IBM Financial Crimes Insight for Claims Fraud

Stay ahead of three emerging trends in insurance financial crime

Highlights

Insurers fight an increasingly complex range of financial crime. Technology alone can't solve the problem. People, business processes and technical tools together are needed to counter growing threats. To support this effort – considering tight counter-financial crimes budgets – transaction-based pricing is gaining attention.

Fragmented approach to fighting financial crimes

Based on conversations with IBM® insurance clients this year, insurers point to three industry trends in financial crime. First, they fight a growing range of offenses such as fraud in all forms (claims fraud, underwriting fraud, and fraud by agents and providers such as medical providers or repair shops) and identity theft. Over 60 percent of insurers say fraud has increased in the past three years,[1] and identity theft is on the rise.[2]

Additional crimes include money laundering, bribery and corruption, collusion and insider threats. Insurers must comply with regulations around Know Your Customer (or Know Your Employee, Know Your Business partner, etc.), privacy, security and more.

Crime syndicates, gangs and terrorist groups are increasingly committing large-scale financial crimes to fund operations.[3] Financial crimes often cross multiple industries; insurers say 84 percent of the cases they investigate involve more than one industry.[1] These heightened risks are why insurers are investing more in anti-financial crimes technology.[1]

Standard technologies and methods used to combat various kinds of financial crime – and comply with regulations – are similar in many ways. They all need to:

- Be integrated into the respective operational processes and systems.
- Use all available data – structured and unstructured – for effective decision making.
- Determine who is who and who knows who.
- Use multiple layers of analytics to assess the risk.
- Efficiently triage and investigate the alerts that are raised.
- Access management information to manage the efficiency and effectiveness of the program.

Traditionally, different types of financial crime are addressed by different teams, processes and tools, using disconnected metrics and data from various silos. Complications include incompatible, duplicated or stand- alone technologies. To ease the fragmentation issues, insurers are looking for a partner with the know-how and platform to help fight an array of financial crime types, instead of buying similar capabilities over and over.

For example, a global insurance company headquartered in Europe has started the transformation of its financial crime prevention organization. Grouped under one leader, the anti-financial crime group will harmonize processes, share data and tools, and integrate management reporting. They aim to transform the people, process and tools required to effectively address a gamut of financial crime with an integrated platform. Figure 1 shows the insurance company's current state and challenges and the desired state of transformation.

Figure 1: IBM Financial Crimes Insight for Claims Fraud

Current state	Desired state
Fragmented view of entities impedes accurate risk assessment	Holistic view of all entities for most accurate risk assessment
Operational capacity and experience challenges across financial crimes capabilities	Trained financial crimes operational teams to migrate exposure and operationalize investments
Inconsistent or no policies, procedures and best practices	Consistent application of policies and procedures based on industry and company best practices
No single source of truth for management information	Management insights from single, trusted source
Duplicate and disparate technology and data	Rationalization of technology, shared financial crimes intelligence database
Bespoke IT integration, initial and ongoing	Vendor integration "in the labs"delivered in product, not projects
Different maturity levels in different parts of the business	Bring all units up to a higher baseline while following more mature units to progress
No objective mechanism to assess current capabilities	Capability maturity model to assess current maturity levels and identify improvement areas
Low delivery speed to get all business units to the right next level	Repeatability and common modules

Transaction-based pricing has clear benefits over perpetual or fixed pricing models. When spread out across many transactions, the per-unit investment is just a small fraction of the total cost of a claim.

Need to optimize people, process and technology to fight complex threats

The second trend insurers see is that financial crime is increasingly complex. Technology alone is not a silver bullet to address today's sophisticated financial crimes. For example: to realize the benefits from a more advanced detection system, insurers also need to make sure their financial crimes teams have the skills, processes and capacity to deal with this sudden avalanche of more and more complex alerts. Insurance leaders are looking for a partner with industry expertise in more than just software implementation.

To successfully fight complex crimes, insurers need to consider and optimize a holistic approach that includes skills, business procedures and intelligent technology. A set of transformative leading practices such as a financial crimes policy and common language, organization, skills, core processes and key performance indicators (KPIs) is shown in Figure 2.

Budget restraints and underfunding

The third trend is that budgets for investments in enhanced capabilities remain tight.4 Anti-crime units compete with other internal funding priorities. Investigation teams often can't buy what they need to stay up-to-date in the arms race with the perpetrators. Adoption of advanced capabilities is happening, but slowly. While 90 percent of insurers continue to invest in basic automated red-flag technologies5, anti-financial crime units lack financing for the cutting-edge skills, processes and tools they need now.

Insurers know that the right cost accounting method and pricing model can lower expenses and better support use cases. Transaction-based pricing has clear benefits over perpetual or fixed pricing models.

