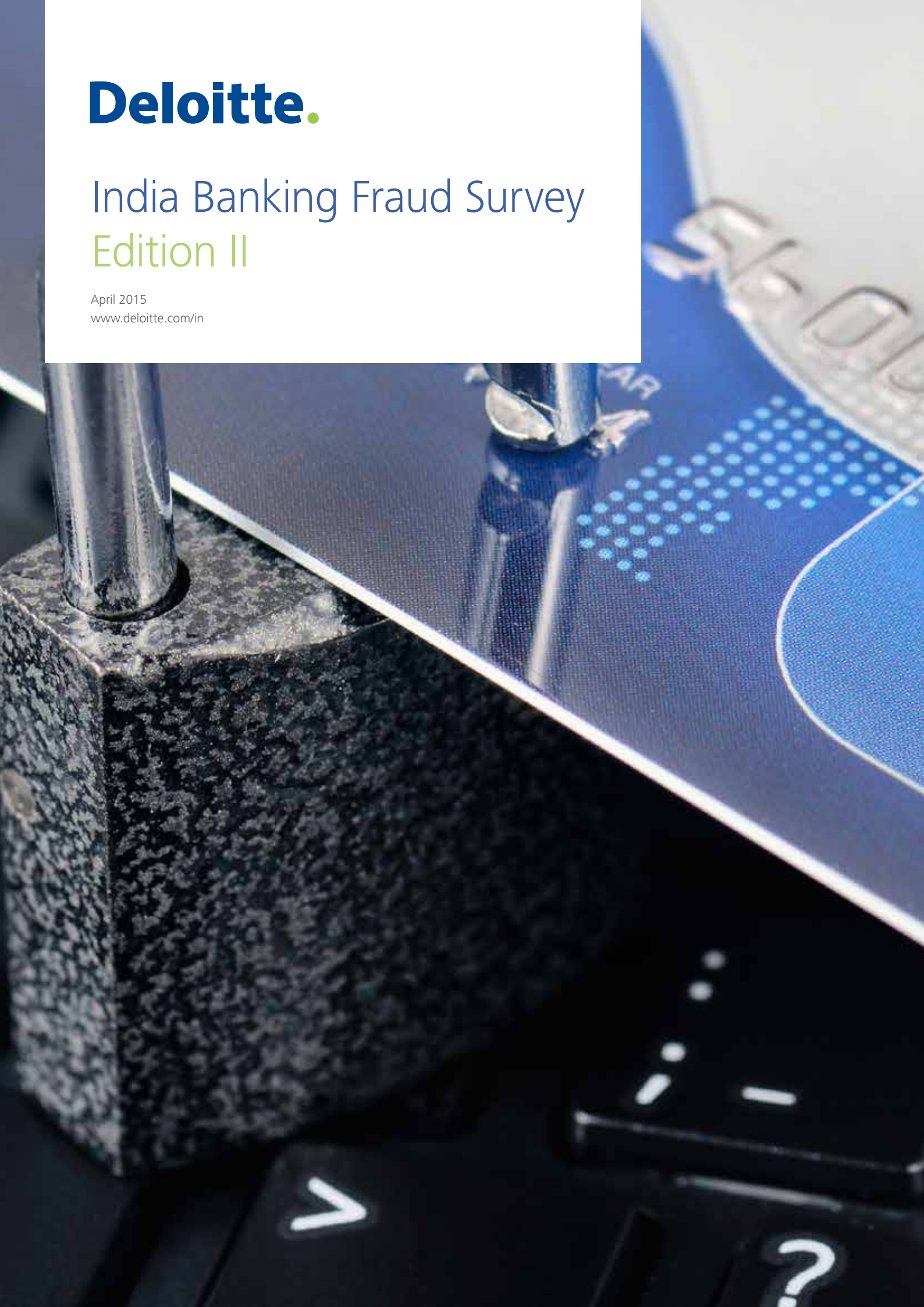
Deloitte.

India Banking Fraud Survey
Edition II

April 2015
www.deloitte.com/in



Foreword

T. M. Bhasin
Chairman, Indian Bank's Association (IBA)
Chairman and Managing Director, Indian Bank

Over the years, IBA has emerged as the voice of the Indian banking industry, and we have always aspired to proactively work for the growth and betterment of the banking and financial services industry, in a manner consistent with public good.

