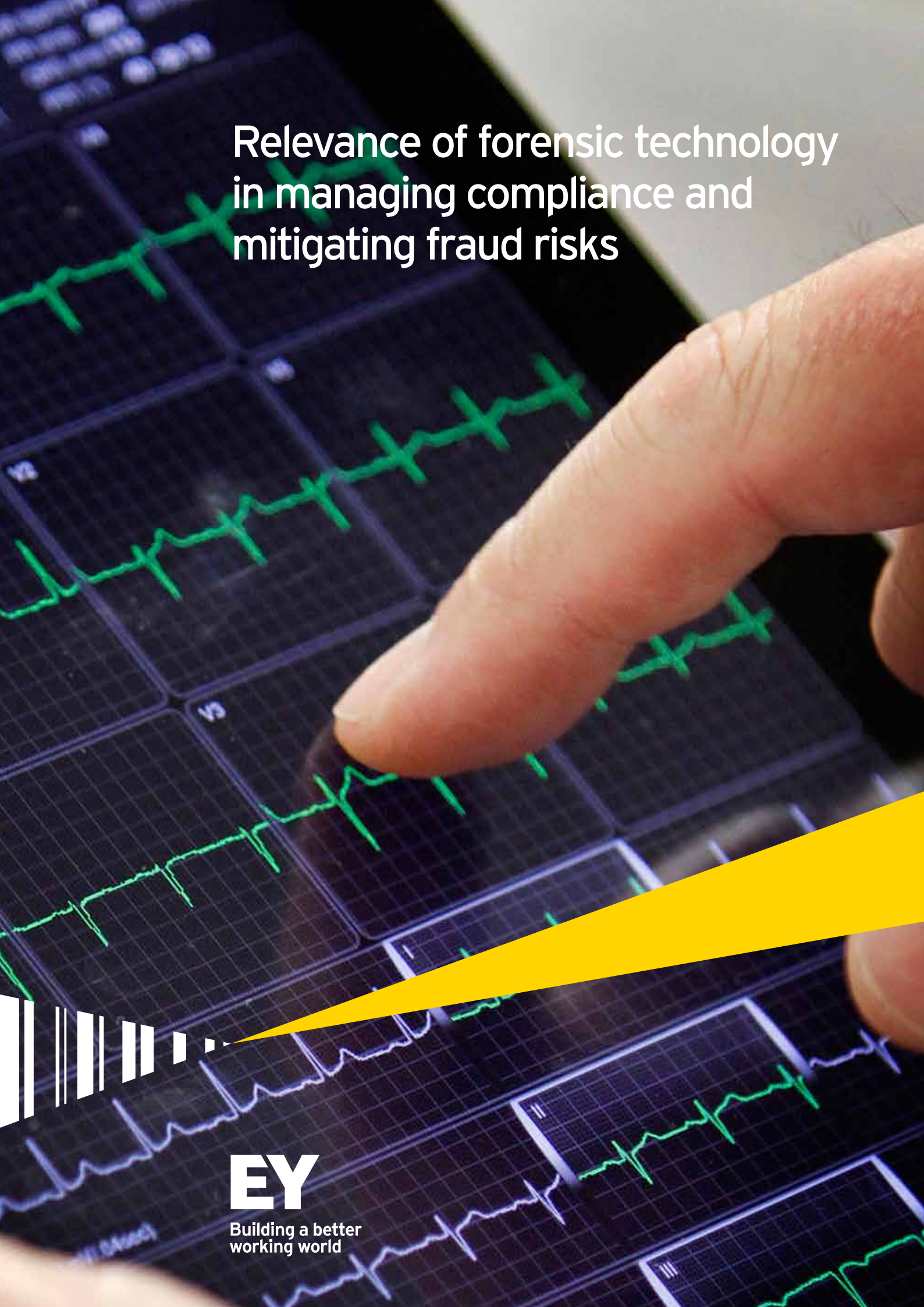
Relevance of forensic technology in managing compliance and mitigating fraud risks



EY
Building a better working world

Contents

Introduction

Worldwide, companies are striving to survive in adverse economic and competitive conditions. This has resulted in their engaging in unethical business practices in many instances. With the increased focus on emerging markets, risks are associated with new opportunities, since many of these markets have been witnessing numerous incidences of fraud, bribery and corruption. According to the EY Global Forensic Data Analytics (FDA) Survey 2014, bribery and corruption constitute the highest area of concern (70%) for fraud risk in Indian companies. This is followed by misappropriation of assets.

Over the years, the regulatory environment has seen a remarkable change with the enforcement of several fraud disclosure and anti-bribery legislations such as the US Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act, to name a few. In India, the Government passed the historic Lokpal Act in January 2014. This Act is an anti-corruption law, which was drafted to establish a Lokpal for the Union Government and Lokayuktas for the states to enquire into allegations of corruption against public functionaries. Today, this Act is making headway for the public sector, where cases of corruption and bribery are widespread. Additionally, the Government also introduced the new Companies Act, 2013 and a new Bill, known as the Prevention of Corruption (Amendment) Bill, to impose more stringent rules and amendments on business markets. In the technology domain, the Information Technology (Amendment) Act 2008, which addresses data protection, was enacted, along with the Information Technology Rules 2011 (Privacy Rules), which detail personal data and privacy rules.

