Insurance fraud is a significant profit loss for insurance providers around the world, impacting profitability and eroding shareholder value. It costs US property and casualty insurers approximately USD 32 billion annually; in the UK, insurance fraud is estimated at £2.1 billion a year. Fraudulent claims, staged auto accidents, identity theft and medical provider fraud committed by opportunistic individuals, organized crime rings and insiders are unfortunately commonplace. Several market factors work in favor of these fraudsters:

- Ongoing digitization and insurers’ efforts to improve the customer experience means there is less time and opportunity to assess contracts and transactions for fraud risk.
- Open borders create new opportunities for cross-border fraud schemes.
- Silos between cybersecurity, the know-your-customer (KYC) process, and underwriting and claims operations allow fraudsters to slip through the cracks.
- Trust in the insurance industry remains low and attitudes towards insurance fraud as a victimless crime, and even a justifiable return on premiums paid, are commonplace.
- Insurtech and the Internet of Things (IoT) enable fraudsters to innovate their business models faster than insurers can protect against them.
- The dark web remains dark to most insurers.

Heads of fraud departments in property and casualty insurance companies are responsible for ensuring their counter-fraud operations are based on scalable technology and processes that handle high volumes of occurrences. Simultaneously, they must nimbly react and continuously adapt to new suspicious patterns and schemes.
Investing in enhanced counter-fraud capabilities is a financial imperative

Insurers know that fraud impacts their bottom line. A new, compelling analysis by Aberdeen Group\(^5\) quantifies this issue rather precisely by revealing two important statistics:

- For every dollar that a property and casualty (P&C) insurer makes in profit, USD 60 cents is likely to be lost to fraud.
- For every dollar saved from fraud, a P&C insurance company’s market valuation can increase by up to USD 24.

“Under the status quo, every US dollar in fraud reduction that falls to the bottom line would, in turn, translate to between USD 10.80 and USD 24 in market valuation.”

— Aberdeen Group, Quantifying the Value of Counter Fraud Analytics in Insurance

Note that the quote starts with “Under the status quo, …” — even with all the measures that insurers are already taking, there’s still a financial imperative to look for further improvements.

There’s no single path to success. To take advantage of the compelling case that Aberdeen Group makes, most insurers need to ramp up their fraud analytics capabilities for detection and investigation purposes.

Elimination of information silos, expansion of the observation space and unification of advanced intelligence enables insurers to increase fraud savings by detecting more fraud, and more complex fraud, more quickly with less false positives.

In addition, insurers need to reduce their spend on disparate systems where each only supports a small slice of the overall counter-fraud effort. Some of the indirect costs, such as bespoke integration of systems, data duplication, customization of general purpose tools and lost investigator productivity, can be eliminated by doing away with disparate fraud management systems.

Optimize people, process and technology

IBM’s industry experience can help your organization address enterprise fraud challenges and drive tangible business value in more ways than what a software solution can offer.

IBM’s insurance fraud specialists have run national and international counter-fraud operations for leading insurers and can help optimize the full range of people, process and technology. IBM’s specialists can help you:

- Assess the current state of your counter-fraud program against industry best practices for the dozens of dimensions of the IBM counter-fraud maturity model.
- Identify and prioritize practical opportunities for improvement.
- Create a target operating model to design organizational constructs, operational governance and technology architecture.
- Provide rapid prototyping to demonstrate business value for enterprise-wide protection.
- Deploy and integrate counter-fraud technology.
- Utilize counter-fraud capabilities as a service — including subscription-based models for hosting; application management; behavior modeling, scoring and analytics; and referral generation.

There’s no single path to success. To take advantage of the compelling case that Aberdeen Group makes, most insurers need to ramp up their fraud analytics capabilities for detection and investigation purposes.

Elimination of information silos, expansion of the observation space and unification of advanced intelligence enables insurers to increase fraud savings by detecting more fraud, and more complex fraud, more quickly with less false positives.

In addition, insurers need to reduce their spend on disparate systems where each only supports a small slice of the overall counter-fraud effort. Some of the indirect costs, such as bespoke integration of systems, data duplication, customization of general purpose tools and lost investigator productivity, can be eliminated by doing away with disparate fraud management systems.
IBM Financial Crimes Insight for Insurance

The IBM Financial Crimes Insight for Insurance software solution is designed to help insurers prevent and intercept fraud attempts while detecting, identifying and building the case against past fraudulent activity and improper payments.

Looking at counter-fraud operations as an entire lifecycle, the IBM solution introduces advanced analytics and investigative analysis throughout the entire process. Implementing this holistic approach translates into lower fraud losses and operational costs, while improving business results and supporting a superior customer experience.

