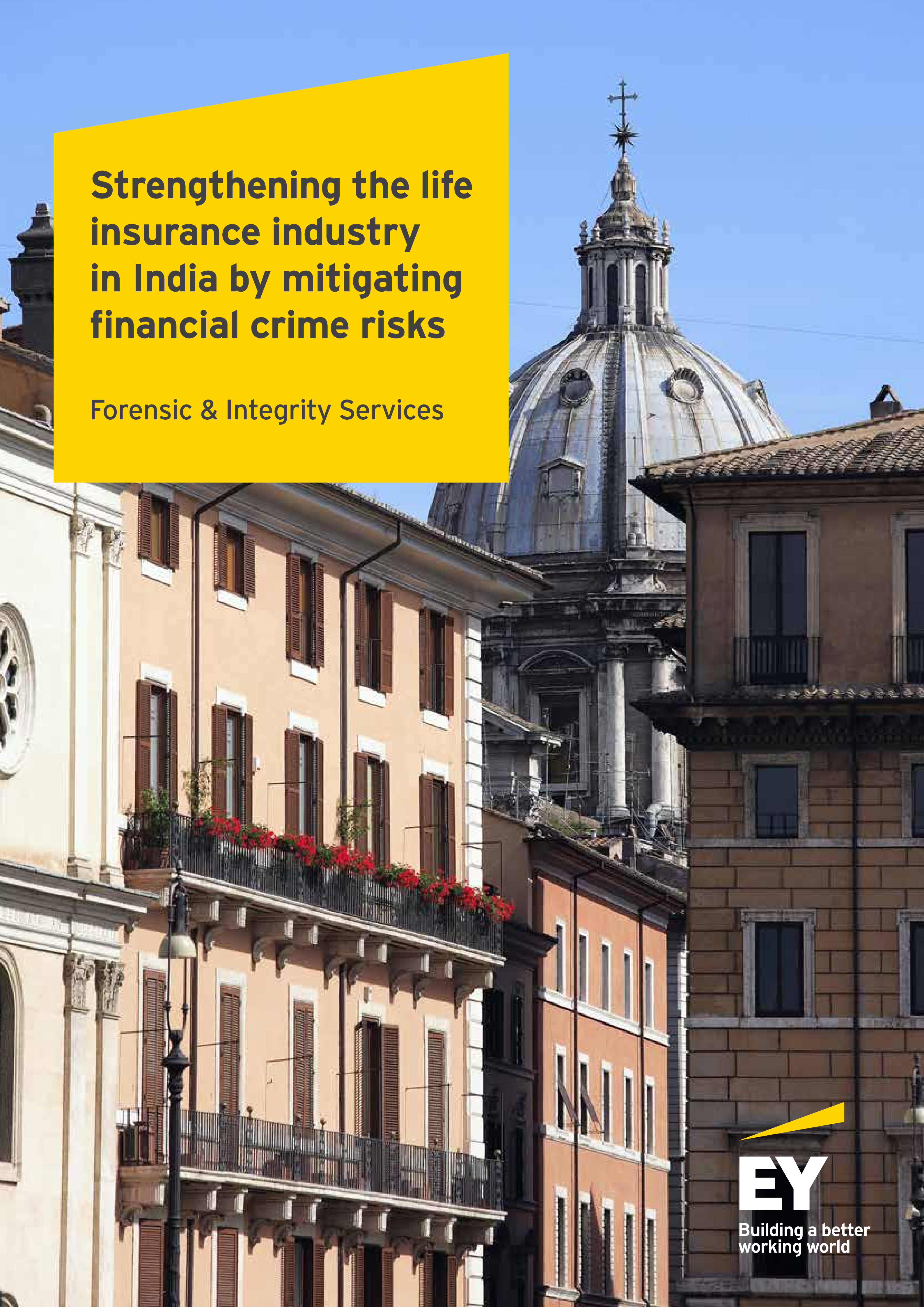
Strengthening the life insurance industry in India by mitigating financial crime risks

Forensic & Integrity Services



EY
Building a better working world

Introduction

The Indian insurance sector has been on a steady growth path, emerging as presumably the largest in the world. A recent report by International Credit Rating Agency (ICRA) suggests that it is poised to grow 12 - 15% in the financial year 2017, and data from India Brand Equity Foundation (IBEF) anticipates it to quadruple in size over the next decade from its current size of US$60 billion. The potential of the sector — both for life and general insurance — is immense, with value multiplying significantly, quantum of premiums rising and new regulations coming in.