With companies expanding their businesses across foreign locations, regulators in countries such as the US, e.g., the Department of Justice (DoJ) and the US Securities and Exchange Commission (SEC), continue to work in conjunction with other countries to curb the growing menace of bribery and corruption around the world. In India, similar regulatory agencies such as the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Serious Fraud Investigation Office (SFIO) and the Financial Intelligence Unit (FIU) have been active in investigating cases of serious and complex fraud, which often transcend geographies. India has been witnessing a staggering increase in the volume, variety and velocity of business information that needs to be monitored for indications of fraudulent activities.

On the one hand, the quantum of data to be analysed is humongous, and on the other, fraudsters are deploying sophisticated technology to commit cybercrime and other fraud. In such a scenario, investigating fraud or a financial lapse in the system is even more challenging. Therefore, the use of cutting edge technology and analytics has become essential to combat this menace.

Use of forensic technology to monitor and testing of compliance can create a cycle of improved adherence with company policy and improved fraud prevention and detection, while providing additional comfort to key stakeholders. **According to the EY Global FDA Survey 2014, respondents using technologies beyond basic tools have generally seen an 11% improvement in results and recoveries, 15% have been able to detect misconduct and 14% have witnessed an increase in their cost-effectiveness.**

This publication elaborates how forensic technology can be used to manage compliance-related requirements and mitigate fraud risks in today's complex business environment.

Section 1

Case study 1

How Indian companies are exposing themselves to unauthorized access and theft of information

EY India's Forensic Technology team conducted a market study on used hard drives and mobile phones. The team obtained these from the local grey market and the online second-hand market. On conducting advanced digital forensic recovery procedures on these acquired digital units, the team retrieved around 700 documents and spreadsheets, 100 presentations, and 50,000 pictures and movies from each of the hard drives. If a basic "format" procedure is performed on these hard drives, it is easy for any trained computer forensic professional to recover data. The search indicated that these hard drives were probably a part of discarded personal and corporate computers.

Forensic findings on the mobile phones showed that personal information such as contacts, caller groups, SMS messages, call logs, email accounts, user names and passwords, web search histories and other relevant information deleted by users could be retrieved easily.

Existing hurdles and crossing them

Dependence on technology

The advent of technology has changed the way we live as well as the way we do business. Communications, work and even recreational activities have undergone a significant change and are now being powered by technology, which is faster, easier and more convenient than ever before. However, just like convenience is being facilitated by advances in technology, risks and challenges have not become less, but have only become more sophisticated.

While the corporate world has taken cognizance of this trend, it has also begun to recognise the importance of using the right technology and IT infrastructure as a defence against such risks, which can result in reputational loss, among other losses. Not only do these risks result in loss of revenue or destruction of shareholder value, they also tarnish the brand.

Changing regulatory landscape

In the last two years, there have been comprehensive changes in the Indian regulatory landscape with the introduction of the Lokpal Act and the new Companies Act 2013. These aim to improve corporate governance practices, enhance transparency in the operations of organizations, protect investments and enforce disclosure norms and push reforms for implementation of structured mechanisms to curtail fraudulent activities.

On the global front, regulations such as the US FCPA and the UK's Bribery Act are applicable for Indian companies with operations in the US and the UK. Compliance with these regulations is onerous because they need to comply with the mandate on Electronically Stored Information (ESI).

While many companies may have been requested in the past to provide relevant data to regulators, they are slowly realising the impact of such legislations, which may require all relevant ESI to be examined. The majority of the companies are yet to frame an integrated response to be able to meet the requirement for data or evidence that may be requested by regulatory bodies to ensure legal compliance.

However, while regulatory bodies are still at a nascent stage in their adoption of advanced technology, a majority of them are now catching up with changing business conditions in terms of relevance as well as reach. Governments across a wide range of markets are also introducing new tools for regulators to impose deferred prosecution agreements, FDA devices and aggressive investigative techniques.

Digitization

Today, on an average, more than 80% of an enterprise's digitized information resides in individual hard drives and personal files. Of this around 80% of the data is unstructured (e.g., email communication and free-text fields in databases), which are unsecured and do not have back-up. Consequently, there is the high possibility of data being exposed to various threats. Therefore, adoption of continuous monitoring programs, including Governance, Risk and Compliance (GRC) tools and sophisticated visualization and forensic technologies such as Big Data, is essential.

Implementing FDA procedures in monitoring and testing compliance can create a cycle of improved adherence with company policy and enhanced fraud prevention and detection, while providing additional comfort to key stakeholders.

80%

Of an enterprise's digitized information resides in individual hard drives and personal files

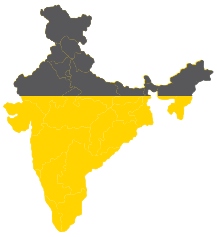
Cybercrime

Cyber risks not only affect business systems in an organization, but also affect its internal and external stakeholders – including regulators. These risks also strain communication between them. According to a recent report published by the Center for Strategic and International Studies (CSIS), cybercrime costs the global economy around US$445 billion every year, with damage to business from theft of intellectual property exceeding US$160 billion lost by individuals due to hacking. Therefore, use of cutting-edge technology and analytics has become imperative to effectively combat high-tech fraud and cybercrime.