IBM Financial Crimes Insight for Insurance is purpose-built. The end-to-end solution supports the key phases of the fraud lifecycle:

- **Detect**: Score and rescore claims, requests or entities using rules and multiple analytical fraud models in real time, embedded in the business process, to detect potential fraud earlier and avoid pay-and-chase situations.
- **Respond**: Apply deep insights to take the next best action for a claim with confidence. Differentiate legitimate actions from suspicious ones, respond immediately to suspicious patterns and activities and encourage fraudsters to abandon planned schemes.
- **Investigate**: Turn fraud intelligence into action. Perform and manage deep inquiries into suspicious activity to compile evidence and build cases.
- **Discover**: Facilitate learning and enable continuous improvement in fraud detection by analyzing historical data, assessing patterns and building watch lists for potentially fraudulent individuals and organizations.
- **Improve**: Utilize analytics to monitor current and potential exposures and identify areas of improvement in the effectiveness and efficiency of your fraud management efforts.

**IBM approaches fraud in a different way**

- **End-to-end, integrated approach across the fraud lifecycle**: IBM has invested millions of dollars in building this business solution to provide a configure-and-integrate-once user experience that unifies virtually all user roles on a common infrastructure and data store. The integration is done by IBM *in the labs* to provide a more simplified implementation and upgrade experience.
- **Integrated into the core processes, such as claim handling**: IBM Financial Crimes Insight for Insurance integrates with your claim-handling application to score claims for fraud risk directly in the claim-handling workflow. From the first notice of loss (FNOL) through the end of the claims management lifecycle, the solution delivers strong insights that enable proactive and anticipatory decision making.
- **Continuous entity resolution**: It's essential to understand the difference between three claims filed by three people versus three claims filed by one person. IBM Financial Crimes Insight for Insurance applies continuous entity analytics that goes far beyond name matching. It applies a combination of deterministic and fuzzy methods to detect the real entities behind all people an insurer deals with, such as claimants, drivers, third parties, witnesses, agents or employees.

- **Multilayered cognitive approach to fraud detection throughout the observation space**: A modern fraud-fighting tool cannot rely only on business rules. Fraud has become more complex, more organized and more digital, so insurers need to layer multiple detection techniques to find these cases.

- **Transparency and ease of use of analytics**: IBM Financial Crimes Insight for Insurance lets you see and control the analytics used in your business and our analytical tools are designed for ease of use with a point-and-click interface that requires no coding.

- **Powerful investigative analytics**: Provide analytic capabilities to special investigative units by combining link, temporal, geospatial and content analysis in one centralized work environment thereby presenting a robust analytical picture and comprehensive analytical depth that helps save time and improve efficiency.

- **Attractive delivery and pricing options**: IBM has implementation options to match your needs; from a traditional license with an on-premises installation to a fully managed and hosted solution that is either usage based or set for gain sharing, or options in between.

### Customer examples

**A multiline carrier in North America aims for a significant reduction in fraud losses** by:

- Lowering fraud operating costs
- Reducing fraud exposure by detecting more fraud sooner, at the source
- Driving investigative productivity
- Improving case management workflow and automation
- Enabling retrospective discovery for subrogation and adjudication

A Latin American financial institution with multiline insurance estimates **USD 12 million savings per year** for every one percent reduction in fraud by:

- Detecting probable fraud automatically
- Applying the counter-fraud intelligence in underwriting
- Improving agility, accuracy and visibility throughout the alert lifecycle
- Improving investigator management

ProBTP, a social protection group for the French construction and civil engineering industries, analyzed 21 months of optics and dental claims to identify **€14 million** in suspicious claims through:

- Using a secure service platform
- Analyzing optical and dental claims in real time so the firm can evaluate them before payment
- Applying enriched predictive models it can use to help detect fraud networks, based on self-learning technology that pools detection schemes and takes advantage of an observatory watch

---

*Figure 3: Multilayered analytics provide an optimum mix of techniques to deliver more accurate fraud detection.*
Conclusion
Fraud threats are continuously evolving. Insurers must remain vigilant, constantly adding and adjusting their models and responses. Merging individual rules, analytics and techniques into a seamless, end-to-end operation enables organizations to have deeper insights and react with more confidence. Using the IBM Financial Crimes Insight for Insurance solution, forward-thinking insurers can:

- Deter suspicious transactions with confidence
- Quickly distinguish fraudsters from valued customers
- Detect fraud before unnecessary payments occur
- Reduce the volume of false-positive fraudulent claims
- Improve the effectiveness and efficiency of investigators
- Focus investigations on high-risk cases
- Manage the claims investigation process from prevention through litigation
- Meet regulatory compliance obligations
- Employ enterprise intelligence to continuously adjust operations and stay ahead of trends

For more information
To learn more about IBM Financial Crimes Insight for Insurance visit ibm.com/insurance-fraud or contact your IBM representative.