We are committed to accelerate the Indian Banking industry's growth through innovation, transformation, inclusion, and better governance. In the last few years, governance and compliance has taken precedence in fueling the economic growth of the nation as well as the sector, in line with our strong focus on accountability and transparency.

To support this ongoing effort, we believe that the Deloitte India Banking Fraud Survey 2015 ("survey") has tried to recognize what is currently working well for the industry and what areas need further work and scrutiny. While the need to improve proactive fraud risk mitigation strategies is paramount, the survey also details emerging fraud risks that are a reality in the banking sector today.

It is clear that while the sector has grown by leaps and bounds in the last few years, the growth in incidents of fraud and cybercrime has also continued, if not accelerated. I am therefore hopeful that this survey report will not only enhance awareness but also push organizations towards furthering their investments and efforts in the area of fraud risk management.

Preface

Rohit Mahajan,
Senior Director & Head
Deloitte Forensic

KV Karthik
Senior Director and Financial services Lead
Deloitte Forensic

The Indian banking sector is experiencing a plethora of changes as it gears up to meet international standards, while balancing its commitment to financial inclusion. The last two years have been particularly significant from a fraud risk management perspective, with the RBI issuing several directives aimed at improving governance and profitability levels among banks, by mitigating the risk of loan defaults and fraud.

The pace of change in the sector has left banks grappling with multiple fraud-related challenges. While financial crime appears to be a major concern for banks as the number of incidents and value of fraud rise, there appears to be a certain lag in the implementation of fraud risk management measures. With the current economic slowdown and increased use of technology, incidents of fraud are also expected to increase further, which has also been substantiated through our survey results. Continued reliance on manual controls to detect red flags and well known frauds such as diversion of funds and fraudulent documentation (leading to loan fraud) continue to impact the sector more significantly than cyber-crime and identity theft, which are dominating the global banking fraud landscape.

The proliferation of the use of the Internet for financial transactions warrants a baseline level of awareness and vigilance at all banks. However, it appears that the banks' own adoption of technology for internal controls and fraud risk management appears to be still work-in-progress. Frauds are detected primarily by customer complaints indicating that in spite of various anti-fraud measures adopted by banks, a significant number of frauds are being detected by means other than those under the anti-fraud control framework. For many years now, the RBI has asked banks to focus on KYC checks and customer data integration; however, it appears that most banks are still investing in this area and are yet to see results. We also observe that while there is sensitization to fraud at higher levels in the organization, the levels of awareness among operational level staff can be improved. Overall, the sector does not seem to be taking a holistic view towards fraud risk management and remains embroiled in day-to-day concerns. We believe the challenge for banks is to develop comprehensive fraud risk management controls that will not only prevent frauds but detect them as soon as they occur and respond to them.

This situation signals the need for quality guidance that banks can use to develop and implement a fraud risk management strategy. We believe that the Deloitte India Banking Fraud Survey report can provide not only greater clarity but also provide focus areas to banks on accelerating their fraud risk management efforts.

We hope that this report provides you with helpful insights into how banks are responding to today's challenges and fosters discussion that will help further enhance fraud risk management across the industry. We also wish to thank all our survey participants for their time and insights, without which this report would not have been possible.

Contents

India Banking Fraud Survey
Key Findings

State of Banking Sector Fraud

93% respondents indicated that there has been an increase in fraud incidents in the banking industry in the last two years

More than half of the respondents indicated that the banking industry has seen more than a **10%** increase in fraud incidents in the last two years

Top reasons for increase in fraud incidents:

- Lack of oversight by line managers/ senior management on deviations from existing processes
- Business pressures to meet unreasonable targets
- Lack of tools to identify potential red flags
- Collusion between employees and external parties

1 in every **4** institutions has witnessed more than **100** fraud incidents in the retail banking segment

The majority of retail banking segment respondents claim they suffered an average fraud loss of INR **10 lakhs**. In contrast, the average fraud loss in the non-retail segment was in the region of INR **2 crore**.