US$445 billion

Loss caused by cybercrime annually to the global economy

Section 2



60%

Of Indian companies use FDA in their anti-fraud and anti-bribery programs

Forensic technology at work

Forensic Data Analytics (FDA) relates to the ability to collect and use structured and unstructured data to identify potentially improper payments, patterns of behaviour and trends. FDA can also include integration of continuous monitoring tools and analysis of data in real or near-real time, and enable a rapid response to prevent suspicious or fraudulent transactions.

As companies continue to expand in various markets, their fraud, bribery and corruption risks also rise. And as regulators and law enforcement bodies intensify their cross border collaboration, the cost associated with non-compliance is also growing. Out-of-date risk assessments, undetected fraud and inefficiently executed investigations, followed by failure to properly remediate internal controls, only exacerbate the risks facing companies. In such a situation, forensic technology plays an important role in detection of potential fraud.

Deploying advanced FDA tools across large data sets provides new insights, leading to more focused investigations, better root cause analyses and contributions in a virtuous cycle for companies to enhance and make more effective their fraud risk management. Such tools can also be deployed against a wide variety of risks, including competitive practices, insider trading or tax controversies.

The common testing areas for FDA in investigations and compliance-monitoring include:

- Payment stream, accounts payable analyses
- Vendor master/employee master analyses and comparisons
- Employees' expenses/travel and entertainment
- Payroll
- Financial mis-statement
- Bribery and corruption
- Capital projects

According to the EY Global FDA Survey 2014, 60% of Indian companies use FDA in their anti-fraud and anti-bribery programs and the majority of them use a combination of in-house and outsourced resources. However, while companies may be executing some forms of FDA, many are missing important opportunities to leverage more refined tools. Advanced technologies that incorporate data visualization, statistical analyses and text mining concepts – as opposed to spreadsheets or relational database tools – can be applied to massive data sets from disparate sources and enable companies to ask new compliance-related questions about their data, which they did not previously question.

Biggest FDA-related challenges

Limited knowledge and expertise

Today, companies lack awareness of the appropriate FDA tools for their business while formulating and implementing anti-bribery and corruption programs. According to the EY Global FDA Survey 2014, 63% of the respondents agreed that they needed to enhance their anti-fraud and anti-bribery procedures; 62% indicated that they needed to improve and increase their managements' awareness of the advantages of FDA; 26% revealed that the greatest challenge faced by their organizations was "getting the right tools and expertise for FDA."

Data volumes analysed relatively small compared to company sales

According to the respondents, 35% of Indian companies with revenues ranging from US$100 million to US$1 billion are working with data sets with less than 10,000 records and 82% of organizations with more than US$1 billion sales were using data sets of one million or less. This clearly indicates that companies may be missing important fraud prevention and detection opportunities by not mining larger data sets to more robustly monitor their business activities.

Technology and data sources not in sync

It was observed that companies using only spreadsheet or database applications in their FDA-related efforts reported that they analysed free-text payment descriptions in the accounts payable fields to identify potentially improper payments. However, without the use of more sophisticated text mining technologies, it can be daunting and inefficient to analyse free-text comments among thousands – if not tens of thousands – of records in a spreadsheet.

Right risks, wrong tools

There are notable differences between FDA technologies that are the most effective and those that are being used by organizations. The EY Global FDA Survey 2014 reveals wide disbursement of tools in use, with no one FDA tool dominating the market. According to the respondents, the most common tool used to manage fraud and corruption risk were "in-house developed tools."

62%

respondents indicate the need to improve and increase awareness of advantages of FDA

Advantages of adopting FDA

The survey revealed that global organizations using FDA technologies beyond spreadsheets and databases generally achieve the following:

- Improved results and recoveries – 11% more than others
- Early detection of misconduct – 15% more than others
- Cost-effective results – 14% more than others
- Increased visibility to their boards – 12% more than others