Consequentially, the prevalence of financial crime within the life insurance sector has perhaps increased. The Insurance Laws (Amendment) Bill 2015 increased the penalty for fraud significantly. Such initiatives are expected to propel a change within the industry in the right direction.

Our survey attempts to assess the current financial crime environment within the life insurance sector. The survey has identified emerging areas of concerns within the financial crime space, moving beyond the most vulnerable area, which is "claims." Apart from period-end pressures, the survey highlights significant manual interventions, disjoint systems and data sets as key reasons for financial crime within organizations. About 30% of the respondents indicated low utilization of transaction monitoring or workflow systems as the key reason for money laundering. From a regulatory standpoint, respondents have been categorical on the need for additional measures and increasing penalizations to strengthen the overall control environment in the industry.

We would like to thank all the respondents for their views and insights. Our survey would not have been successful without their contribution. We hope you find it helpful in driving meaningful discussions within your organization, board and other stakeholders.

A Singh

Arpinder Singh

Partner and Head - India and Emerging Markets
Forensic & Integrity Services, EY

Executive summary

Life insurance companies still not compliant with implementation of IRDAI-mandated Fraud Monitoring Framework

One in three
respondents stated that their organization did not have fully established fraud-response procedures

- Whistle-blowing mechanisms
- Enhanced third-party due diligence systems
- Robust fraud-response procedures

Emerging fraud prone areas

- Underwriting
- Commission payout to agents and intermediaries
- Vendor management

Vulnerabilities continuing to impact operations

- Data leakage and cybercrime issues
- Fake documentation
- Unauthorized modifications to customer data

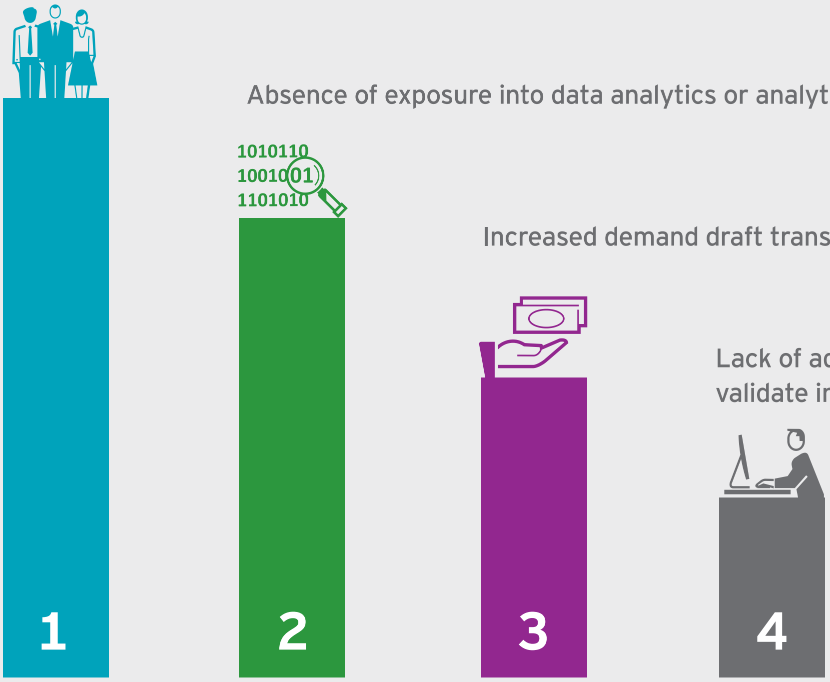
KYC and Money Laundering - A growing concern for life insurance sector

Lack of requisite skill-sets and investigative mind-set in identifying and monitoring red flags

Absence of exposure into data analytics or analytical capabilities

Increased demand draft transactions made through co-operative banks

Lack of adequate methodologies to validate income sources vis-à-vis occupation



Financial crime sliding up the charts

56%
of the respondents stated up to **30% increase** in fraud over the last two years

7%
of the respondents confirmed up to **50% increase** in fraud over the last two years

Significant investments that are expected over the next two years

Building financial crime skill-sets

Setting up a central repository to identify red flags

Enhancing due diligence for intermediaries and agents ("Know your Agents")

Financial crime sliding up the charts

56% of the respondents in the life insurance sector confirmed that there has **been up to 30% increase** in the financial crime rate in the last two years.