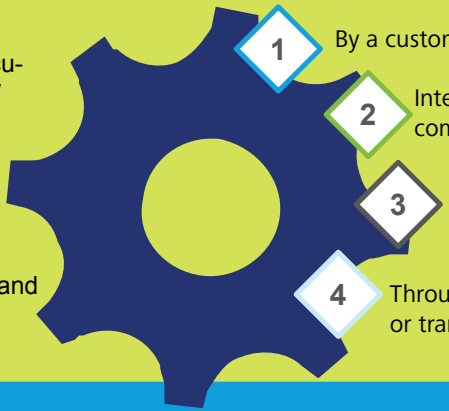
Common frauds observed:

Retail banking: 'Fraudulent documentation' and 'Over valuation/ absence of collateral'

Corporate banking: 'Diversion of funds' and 'Siphoning of funds'

Private banking: 'Identity theft' and 'Fraudulent documentation'

How is fraud discovered?

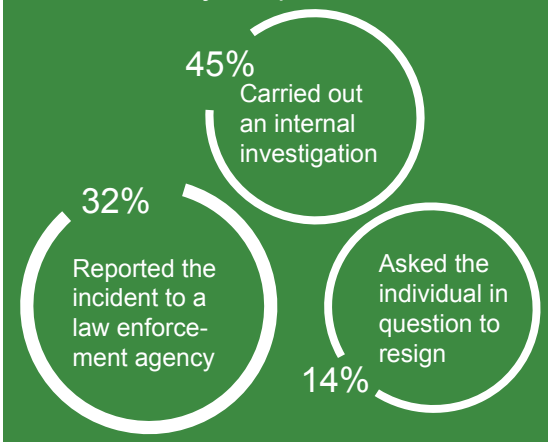


1. By a customer complaint
2. Internal whistleblower/ anonymous complaint
3. During account reconciliation
4. Through automated data analysis or transaction monitoring software

Average time taken to uncover a fraud incident: Less than 6 months by approx. 70% of the respondents

Majority of respondents said they were able to recover less than 25% of the reported fraud loss value

How did they Respond?



Challenges faced in the prevention of fraud

- Lack of customer and/ or staff awareness
- Difficult to integrate data from various sources
- Inadequate fraud detection tools and technologies

Preparedness to tackle fraud

Top three fraud risk management measures that have been implemented effectively by banks:

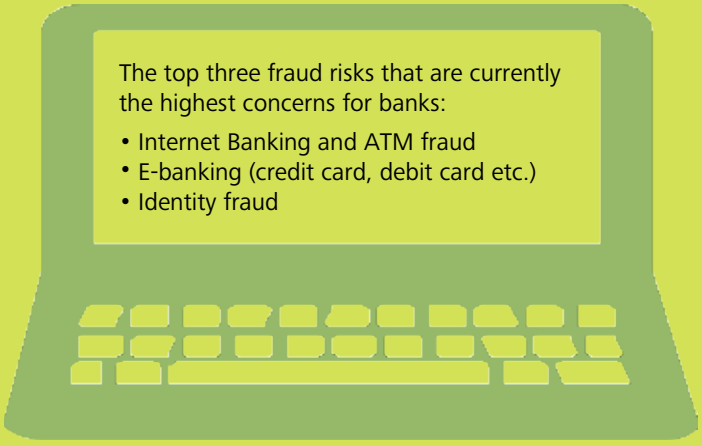
Customer screening against negative list

Fraud control strategies and policies

Employee code of conduct

Future trends

Technology to fuel fraud in the future



Greater investment towards the adoption of anti-fraud measures

83% of the respondents foresee an increase in their investments in adopting anti-fraud measures, especially in the areas of:

- Fraud detection and monitoring systems
- Upgradation of technology to combat cybercrime
- Fraud risk assessments and investigations

Section 1
Banking sector fraud on a rise

The big picture

Banking sector frauds have been in existence for centuries[1], with the earliest known frauds pertaining to insider trading, stock manipulation, accounting irregularity/ inflated assists etc. Over the years, frauds in the sector have become more sophisticated and have extended to technology based services offered to customers. The Indian banking sector too is experiencing the pain due to increase in fraud incidents with 93 percent of our survey respondents indicating that fraud has grown over the last two years.