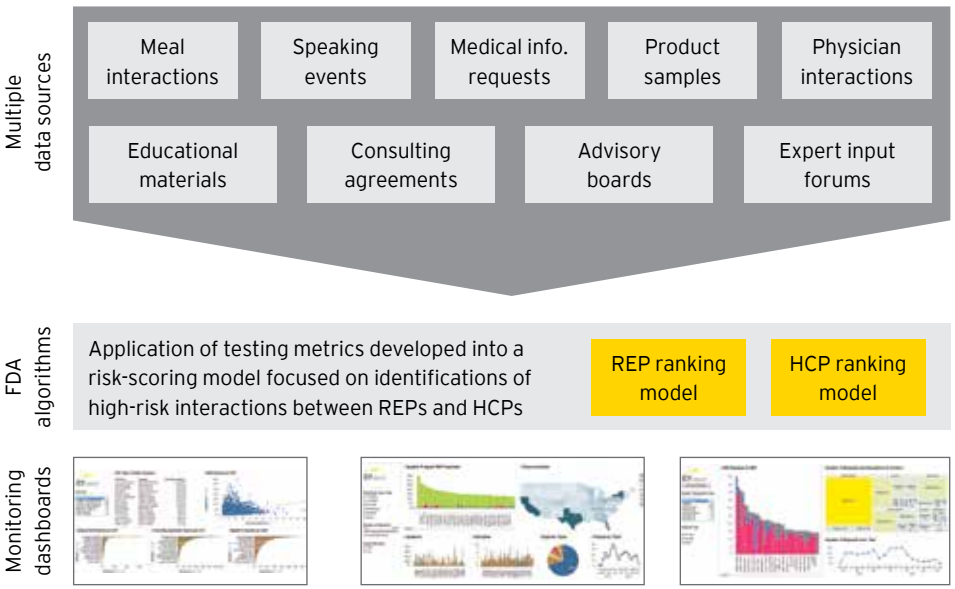
Case study 2

Using multiple data sources for monitoring compliance

A leading global pharmaceutical company integrated FDA in its operations to support compliance monitoring between its sales representatives (REPs) and the Health Care Professionals (HCPs) with whom they interact in certain high-risk countries. Whereas traditional FDA-related thinking would consider only one data source for analyses, this company incorporated "Big Data thinking" and integrated multiple structured and unstructured data sources with sophisticated applications – in addition to spreadsheet and database applications.

As the adjoining figure depicts, the company developed new analytics that incorporated multiple data sources to "risk rank" REPs and HCPs across a range of regulatory and corporate integrity risks, including fraud, corruption and off-label marketing. Dynamic monitoring dashboards were provided to local in-country compliance officers and/or division managers, along with adequate training and instruction on how to spot trends and anomalies. With increased transparency in its business operations, coupled with its findings and success stories of detecting rogue employees, the company deployed its FDA program across several regions over the course of approximately 18 months.

Figure 1.



Big Data

According to Gartner Research, Big Data includes high-volume, high-velocity and high-variety information assets that require cost-effective and innovative ways of processing information to achieve enhanced insights and decision-making.

According to an IBM report, 90% of the world's data has only been generated in the past two years. Clearly, the data volumes enterprises generate every day affect the effectiveness of how they synthesize and interpret fraud and corruption risks in time. Going beyond traditional databases and spreadsheets, new FDA technologies are available today that enable organizations to keep pace with increasing data volumes as well as business and regulatory complexities. Going forward, the convergence of social media, email, free-text and other unstructured data sources is making its way into traditional accounting analytics that only relied on numerical data historically. Consequently, emerging Big Data technologies can play a key role in prevention and detection of fraud by enabling companies to analyse large data in short periods of time.

Big Data presents significant opportunities for business executives in multiple functions across many industries and geographies. It can be used to identify shopping trends and tailor companies' strategies in the marketplace. For those charged with deterring, detecting and investigating misconduct, mining data exhaustively, it can be a powerful tool that can be utilized in their overall compliance and anti-fraud-related efforts.

While spreadsheet and database applications are components of the overall FDA toolset, global companies with increasing volumes, velocities and varieties of data may require more sophisticated technologies. To address increasing data volumes, Big Data technologies such as Hadoop and other parallel processing or in-memory processing systems can significantly increase the speed at which analytics are conducted and make data less complex to improve decision-making in companies.

From a data volume perspective, it has been observed that a 10-million-record, complex duplicative payment query was reduced from three-and-a-half hours in a traditional SQL environment to less than four minutes in a Hadoop distributed computing environment.

It has also been observed that in order to handle data velocities that involve increased real-time analyses of transactions, leading practices leveraging statistical tools that incorporate predictive modelling, anomaly detection and risk-scoring algorithms seek to flag or stop potentially improper payments much sooner in their procure-to-pay processes. Finally, to address multiple kinds of structured and unstructured data, effective use of natural language processing or text-mining tools, combined with data visualization tools, can be done to identify "corrupt intent" in payment or transaction descriptions.

10 million

Record of complex data query reduced from 3.5 hours to less than 4 minutes with Big Data technology

Case study 3

Use of Big Data techniques in a complex environment

A European bank evaluated its third-party banking client sanction screening process. The project involved identifying the most relevant information in its Customer Relationship Management (CRM) database and utilising "fuzzy matching" and "near-matching" FDA techniques to scan millions of records against numerous watch lists and information sources.

A database of nearly 26 million records with additional third-party data sources, and internet and news feeds, along with due diligence procedures, needed to be completely scanned in less than 90 days.

The bank implemented advanced data-matching techniques to match 650,000 entries to all sanctioned individuals and entities from Anti Money Laundering watch lists, and used validation techniques to eliminate false positives. With the help of Big Data techniques, it was able to identify, validate and classify high-risk entities and individuals into a complex scoring model that incorporated multiple risk attributes.

The bank's use of advanced Big Data techniques enabled the project to be completed in less than 90 days. This would have been impossible if it had used traditional techniques.

