrated systems, and robust and repeatable processes, along with enhanced investigative skills and capabilities. Such are the attributes of an effective and efficient fraud operating model to detect, investigate and mitigate emerging fraud risks – one that simultaneously produces significant and tangible value for the business.

The bottom line: new capabilities to fight fraud

As fraud within the insurance industry grows more sophisticated, insurers must step up efforts to protect good customers, uncover organized fraud and improve the effectiveness of analytics tools and specialized investigative units. But the most powerful weapon in the fight against fraud may be a broad-based and strategic rethink of the overall anti-fraud program, with a focus not just on the "what" is being done, but also on the "why" and the "how." As early-adopter insurers are learning, it is not best implemented as a stand-alone capability or unit, but rather as an integrated capability that underpins processes ranging from product development to underwriting to claims. Just as cybercrime has moved up the strategic agenda, so too must counter-fraud. As it does, insurers will be best served with a more holistic and business-driven approach to their anti-fraud programs and capabilities.

For more information, contact:

Clark Frogley
Executive Director
Ernst & Young LLP
clark.frogely@ey.com
+1 212 773 2748

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

SCORE no. CK0960

1508-1592571 NY

ED None

ey.com