A majority of survey respondents indicated that they have experienced more than 50 fraud incidents in the retail banking segment in the last two years (average fraud loss of around INR 10 lakh per incident) and an average of 10 fraud incidents in the non-retail segment (average loss amount close to INR 2 crore per incident). This is a significant jump compared to the survey findings of the previous edition of the Deloitte India Banking Fraud Survey report where only 40 percent of respondents claimed such fraud losses.

While most respondents have indicated an overall increase in frauds incidents across all banking segments, it comes as no surprise that retail banking has been identified as the major contributor to fraud, followed by corporate banking. As retail banking is more process as well as volume-driven, increased fraud incidents in this area should trigger a wider review of the process and controls to identify the root cause as these incidents could be just the tip of the iceberg.

Figure 1: What has been the percentage of change in fraud incidents encountered by the Banking industry as compared to the last two years?

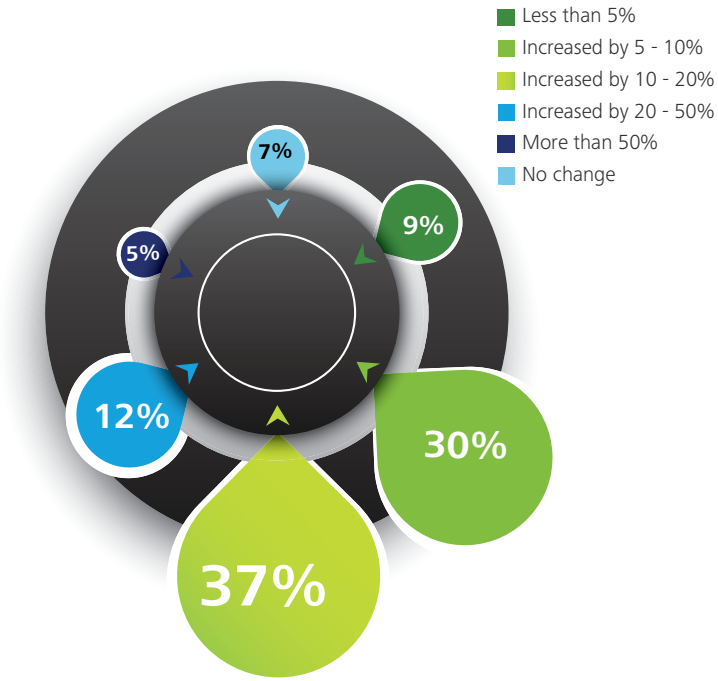
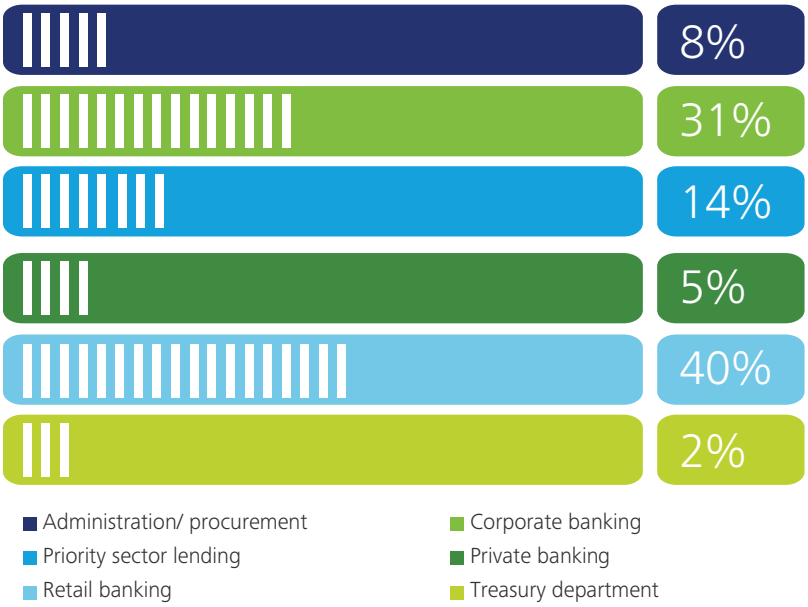
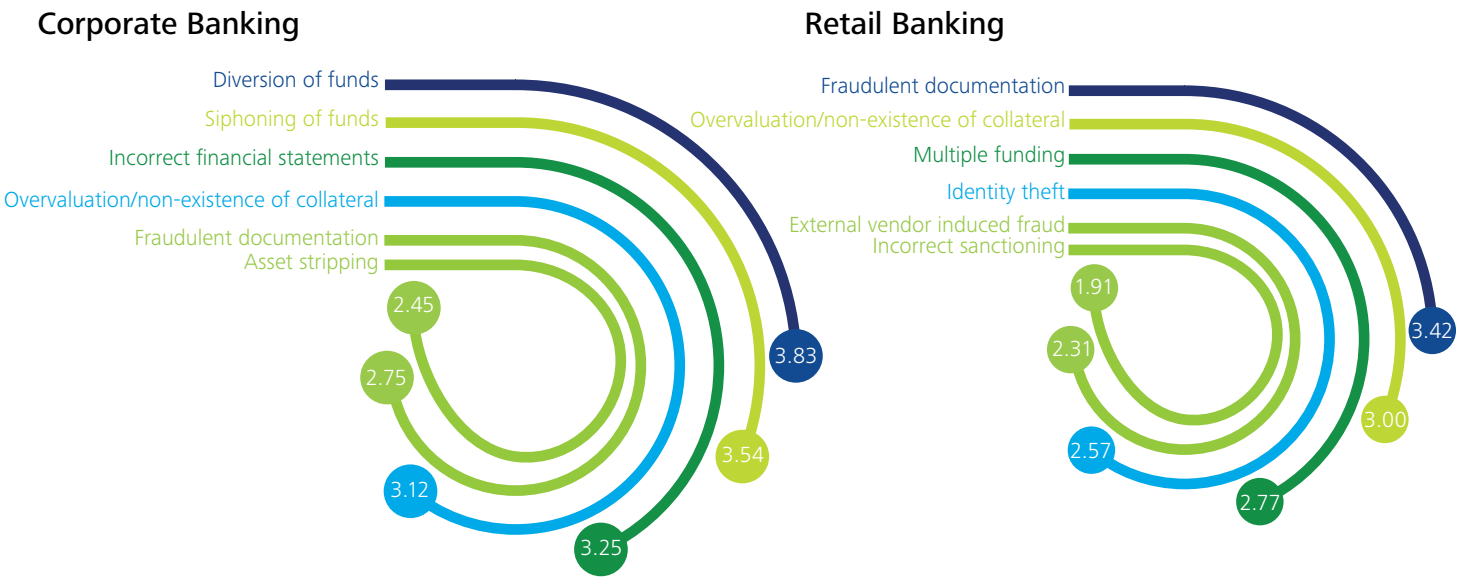