80%

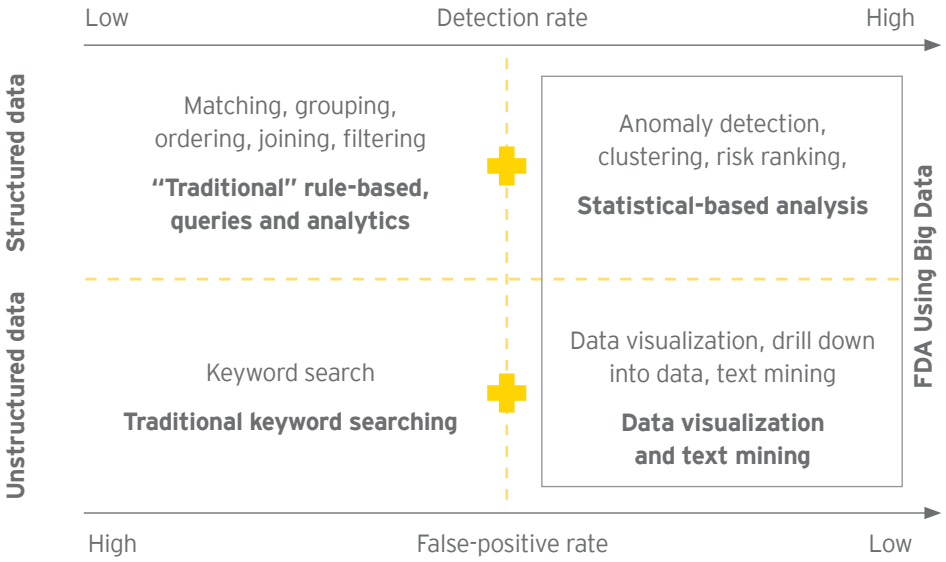
believe emerging Big data technologies will play an important role

The challenge

While the market buzz on the potential of Big Data is fairly strong, the EY Global FDA Survey 2014 indicates that only 7% of the respondents were aware of any specific uses of Big Data and that only 2% were actually leveraging its processing capabilities in their FDA programs. The opportunity to provide enhanced compliance-related insights to their managements and other stakeholders by mining Big Data is therefore significant.

Indian companies have high potential to adopt Big Data, but currently, there is low deployment of such emerging technologies to mitigate fraud risks. According to the EY survey, overall awareness and adoption levels of Big Data are as low as 3% in India and 7% globally. However, 80% of the respondents strongly believed that emerging Big Data technologies can play a key role in prevention and detection of fraud.

Figure 2. FDA maturity model using Big Data



Continuous monitoring programs

Most fraud is only detected after many months. This leaves an enormous window for the fraudster to exploit the gap to commit more or higher value fraud and can significantly affect a company's finances and operations.

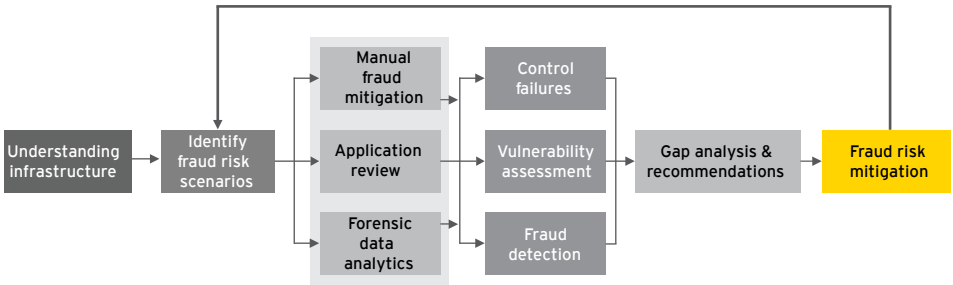
Adoption of Continuous Monitoring Programs, including GRC tools, along with sophisticated visualization and forensic technologies such as Big Data is important to significantly reduce the lag time between commission of fraud and its detection.

Continuous Monitoring Programs integrate well with the ERP systems and business processes of companies, and are typically implemented with alert mechanisms. These automatically alert the management of any suspicious transactions or authorization, based on configured guidance rules. Although this system does not operate on a real-time basis to avoid impeding any critical business processes, the insight and overview it offers to top management or internal compliance committees has hardly any lag.

This makes companies' top management and compliance heads aware of loop holes that are being exploited. While many of these can be false-positives and relate to genuine transactions or approvals, this can be brought to the notice of relevant people before it can cause any damage. Instead of putting in place large internal audit or control teams, advanced technology can be utilized to provide more power and information to existing audit and management teams.

Continuous Monitoring Programs are supported by optimum and effective use of techniques for data mining, monitoring transactions and reporting to management.

Figure 3. Fraud mitigation with continuous monitoring program



Case study 4

Continuous monitoring of programs to combat fraud

A large Indian manufacturing company wanted to implement a continuous monitoring program to minimize revenue leakage in its supply chain.

An analytics framework was put in place to periodically analyse transactions in its procurement and payment modules and support its existing data warehousing and ERP systems. Based on the company's requirements, the most sensitive checkpoints were continuously being checked for anomalies and reports provided to top management for action, as and when required.

With the help of this solution, the company was able to quickly identify suspicious transactions. Timely oversight by the management enabled it to prevent fraudulent practices. This also strengthened its internal processes and procedures.

Case study 5

Having a right eDiscovery approach is a must

A leading bank initiated a thorough investigation into allegations of fraud in one of its subsidiaries. This involved questioning over 100 employees for wilful misconduct as well as negligence.

In view of the sensitivity as well as confidentiality, an eDiscovery in-house environment with sophisticated mobile kits (mobile data centre) was created within two weeks in one of the offices of the bank. This data centre was capable of acquiring and processing petabytes of digital data. Thereafter, an advanced digital forensic recovery procedures was conducted on all the acquired digital assets. A separate environment for hosting and review of the documents was also setup for the team of lawyers and accountants to examine transactions.