7% confirmed that there has been **up to 50%** increase in the crime rate in the last two years.

With increasing interactions with third parties, greater complexities around data privacy controls, technological advancements and increasing use of life insurance products as a lever for money laundering, the propensity for financial crime has enhanced significantly. The vulnerable areas in the sector are not limited to "claims" or on-boarding. Life insurance companies can no longer just focus on specific business areas to mitigate fraud but need to assess inherent risks within and outside the organization, and proactively monitor them.

With IRDAI releasing a guidance on monitoring and regulating fraud within life insurance companies through the "Fraud Monitoring Framework" circular, insurers have taken action to implement aspects, specifically in the areas of fraud policies and guidelines, response plans, training and awareness.

However, certain areas still continue to ail life insurers.

Over 35% of the respondents observed that **"effective whistle-blowing mechanism"** and **"enhanced third party due diligence"** were either not implemented or in the process of implementation within their organizations.

Over 40% of the respondents believed **that collusion with third parties is one of top three areas susceptible to fraud.**

Over **20%** highlighted that vendor management and payouts is another function prone to fraud, thus highlighting the importance of effective background checks or due diligence on third parties.

Therefore, the need to institute a robust framework around third party due diligence and having a whistle-blowing mechanism is imperative.

EY viewpoint

Insurance regulator IRDAI released a set of guidelines on corporate governance for the sector focusing on key areas such as whistle-blowing, governance structure and disclosures. The guidelines state that insurers are required to have a whistle-blowing policy in place that would allow employees to raise concerns about possible irregularities, gaps in governance and financial reporting issues, among others. The guidelines also state that the appointed actuary or internal auditors have a duty to address the concerned situations.

Rising vulnerabilities for life insurers

Our survey has highlighted certain areas that could be more susceptible to fraud than others. Some of the key areas of concern for the sector are as follows:

Payouts and underwriting emerge as key concern areas

Traditionally, the "claims" process has been an area of focus as it has been relatively more susceptible to fraud risks. But with millions at stake, areas related to commission payouts and underwriting have emerged quite vulnerable as well. Insurance companies are under significant pressure to increase revenue, which could lead to lapses if the application and document details are not properly checked for reliability or precision.

A major provision under the Insurance Law (Amendment) Bill allows insurers to repudiate claims on grounds of fraud only if they are received within three years of policy issuance. This three-year cycle is expected to result in insurers incurring additional costs for background checks and enhanced customer due diligence prior to issuance of policies.

Therefore, the need for an effective underwriting process, due diligence, background checks and reviews becomes critical. Additionally, the overall process of "auto-underwriting" would also have to be monitored to incorporate fraud scenarios and vulnerabilities. This would also mean that "on-the-ground" branch level capabilities to assess and profile customers also need to be enhanced. Given the workflow systems within life insurance companies, the need to deliberate on customer due diligence and risk profiling has become crucial.

Third party (non-core) business payout has garnered importance in terms of fraud vulnerabilities in recent times. With the potential for bribery and corruption, commission-related issues and conflict of interest with employees emerging as key concerns, the propensity for financial crime has become quite high.

From a general "forensic thumb rule" viewpoint, an increase in the interaction of an internal function with third parties can lead to greater fraud vulnerability. It is not surprising that given the current business environment, insurers believe this to be a focus area from a fraud vulnerability standpoint.

Gaps in operational processes

One of the key operational issues faced by life insurers is multiple silo systems enabling work flows within the organization. Although the systems may individually contribute to streamlining the processes, in most cases they do not "speak" to each other, thereby resulting in iterative back-end mapping of data sets to generate analytics for fraud analysis. It has been observed that such situations could lead to multiple issues, including inaccurate flow of data, incoherent mapping of information and gaps in tracking of critical data sets.

It is hence no surprise that nearly half of the respondents believed that "disjoint units, systems and data sets" or "manual processes" contributed most to frauds within their organization, apart from period-end business pressures.