Figure 2: Which of the following areas in your organization have encountered fraud incidents?



[1] Source: Book titled 'William Duer and America's first Financial scandal', Authored by David J Cowen

Figure 3: Which of the following fraud incidents have been encountered in Corporate and Retail Banking?



Note: An aggregate of the responses received have been collated in this figure

Within retail banking, it is interesting to note that survey respondents highlighted 'fraudulent documentation' and 'overvaluation/ absence of collateral' as areas where incidents of fraud were most likely to occur. Whereas, within corporate banking, 'diversion of funds' has been identified as the biggest area where fraud incidents were encountered.

Retail banking is considered relatively more process-oriented, requiring significant control and meticulousness over the due diligence carried out while on-boarding a customer. Given the limited resources banks have to monitor these processes and adequately verify documents/ information, and the increasingly fragmented nature of customer information available, the risk of fraud becomes significantly high and banks need to realize the importance of investing in preventive mechanisms.

In case of corporate banking, the key challenge for a bank is to ensure that the borrower utilizes the funds for the purpose stated in the loan sanction, and periodically reports progress, while meeting the loan repayment criteria. While this may not appear to be as process driven as retail banking, the absence of standard processes and automation makes end use monitoring in corporate banking more challenging compared to the fraud risks in retail banking. The RBI's annual report of 2013-14 places NPAs from retail banking at 2 percent, whereas NPAs from corporate banking were at 36 percent[2]. Given the size of transactions in corporate banking and the challenges mentioned above, it is important that banks implement a robust monitoring mechanism post sanction and disbursement of facilities and be vigilant to early signs of stress in the borrower accounts.