About one petabytes of data was acquired from the employee laptops, workstations as well as internal servers. Out of this data, six terabytes of responsive documents were reviewed by lawyers and accountants.

As a result, the analysed documents were able to show the complicity of key employees involved in the fraud. All the documents and communication retrieved were presented as evidence in a court of law.

eDiscovery

With the rising tide of global regulations, proliferation in the volume, velocity and variety of ESI and the ever-expanding reach of businesses, the compliance-related and legal challenges organizations face have assumed gigantic proportions.

Meeting these challenges requires a robust eDiscovery solution, which supports organizations and facilitates its flexibility. Having a right eDiscovery approach is an enabler for a company and helps it remain agile, despite restricting technical and legal conditions.

The important components of an eDiscovery approach are listed below:

- **Preservation and collection of ESI:** Performance of time-critical ESI and forensically sound preservation and collection activities simultaneously
- **Processing of emails and documents:** Utilisation of email and document-processing techniques to normalize data from various systems and enable emails and user documents to be accurately loaded into a document review environment
- **Audio processing:** Utilisation of phonetic indexing technology to use large volumes of audio as a cost-effective and efficient alternative to traditional reel-to-reel reviews or inconsistent transcription
- **Production of documents:** Production of documents and emails for various regulatory authorities, conforming to the guidelines of the DoJ, SEC, Public Company Accounting Oversight Board (PCAOB), etc.
- **Early case assessment:** Rapidly narrowing corpus of ESI through triage of targeted data collection to enable the most relevant information to be reviewed
- **Technology-assisted reviews:** A systematic method of leveraging and extending professional judgement through technology, linguistics, analytics and statistics to enhance review of documents
- **Managed reviews of documents:** Secure and scalable review facilities that are fully integrated with technology platforms
- **Data disposition:** Identification of potential sources of ESI requiring decommissioning and execution of appropriate strategies for secure decommissioning of ESI, supported by appropriate certification
- **Case portfolio management:** Management of wide portfolio of eDiscovery issues, sometimes spanning geographies, by achieving consistency across teams and repeated processes
- **Information governance policies:** Reliable retention policies and procedures for information assets that are directly aligned with strategic objectives, active eDiscovery strategies to balance in-sourcing and outsourcing of resources and customized documentation to provide complete knowledge on ESI sources

It is very important for an eDiscovery service provider to have the right people, right technology, right timing and right integration across its teams, which are generally dispersed geographically, for it to achieve seamless integration of tasks from one stage to another and to reduce time, risks and costs. Throughout the lifecycle of such engagements, eDiscovery professionals can help legal teams understand the results of each phase of the eDiscovery process and put in place strategies to resolve any issues or exceptions.

Computer forensics

Computer forensics or digital forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage media. It is the practice of collecting, analysing and reporting digital information in a manner that is legally admissible. It can be used to detect and prevent crime and in any dispute where evidence is stored digitally.

The increasing number of fraudulent incidents and the growing degree of risk makes it imperative that companies regularly review their policies, build in checks and use new and advanced technology to avoid IT-related fraud. Additionally, computer forensics can help the risk management functions of organizations by creating a competitive advantage for them to improve their business performance.

Law enforcement agencies were among the earliest and most prolific users of computer forensics, and consequently, have often been at the forefront of developments in this field.

It is not just the content of emails, documents and other files that may be of interest to investigators, but also the "metadata" associated with such files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed, and which user carried out these actions.

Computer forensic analysis can achieve the following:

- Find the "smoking gun" in the case
- Help to determine which devices need to be investigated
- Determine whether evidence has been modified or tampered with
- Discover or prove whether the "opposition" is guilty of wrongdoing
- Offer strategies relating to the findings of the report
- Provide facts that are backed by the forensic community
- Testify in court as an expert witness

Case study 6

Forensic audit to help in determining fraud

There was a data breach incident related to leakage of critical employee information in a top consulting firm in India. This confidential data was shared with a third party company through an external email, which was leaked to a competitor for monetary benefits. Computer forensic imaging was performed on the suspect's computer and laptop. All data that was either formatted or deleted from the systems was also retrieved.

Computer forensics revealed the email traces from which data had been received. This helped the firm track the suspected company, based on its IP address. All email communication and data related to the breach was traced and recovered. All these documents were submitted as evidence in a court of law.

Hereafter, the firm's complex IT infrastructure was analyzed and training was conducted on how potential vulnerabilities resulting from advanced social engineering techniques, which lead to data theft, could be addressed.

Section 3

General Counsels build value to the business and help in shaping the organization's culture

Emerging risks and expanded role of General Counsels

In the complex, highly regulated world in which business corporations operate, a General Counsel (GC) plays a key role in promoting organizational integrity and ethical operations. A GC is well-positioned to shape an organization's culture, influence how it will internalize its compliance-related duties and make sure it is on the right side of the law. This places a great responsibility on GCs in fulfilling their stakeholders' expectations.

In today's modern business environment, the role of the GC is undergoing a major transformation, with their strategic and commercial responsibilities assuming greater importance than ever before. GCs are not only helping companies identify and reduce their risks, and facilitate their regulatory compliance, but they are also building value.