Rather than acquire new capabilities through an IT capital investment, insurers are looking to shift to an operational expense on a per- claims basis, turning the investment into an allocated loss adjustment expense. When spread out across many transactions, the per-unit investment is just a small fraction of the total cost of a claim.

Figure 2: Financial crimes policies, procedures and leading practices

Our approach...
Focusing on people, process and technology

Continuous improvement

Technology Tools and automation		**Enablers** KPIs and measurement
Process Detection and discovery	Investigation and response	**Core process** Investigation and response
People Skills and training		
Foundations Organization Fraud policy and common language		

End-to-end solution for the detection and investigation of financial crimes

From the first notice of loss (FNOL) through the end of the claims management lifecycle, Financial Crimes Insight for Insurance (FCII) from IBM delivers comprehensive integrated capabilities for the detection and investigation of all types of financial crimes:

- Integration with enterprise systems
- Security and access control
- Entity resolution
- Reporting and dashboarding
- Triage and case management
- Multi-layered analytics for text, business rules, machine learning, anomaly detection, link analysis and more. The solution is designed to protect IT investment by enhancing existing systems, without the need to "rip and replace." Figure 3 illustrates the platform's capabilities, which can be configured to support a range of financial crimes use cases.

Consulting method addresses trends and leading practices

IBM helps insurers evaluate and advance from current to desired states. Figure 4 shows the client engagement method workflow. It

Figure 4: IBM consulting methodology

Leading practices, maturity model, assessment tool and transformational roadmap

1 Client-defined scope is linked to leading practices

2 Maturity model defines requirements

3 Assessment tool enables visualizations of strengths and gaps

4 IBM Design Workshops develop the roadmap to improved outcomes

is tied to leading practices and geared to meet insurance financial crimes challenges and trends. The scope of work, maturity model, assessment tool and transformational roadmap across people, process and technology are designed to lead to improved outcomes. IBM has completed several such consulting engagements for clients.

Cost control with consumption-based pricing and flexible delivery

IBM FCII offers transaction pricing and other pricing models as well. FCII can be either a stand-alone solution or integrated with existing detection engines. There are a range of engagement options, from advisory and managed services to implementation of domain-knowledge machine-learning capabilities. Flexible delivery and deployment choices include cloud, hybrid or on- premises, with global delivery capability.

A platform built for change

IBM Financial Crimes Insight runs on IBM Cloud Pak for Data, providing financial institutions an advanced data science tool kit to build and govern models as well as a flexible, containerized deployment architecture. IBM Cloud Pak for Data manages the entire AI lifecycle, from preparing data for AI use to model creation, deployment and governance. In addition, Red Hat OpenShift offers the ability to deploy IBM Financial Crimes Insight anywhere, as well as access management and audit capabilities. These capabilities enable IBM Financial Crimes Insight to meet your organization's financial crime challenges today as well as adapt to your changing infrastructure and business needs.

Author

Martijn Wiertz,
Principal Consultant,
IBM Financial Crimes,
IBM Industry Platform

About IBM Financial Crimes Insight

By resolving relationships and scrutinizing behaviors to identify high-risk entities before they commit financial crimes, IBM Financial Crimes Insight empowers institutions to increase both the efficiency and the effectiveness of their payment fraud detection, anti-money laundering compliance, know-your-customer, conduct surveillance, and insurance claims investigation programs. Only IBM uses the broadest set of market-leading AI, cognitive services, big data and automation technologies, driven by input from leading regulatory experts to minimize the financial and regulatory burden of compliance while reducing reputational risk.

For more information

To explore how insurers prevent financial crime and deliver more precise risk assessments, visit the IBM Financial Crimes Insight for Claims Fraud marketplace page here.

Footnotes

1.
Coalition against insurance fraud. "By the numbers: fraud statistics." http://www.insurancefraud.org/ statistics.htm

2.
National Association of Insurance Commissioners. https://www.naic.org/cipr_topics/topic_identity_theft.htm

3.
International compliance Association. "What is financial crime?" https://www.int-comp.org/careers/a- career-in-financial-crime-prevention/ what-is-financial-crime/

4.
Insurance Information Institute. Background on Insurance Fraud, November 6, 2017. https://www.iii. org/article/background-on-insurance-fraud

5.
Coalition against insurance fraud. "The State of Insurance Fraud Technology: A study of insurer use, strategies and plans for anti-fraud technology." https://www.sas.com/ content/dam/SAS/en_us/doc/ whitepaper2/coalition-against-insurance-fraud-the-state-of-insurance- fraud-technology-105976.pdf

IBM Global Business Services
Route 100 - Somers, NY 10589

Produced in the United States of America, November 2019