[2] Source: RBI Annual Report 2013-14 http://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/RBIARE210814_FULL.pdf

What is contributing to the rise in fraud?

Fraud tends to be committed primarily due to the presence of three major factors: financial pressure, opportunity, and rationalization. While these factors are present in a growing economy, they can get exacerbated during an economic downturn, when margins are tight and profitability is a challenge. This has been clearly brought out in our survey results, where respondents have attributed the increase in fraud to the lack of oversight by line managers or senior management on deviations from existing process/ controls; business pressure to meet targets; and collusion between employees and external parties.

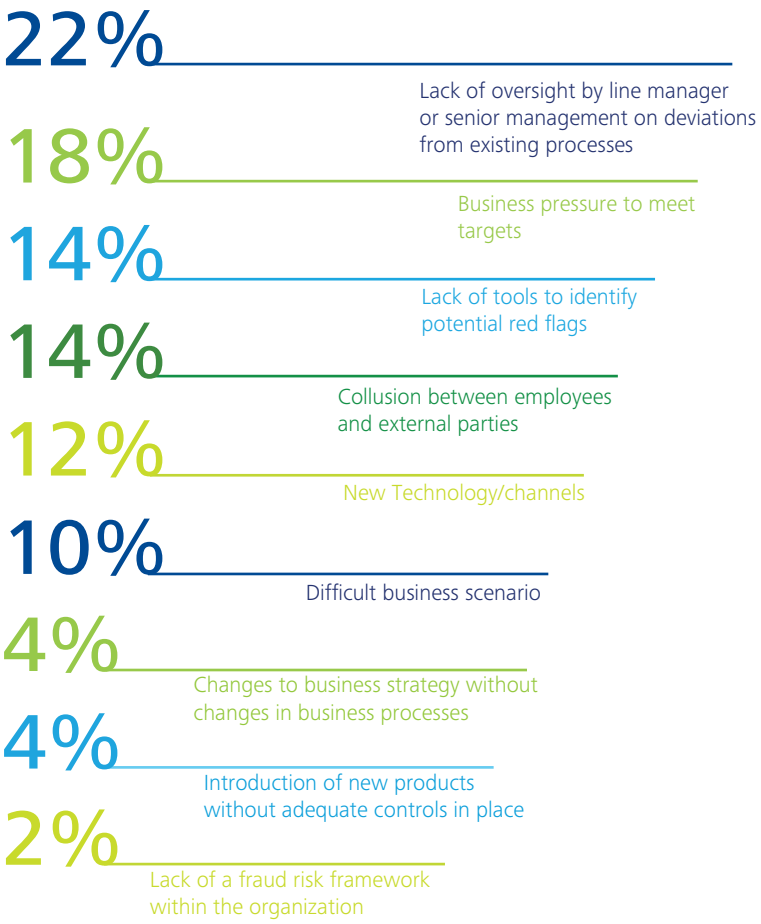
Lack of oversight by line managers/ senior manager on deviations from existing process/ controls

Poor internal controls, dilution of existing systems/ controls and non-adherence to procedures can increase the likelihood of frauds in banks. Based on our experience, the following are some instances where controls tend to be overlooked.

- Lack of segregation of duties: The same individual is responsible for making bank deposits, posting them to the accounts receivable system and performing monthly bank reconciliations
- Poor physical controls: Custody of security forms such as bank draft forms, deposit receipts and cheque books is handed over to counter staff without obtaining a written acknowledgement
- Low priority areas, such as internal/ inter-branch accounts tend to be less frequently monitored for oversight or malpractice.

In addition to the instances listed above, limited oversight is also a reason for fraud in areas such as loans and advances. Some examples include inadequate KYC checks on prospective borrowers by bank managers, and the subsequent limited monitoring of the use of funds loaned. Further in many cases, loans may be processed based on insufficient documentation/ wrong valuation of collateral. We also observe that banks are increasingly outsourcing these tasks – KYC, documentation support etc. – to third parties, which can further dilute the scope of managerial oversight.