Being included at the initial stages of transactions, GCs can act as a filter to determine what is legal, ethical and executable. They help finance teams or sales and business units develop proof-of-concept for transactions, vet plans for any flaws and then help in structuring transactions. They can also provide vital advice by determining the risk of violating government regulations, and whether vendors and third parties are not complying with contractual agreements and could break a law.

In view of stringent regulatory requirements, the GCs of organizations have become increasingly alert to the risks faced by companies and are highlighting this to their managements, boards and audit committees. It is also imperative that they update themselves with the latest tools, techniques and trends in detection and prevention of fraud, so that they can equip themselves as well as their companies with the best tools to ensure compliance.

Regulations

Companies across various industries face the challenge of regulatory risk, which a GC can help to mitigate. The role of GCs is even more challenging when their companies expand their operations in markets, where laws and regulations may not be clearly defined or consistently interpreted and enforced.

GCs need to keep abreast with constant changes in regulatory patterns and laws in markets where their companies operate.

Shaping corporate compliance and information governance policies

Regulatory and corporate compliance is very important for companies due to increasing legal and regulatory scrutiny, as well as a tough business environment. The role of GCs has become even more important than earlier with their becoming the chief advisors in drafting of organizations' compliance-related policies, which are not only in line with the regulatory environment, but are also stringent enough to deter incidents of fraud that can affect the companies' revenues. This includes internal policies for employees, e.g., sexual harassment, as well as information governance policies such as IT policies, data retention and storage policies, ESI management policies and whistle-blowing mechanisms.

Driving internal investigations

The responsibilities of GCs are increasing with organizations increasingly conducting investigations on internal non-compliance with their policies, sexual harassment of employees, data integrity and other human resource issues. In the event of such incidents, a GC's role quickly shifts from that of an advisor to the lead driver in the company's response, crafting the messaging for the authorities, leading internal investigations and providing the requisite disclosure. In such cases, record-keeping takes on a high degree of importance because a court of law can summon any and all documentary evidence. It is also important to track the company's remediation-related actions. Thorough documentation enables organizations to demonstrate that their leaders were in unchartered territory and made reasonable judgements in dealing with such incidents, based on facts and hard defendable evidence.

Managing disputes

Disputes have always constituted an occupational hazard of doing business, as well as a major part of the GC's job, but the complexity and the type of disputes that legal departments are required to handle is changing. GCs are now looking at alternative means of dispute resolution such as mediation and informal negotiations. These help to minimise costs, disruption and damage to business relationships.

New markets and risks

Today, companies are not restricted to a single market. The larger the number of jurisdictions in which they operate, the higher are the risks they face. GCs need to be completely aware of the laws of the different countries in which their organizations operate and ensure that that they comply with and respect these. One needs to understand the legal, ethical and social environment of a country as well. GCs are required to spend more time with operational teams in their companies and in different countries to understand how things work in practice. Their of knowledge — strategic, operational and regional — in a theoretical as well as a practical sense is essential for making the process as smooth as possible and preventing risks.

Conclusion

In today's modern business, companies face the harsh reality of becoming the target of complex and sophisticated fraud, with even insiders or employees being the perpetrators. In addition to this, they also have to gear up to being party to human resource-related investigations, e.g., sexual harassment of employees. In such situations, it is important that companies have an organised, advanced and integrated approach to face such challenges, with the total involvement of their top management right down to the bottom layer of executives.

In this environment, the role of GCs is not only restricted to being legal advisors, but also trusted business advisors. They help companies assess their risks and build compliance into their overall strategies. While dealing with incidents of fraud, the role played by GCs is even more pivotal. They need to be aware of the latest technology trends and anti-fraud mechanisms and should have in place effective strategic plans that include clear guidelines on how to respond and act when fraud or other incidents such as data breaches and sexual harassment allegations are made.

Need for companies to build successful mechanisms to manage compliance and mitigate fraud risks, and adopt an approach that involves use of forensic technology tools and considers the following success factors:

1. Preparing the groundwork: set governance policies and power up IT infrastructure

Companies should begin their groundwork by evaluating their existing compliance and governance policies. They need to update these to suit their operating environment and put in place robust frameworks to identify potential violations. These policies include internal business processes, IT governance, data storage and retention policies, employee harassment policies, escalation mechanisms, etc. It is important to correctly identify the risks facing the critical parts of value chains and install mechanisms to gather more information about individual transactions that may otherwise escape regular scrutiny. This can be done by installing or upgrading existing ERP systems to capture as much information and data as may be relevant, but being careful not to flood the system with too much data. A regular periodic assessment to check whether policies and systems are updated is also necessary.

2. Utilizing the framework: focus on low-hanging fruit

Once the framework is in place, it can be used to identify anomalies that may indicate potential violation of compliance or fraud. However, it is important to note that integration is a journey. While quick-hit projects may take four to six weeks, the program and integration can take one to two years or more. Start with the low-hanging fruit — since the first project normally incurs the largest cost associated with setting up infrastructure and anti-fraud mechanisms, it is important that the first project yields tangible recoveries.