Case study

A life insurance company conducted a fraud risk vulnerability assessment on the vendor payout function to ascertain existing vulnerabilities in the processes and system. The review included detailed vulnerability assessment of the processes, existing systems and IT controls and forensic data analytics.

Some of the key vulnerabilities observed included:

- Vendor empanelment process and vendor creation process not interlinked, resulting in non-empaneled vendors getting on-boarded
- Data de-duplication based on limited parameters, leading to duplicate payments to the vendors or creation of dummy vendors
- Absence of a job rotation process for employees in the payout function, thereby increasing the risk of conflict of interest
- Payout file uploaded could be subjected to manual intervention, leading to a risk of unauthorized manipulation

Impact of money laundering and associated risks

The insurance sector witnessed an increase in people investing in life insurance policies – especially under the "one-time" premium category. The risk that emanates with this is the amount of cash received for this premium and the extent to which is it monitored to gauge any money laundering risks.

Our survey aimed at understanding the level of preparedness of life insurance companies to the increasing vulnerabilities around money laundering risks.

25% of the respondents indicated that transactions made through demand draft are more vulnerable from a money laundering perspective.

In many cases, it has been observed that these demand drafts could potentially be funded through cash deposits in case of smaller banks, to evade scrutiny. This could make these local or smaller banks more susceptible, especially if they have weak anti-money laundering (AML) controls.

As per a media report, around 500 urban co-operative banks[1] had come under the scanner of the Reserve Bank of India (RBI) for alleged violation of AML laws. It was reported that the irregularities observed in the banks were of a "grave nature," given their wide reach and penetration across the country. This covered over 8,000 branches, deposits to the tune of over INR2 lakh crore and advances worth INR1.35 lakh crore, according to a report by the Central Economic Intelligence Bureau.

EY viewpoint

It has been observed that individuals with certain occupations have a relatively higher income and are paying an even higher life insurance premium. Of late, this issue has been on the rise in tier 3 cities and villages where it may be difficult to ascertain an individual's income. This is typically because the document submitted may not always be verified or cross-checked. Often, individuals from these regions are insured for a higher amount than what they should be for because their income proofs include crop receipt and incomplete or new account bank statements, which may not be sufficient to determine their actual income.

Policyholder profiling and due diligence background checks could further enhance the quality of controls and lead to early identification of potential fraudulent or money laundering cases.

1. Lack of requisite skill-sets and investigative mind-set in identifying and monitoring red flags

2. Absence of exposure into data analytics or analytical capabilities

3. Increased demand draft transactions made through co-operative banks

4. Lack of adequate methodologies to validate income sources vis-à-vis occupation

[1] Business Standard 'Money laundering: Over 480 urban cooperative banks under lens'

Transaction monitoring capabilities still at a nascent stage

More than 50% of the respondents stated that the overall reporting and transaction monitoring capabilities are in the very early stages of development at life insurance companies.

The need of the hour is to have stringent processes in place, along with a transaction monitoring system for identification and reporting of unusual transactions, patterns and activity.

A robust transaction-monitoring framework must be embedded in an organization's AML program, including checks around sanctions/negative lists to screen customers and third party vendors. Further, the efficacy of the framework should be verified periodically, specifically around ascertaining the validity of the AML scenarios and the thresholds set for them, updating negative and sanctions lists.

30%

of the respondents indicated the absence of a transaction monitoring/workflow system. They also indicated that review and subsequent reporting of vulnerable transactions are mostly through spreadsheets with basic or no standardized MIS reporting systems.

EY viewpoint

Life insurance companies have an immediate need to assess the enhanced use of technology to identify risks emanating from money laundering. They should also be cognizant that an AML transaction monitoring system does not result in the reduction of staff vigilance. It has been often observed that suspicious activities tend to be frequently identified in circumstances that do not lend themselves to standalone automated surveillance.

A strong AML transaction monitoring system can enable:

- Regulation of internal policies, procedures and controls
- Analysis of KYC and risk profile of the customer and income justification
- Reporting of suspicious transactions through unusual trends and patterns analysis
- Identification of AML risks throughout the customer life cycle – on-boarding, on-going transactions and claim stages

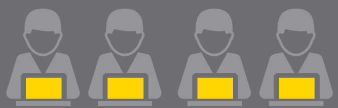
Data leakage, cybercrime and other areas of concerns

Almost 40% of the respondents stated that data leakage and cybercrime are one of the biggest financial crime risk scenarios today. This is closely followed by fake documentation, as believed by 28% of the respondents.

