Shielding the Life Insurance sector from fraud risks

Forensic & Integrity Services
With the Insurance Laws (Amendment) Bill 2015 passed recently, the penalty for fraud has increased multi-fold. One of the major highlights of the Insurance Law (Amendment) Bill, 2008 constitutes Section 45, which gives insurers three years to establish reasons for rejecting claims after the Bill has come into force. After this period, they will not be able to reject claims on any grounds, even if fraud is detected.

The latest news article quoted the Chief Risk Officer of a bank-promoted life insurance company, “Several organized cartels operate in the insurance space that file fake claims. As an industry, we do not want to pay claims that are not genuine.”¹ This three-year cycle is expected to result in insurers incurring extra costs for the background checks and investigation of new policies, since fraudsters are generally organized and often operate as syndicates.

The Insurance Regulatory and Development Authority of India (IRDAI), has outlined multiple solutions, including setting up of a common fraud-prevention center, and guidelines to implement an effective fraud framework. It is a step in the right direction, and should propel a change within the industry. Insurance companies have begun to take note and are planning to initiate the dissemination of quarterly reports on fraudulent claims. They are also in the process of formulating robust anti-fraud policies and frameworks to identify potential areas of fraud. In order to sync-up on the evolution taking place within the industry, insurers have begun to form forums such as the Life Insurance Council and the General Insurance Council, which are informal platforms for information-sharing on fraud and detection of crime patterns.

Given the current trends and the significant rise in the number and value of insurance frauds, the life insurance sector needs a robust system and framework to overcome losses due to financial crimes. It is time for insurance companies to team up with various stakeholders and put in place deterrents to combat these crimes. Going forward, in addition to the losses due to fraud, the insurance sector will also have to invest to manage stringent regulations and pay hefty fines, further adding to their losses.

Expectations of the industry from a fraud perspective

- Industry level benchmarks for the implementation of fraud monitoring frameworks that go beyond the basic requirements, as stipulated by the IRDAI
- Sufficient visibility or perspective of “on the ground” implementation of fraud guidelines; need for assessing whether systems and practices are robust to withstand fraud typologies/scenarios observed
- Up-gradation of fraud training and development programs, given the changes in the environment
- Independent assessment of the integrity of vendors who may either be involved in malpractices in collusion with employees, or involved in fraudulent practices
- Reduction in misselling and spurious calls to prospective clients
- Increased use of data analytics to identify red flags/early warning signals, and enhancing alert monitoring tools to minimize large number of false positives
- Mitigating risks and managing data privacy and data theft (cyber-crime) issues

¹ Life insurers to move IRDA against Section 45 on claims, Business Standard, 26 January 2015, via Dow Jones Factiva, © 2015 Business Standard Ltd
Fraud risks observed

- Customers submitting fake/forged KYC documents
- Misstatement of medical reports/medical facts hidden at the proposal stage
- Agents providing their own personal details, instead of the customer’s details at the time of policy creation
- Customer collusion with third party/internal employee with the intent of hiding relevant information that may affect the amount of coverage/premium
- Fraudulent claims submitted by fraudulent surrenders
- Lack of adequate/duplication within the system during pay-outs
- Unauthorized modifications or forged signatures for withdrawal of funds
- Misselling of policies to customers
- Fictitious or deceased customers and claims fraudulently submitted
What can companies do?

At an enterprise level

**Assessment of fraud risk environment**
Assessment of the ‘As-Is’ Fraud environment through a holistic review of the existing Fraud Governance Framework, Proactive and Reactive Fraud risk mitigation mechanisms including Benchmarking against IRDAI & overall industry.

**Setting up of a comprehensive fraud framework**
Implementation of a comprehensive fraud governance framework. This would include documentation of policies & procedures for fraud prevention and detection, establishing fraud response procedures, whistle blowing mechanism and training & awareness.

**Fraud-related training for senior/middle management**
Conduct case study based training/workshops for Senior/Middle Management to sensitize on fraud vulnerabilities they may encounter during regular operations, good practices and control mitigation mechanisms and recent trends & typologies.

**Whistle-blowing mechanism**
Making available a whistle-blowing platform where an employee, third party, vendors, etc., can anonymously inform the company’s senior management about wrongdoings in the organization.
At a process level

Proactive

► **Fraud vulnerability assessment**
   Conduct end-to-end review of processes and discover flaws/gaps in these, risk assessment surveys to understand the level of awareness among various levels of employees, transaction testing to understand whether the process had been followed.