3. Optimising the framework: integrate advanced forensic technologies

One of a company's key goals should be to increase its detection rate of non-compliance while reducing the risk of false positives. From the perspective of technology, organizations need to move beyond rule-based spreadsheets and database applications, and seriously look at using structured and unstructured data sources that consider the use of data visualization, text-mining and statistical analysis tools. Moreover, in cases where anomalies are detected, specialised computer forensic tools can be used to discover evidence of wrongdoing or the complicity of suspected individuals. Companies for whom data integrity is important and where implementation of structured anti-fraud mechanisms are required, either by virtue of their industry profiles or historical fraudulent incidences, can avail the benefits of sophisticated near real-time continuous monitoring programs.

4. Setting the tone at the top: communicate early and broadly

The success of any initiative depends on the support it receives from the top management. This not only requires resources, but also their time, to nurture it. Once validated, success stories generate an internal demand for a compliance program at a company. It is imperative to involve a multidisciplinary team, including IT professionals, business users (end users of analytics) and functional specialists (those involved in designing analytics and day-to-day operations of programs) in this process. Communication across multiple departments, keeping key stakeholders updated on the progress under a defined governance program is a key success factor.

5. Providing sustainable mechanisms: use experienced or trained professionals on a regular basis

Keeping analytics simple and intuitive, and investing in automation and not manual "refresher" initiatives can make such efforts sustainable. Moreover, investing in acquiring and developing professionals with the right skill-sets is imperative for organizations to sustain and leverage such mechanisms to provide benefits over the long term.

EY offices

Ahmedabad
2nd floor, Shivalik Ishaan
Near C.N. Vidhyalaya
Ambawadi
Ahmedabad - 380 015
Tel: + 91 79 6608 3800
Fax: + 91 79 6608 3900

Bengaluru
6th, 12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 4027 5000
+ 91 80 6727 5000
Fax: + 91 80 2210 6000
(12th floor)
Fax: + 91 80 2224 0695
(13th floor)

Chandigarh
1st Floor, SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: + 91 172 671 7800
Fax: + 91 172 671 7888

Chennai
Tidel Park, 6th & 7th Floor
A Block (Module 601,701-702)
No.4, Rajiv Gandhi Salai,
Taramani Chennai - 600113
Tel: + 91 44 6654 8100
Fax: + 91 44 2254 0120

Hyderabad
Oval Office, 18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500081
Tel: + 91 40 6736 2000
Fax: + 91 40 6736 2200

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682304
Tel: + 91 484 304 4000
Fax: + 91 484 270 5393

Kolkata
22 Camac Street
3rd floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400
Fax: + 91 33 2281 7750

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400028
Tel: +91 22 6192 0000
Fax: +91 22 6192 1000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 3000

NCR
Golf View Corporate Tower B
Near DLF Golf Course
Sector 42
Gurgaon - 122002
Tel: + 91 124 464 4000
Fax: + 91 124 464 4050
10th Floor, Tower D&E
Cyber Green, DLF Phase-3,
Gurgaon 12202 Haryana
Tel: + 91 124 671 4400

6th floor, HT House
18-20 Kasturba Gandhi Marg
New Delhi - 110 001
Tel: + 91 11 4363 3000
Fax: + 91 11 4363 3200

4th & 5th Floor, Plot No 2B,
Tower 2, Sector 126,
NOIDA 201 304
Gautam Budh Nagar, U.P. India
Tel: + 91 120 671 7000
Fax: + 91 120 671 7171

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 6603 6000
Fax: + 91 20 6601 590

We would like to hear your feedback and suggestions at forensic@in.ey.com

Contact us

Arpinder Singh
Partner and Head – India and Emerging Markets
Direct: + 91 12 4443 0330
Email: arpinder.singh@in.ey.com

Sandeep Baldava
Partner
Direct: +91 22 6192 0817
Email: sandeep.baldava@in.ey.com

Vivek Aggarwal
Partner
Direct: + 91 12 4464 4551
Email: vivek.aggarwal@in.ey.com

Mukul Shrivastava
Partner
Direct: + 91 22 6192 2777
mukul.shrivastava@in.ey.com

Anurag Kashyap
Partner
Direct: + 91 22 6192 0373
Email: anurag.kashyap@in.ey.com

Rajiv Joshi
Partner
Direct: + 91 22 6192 1569
Email: rajiv.joshi@in.ey.com

Yogen Vaidya
Partner
Direct: + 91 22 6192 2264
Email: yogen.vaidya@in.ey.com

Dinesh Moudgil
Partner
Direct: + 91 22 6192 0584
Email: dinesh.moudgil@in.ey.com

Jagdeep Singh
Partner
Direct: + 91 80 6727 5300
Email: jagdeep.singh@in.ey.com

Amit Rahane
Partner
Direct: + 91 22 6192 3774
Email: amit.rahane@in.ey.com

Amit Jaju
Partner
Direct: + 91 22 6192 0232
Email: amit.jaju@in.ey.com

Vikram Babbar
Partner
Direct: + 91 22 6192 2155
Email: vikram.babbar@in.ey.com

Harshavardhan Godugula
Partner
Direct: + 91 40 6736 2234
Email: harshavardhan.g@in.ey.com

Ernst & Young LLP

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 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

EYIN1407-069
ED 0914

PB

EY refers to the global organization, and/or one or more of the independent member firms of Ernst & Young Global Limited