With the shift in insurance businesses to the online platform, most consumers prefer insurers interacting through online channels or websites. As a result, insurers will need to account for additional security layers to mitigate cybercrime risks.

The frequency of data breach incidents has risen dramatically over the last few years. A data breach can be defined as an incident that takes place if critical company information (customer or business related) is compromised because of unauthorized access or misuse. Data breaches raise concerns around privacy and could potentially lead to financial and reputational loss.

40%



indicated that "unauthorized modifications" to customer data is another area of concern. Instances relating to fake documentation have also been on the rise. For instance, there have been many cases reported in the media where claims have been filed on behalf of someone who may be still alive or, in some cases, never existed. These could only have been perpetrated with the help of fake documentation.

Case study

A life insurance company conducted a fraud risk vulnerability assessment on the customer payout function to ascertain vulnerabilities in the processes. Multiple instances of fraud red flags were noted during the course of review and mostly perpetrated by modifying customer demographic information.

Some of the key red flags included:

- Customer phone number and address modified 30 days before submission of a surrender request
- Agent (not servicing the policy) taking the proceeds of full or partial surrender into their own account by submitting forged or fake documents
- Bank passbook copy submitted with claim documents, having altered customer name and address
- Surrender requests processed using a fake bank authorization letter, without obtaining canceled check or bank statement copy
- Date of death altered for a policy issued after the actual date of death of the customer

Way forward

Forensic data analytics: a dependable enabler

71%

of the respondents concluded that "proactive data analytics" is one of the primary enablers to identify irregularities or red flags from a financial crime perspective.

Analyzing data intelligently as a preventive strategy can mitigate fraud risks to a large extent. Forensic analytics can help improve the process but a strong fraud mitigation and detection framework complementing it will be important. Data analytics can assist in spotting patterns of fraudulent behavior in enormous amounts of structured and unstructured data. Establishing data analytics through the organization can be a one-time investment for the companies and may see a huge return on investment.

Insurance companies have performed quantitative analysis using data analytics for different areas, to determine the reliability of existing systems and data points. However, the approach has been quite fragmented. The need right now is to provide extensive insights into the available data by having dashboards and visualization.

The survey highlights that data analytics as a business enabler has not been utilized optimally and can be used to tackle challenges relating to proprietary vendor systems, gaining control over enterprise wide data, improving the transaction monitoring system and being proactive instead of reactive.

Life insurers are opting for small in-house or over the counter tools for better performance of periodic analytics on data sets to support enhanced decision making and identifying anomalies, trends and patterns.

It is important to note that often when analytics does not lead to results, the reason tends to be the incoherency of the data itself. Hence, consistent mapping of data within existing workflows could eventually lead to significantly improving the results of analytics.

Augmenting review and monitoring skills

40%

of the respondents stated that there is a lack of experience in process reviews, with specific focus on financial crime and monitoring of red flags.

Instituting a fraud containment unit that is proficient could help lower the costs of fraud considerably, and consequentially improve bottom-line numbers.

23% of the survey respondents believed that control functions teams typically lack an "investigative mind-set."

The commitment to mitigate fraud proactively depends on the internal teams' capability and the professional skepticism adopted during the course of financial crime reviews.

Some other points that may be considered while establishing a strong fraud containment unit include:

- Setting up a mechanism where any identified anomaly is directed to the correct person within the team
- Creating a repository of red flags and updating it regularly
- Following up investigation of reported anomalies by a review of controls so that existing controls are enhanced to mitigate future vulnerability; this should also suitably link with making appropriate changes to the investigation or internal audit testing, and updating training materials, policies and procedures
- Having an adequate fraud risk repository as a part of the overall financial crime framework
- Maintaining proper records on investigations and typical red flags, which can help identify trends in fraudulent and corrupt activities

Investing in hiring skilled resources

40%

of the respondents stated that hiring skilled resources should be the most significant area of investment over the next two years, highlighting the continued focus around the need for skilled staff.