► **Forensic data analytics to identify red flags by using special tools**
   - Forensic data analytics on key data sets including policy, claims and payouts to identify trends/anomalies/red flags basis benchmark typologies/scenarios.
   - Select review of red flag transactions to assess inherent operational level people, process and systemic fraud vulnerabilities.

► **Mystery shopping and background checks**
   Assist in carrying mystery shopping to assess 'on-the-ground' process level deficiencies, identify potential conflict of interest amongst specific employees/third parties and overall effectiveness of the implementation of fraud framework.

► **Network scan/Surprise audits**
   - Conduct network scans within vulnerable functions/critical processes to assess inherent conflict of interests.
   - Assist in performing surprise branch audit to review control mechanisms from a fraud perspective and implementation of policies/guidances in line with business expectations.

Reactive

► **Investigation of fraud and misconduct**
   Investigation/fact finding reactive reviews on red flags, trends that may have been identified by management. This includes review of specific transactions, whistleblower allegations or suspicion of potential conflict of interest within employees/amongst employees and third parties.

► **Assistance in litigation/disputes**
   Provide litigation support for claims against tainted employees, resolution of disputes with the customers/key stakeholders etc.

► **Disk imaging and analysis of emails (investigation-related support)**
   Image the disks of suspected employees and conduct Electronically Stored Information (ESI) reviews toward obtaining evidences/substantiation against allegations/suspicions of potential conflict of interest. Prepare evidence matrices and conduct interviews if suspicions are confirmed and confront tainted employees.
### Our experience

#### Case study 1

<table>
<thead>
<tr>
<th>Business Need</th>
<th>Our Approach</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Study the existing fraud framework and recommend broad-level mitigating controls, improvement opportunities to address the fraud risks</td>
<td>Assessment of the “As-is” fraud environment through a holistic review of the existing fraud governance framework, proactive and reactive fraud risk mitigation mechanisms, including benchmarking against the IRDAI and the overall industry</td>
<td>Thematic fraud framework concerns including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gaps within the implementation of fraud framework as stipulated by the IRDAI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ineffective maintenance of fraud risk registers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lapses within the internal fraud risk assessments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ineffective utilization of forensic data analytics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Weak fraud response plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ineffective whistle-blower mechanism</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Need</th>
<th>Our Approach</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud risk assessment of the policy payout process</td>
<td>Review of the existing procedures, followed for all types of claims to identify fraud vulnerabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detailed study of the previous instances of fraud reported to understand the key gaps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evaluation of design and operating effectiveness of internal controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review of IT processes and controls to identify fraud vulnerabilities and capability of audit trails</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data analytics to formulate fraud scenarios based on past cases and EY database</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Results</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Existence of fraud vulnerabilities, due to manual processes and high dependence on outsourced vendors</td>
<td></td>
</tr>
<tr>
<td>• Lack of adequate controls in place at key customer touch points</td>
<td></td>
</tr>
<tr>
<td>• Lack of adequate audit trials and maker checker concept at various stages of the process</td>
<td></td>
</tr>
<tr>
<td>• Lack of integration between various systems being used</td>
<td></td>
</tr>
</tbody>
</table>
Case study 3

Business Need
Assess effectiveness of fraud risk controls implemented in payout processes (core and non-core)

Our Approach
Proactive fraud vulnerability assessments
- Detailed process understanding pertaining to core and non-core business payouts
- Forensic analytics on key data sets including de-dupe tests, exception and variances analysis, anomaly trending, business/marketing spend analysis
- Transaction testing based on red flags emerging from data analytics
- Assessment of internal systemic workflows, system validation controls, and segregation of duties

Results
Key concerns highlighted:
- Potential fraud instances within payouts related to:
  - Surrender
  - Partial withdrawal
  - Foreclosure
  - Death
- Potential nexus between vendors and employees:
- Significant manual intervention within the workflow, leading to the manipulation of data
- Gaps within the calculation of incentive/commission and payout
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.

About EY’s Forensic & Integrity Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016
© 2018 Ernst & Young LLP. Published in India.
All Rights Reserved.

EYIN1507-080
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

RB