In various reviews and investigations, it has been found that insurers do not have a dedicated fraud containment unit. In many cases, the job of detecting fraud is allotted to the compliance function of the organization. In cases where the fraud containment unit is available, they do not have sufficient workforce or the employees do not have enough sector or business knowledge. In organizations where the job of detecting fraud is part of the compliance function, the mandate tends to be less effective. This is because the compliance function has its own set of duties to perform and is additionally given the responsibility of proactively managing fraud and vulnerabilities.

A dedicated fraud containment unit with the requisite skill set can assist in monitoring and mitigating financial crime risks within the organization. The main responsibility of the team would be to conduct periodic assessments of key business processes and thereby identify any lapses in the internal control system from a fraud risk perspective.

As per the survey, the other major areas of investment include "screening of policy holders from a consolidated database," "enhanced due diligence prior to appointing new intermediaries or agents" and "mystery shopping" in the expected vulnerable areas.

Addressing key industry issues

50%

of the respondents opined that additional guidance or measures are imperative to address financial crime.

Further, the development of an independent consolidated database of fraud and financial crime cases was also been raised by nearly 30% of the respondents as a key measure to curb financial crime.

Conclusion

A large number of life insurers are now entering into agreements to create a repository that could help detect fraud or duplicate claims in the life insurance industry.

The regulatory guidelines and our survey results highlight that although organizations have taken significant corrective steps over the last few years, there is significant room for improving overall control mitigation and processes.

An analysis of the present situation indicates that life insurance companies need to adopt proactive measures in institutionalizing a comprehensive fraud framework to include analytics, product-based vulnerabilities, third party due diligence and a robust governance around AML. It is also inevitable to create a fraud management ecosystem that will include the continuous update of the overall framework, to reflect periodic changes within the business environment.

The life insurance sector should adopt digitization, thereby curbing premium payment in cash or cash equivalents and lowering money laundering risks. After demonetization, the single premium market grew by approximately 506% [1] (Y-o-Y) whereas the non-single market merely grew by around 22% [2] (Y-o-Y). There will be emphasis on enhanced due diligence for these policies and taking appropriate measures to ascertain the ultimate beneficiaries. With interest rates coming down, insurance becomes a lucrative investment choice with guaranteed returns. This also increases the risk of potential money laundering or routing of money through the life insurance channel.

Going forward, the industry needs to have robust processes and controls with respect to customer due diligence and transaction monitoring. It is evident that the insurance market in India has a long way to go before the potential of a robust financial crime governance mechanism is completely realized.

[2 & 3] Mint 'Life insurers get demonization bonus'

About the report

This report was prepared by the Forensic & Integrity Services team of EY in India. The findings presented have been derived from responses of over 100 individuals, representing a majority of the public and private life insurance companies in India.

The questionnaire sought views and opinions of the top and middle management on various issues, ranging from vulnerable financial crime areas, the impact of fraud, areas that needed anti-fraud regulations and methods of fraud detection in the industry. The principal respondents were senior executives from business functions including internal audit, fraud containment units, and legal and compliance departments.

In addition to the survey results, the report includes our viewpoint based on experience over a period of time.

Note: Some of the percentages in the charts total to more than 100%, because the respondents were allowed to make multiple selections. Not all the questions in the survey were answered by all the respondents. Therefore, all the percentage figures are derived from the total number of respondents who answered a particular question and not on the total number of overall respondents.

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.

Contact us

Arpinder Singh
Partner and Head - India and Emerging Markets,
Forensic & Integrity Services
Direct: +91 124 443 0330
Email: arpinder.singh@in.ey.com

Vikram Babbar
Partner, Financial Services Lead,
Forensic & Integrity Services
Direct: + 91 22 6192 2155
Email: vikram.babbar@in.ey.com

Rohan Sachdev
Global Insurance Emerging Markets Leader,
Partner & Leader - Financial Services Advisory Services
Direct: +91 22 6192 0470
Email: rohan.sachdev@in.ey.com

Sandeep Ghosh
Partner, Financial Services Advisory & Leader,
Insurance Advisory
Direct: +91 22 6192 2800
Email: sandeep.ghosh@in.ey.com

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

EYIN1709-106
ED None