Figure 4: What are the reasons for the increase in fraud incidents in your organization?



Business pressure to meet targets

One of the common reasons cited for limited oversight is the heightened pressure to exceed business targets that are often linked to compensation. Under the current economic climate of tepid credit growth, banks may face increased pressures to meet or exceed financial targets. With increased pressure, the risk of fraudulent activity can tend to escalate due to the sensitivities involved in cases of missed earnings or perceived bad news. With employee compensation increasingly being tied to performance, it may therefore drive individuals to achieve overly optimistic results.

Collusion between employees and external parties

Insider fraud, whether arising from coercion, collusion, or otherwise, are increasingly considered to be one of the most serious fraud threats faced by financial institutions. An aspirational work force can resort to unethical ways of meeting business targets, thereby putting the bank at risk to fraud and reputational damage. A number of instances of employee-external party collusion have been seen in recent incidents of payment fraud and account take-over.

"Fraud and its redressal is a major concern area for the banking sector and across all portfolios - retail, corporate, and priority sector. The State Bank of India has put in place frameworks that enhance the existing state of controls to deter fraud. In addition to these measures, it is also important to develop an organizational culture of zero tolerance towards fraud. Such a culture can, in the long term, fortify fraud risk management efforts at banks and help reduce incidents of fraud."

B Sriram
Managing Director & Group Executive (National Banking)
State Bank of India

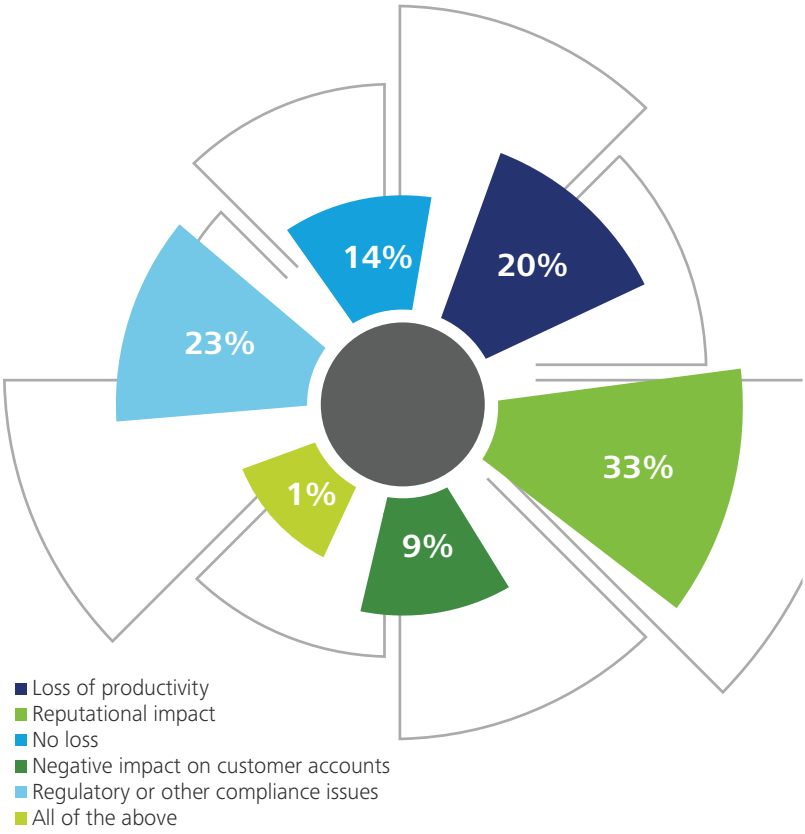
Impact of fraud

Some of the recent fraud incidents in India reported by the media relate to fixed deposits, loans disbursement or extending credit facilities for bribes, phishing and other internet/ ATM based frauds. These high-profile cases in recent times have shown that frauds not only undermine profits, operating efficiencies and reliability of services but can also have a severe impact on an organization's reputation. In addition to potential fines levied by regulatory bodies, it can have a negative impact on employee morale and investor confidence. Survey respondents have concurred with this.

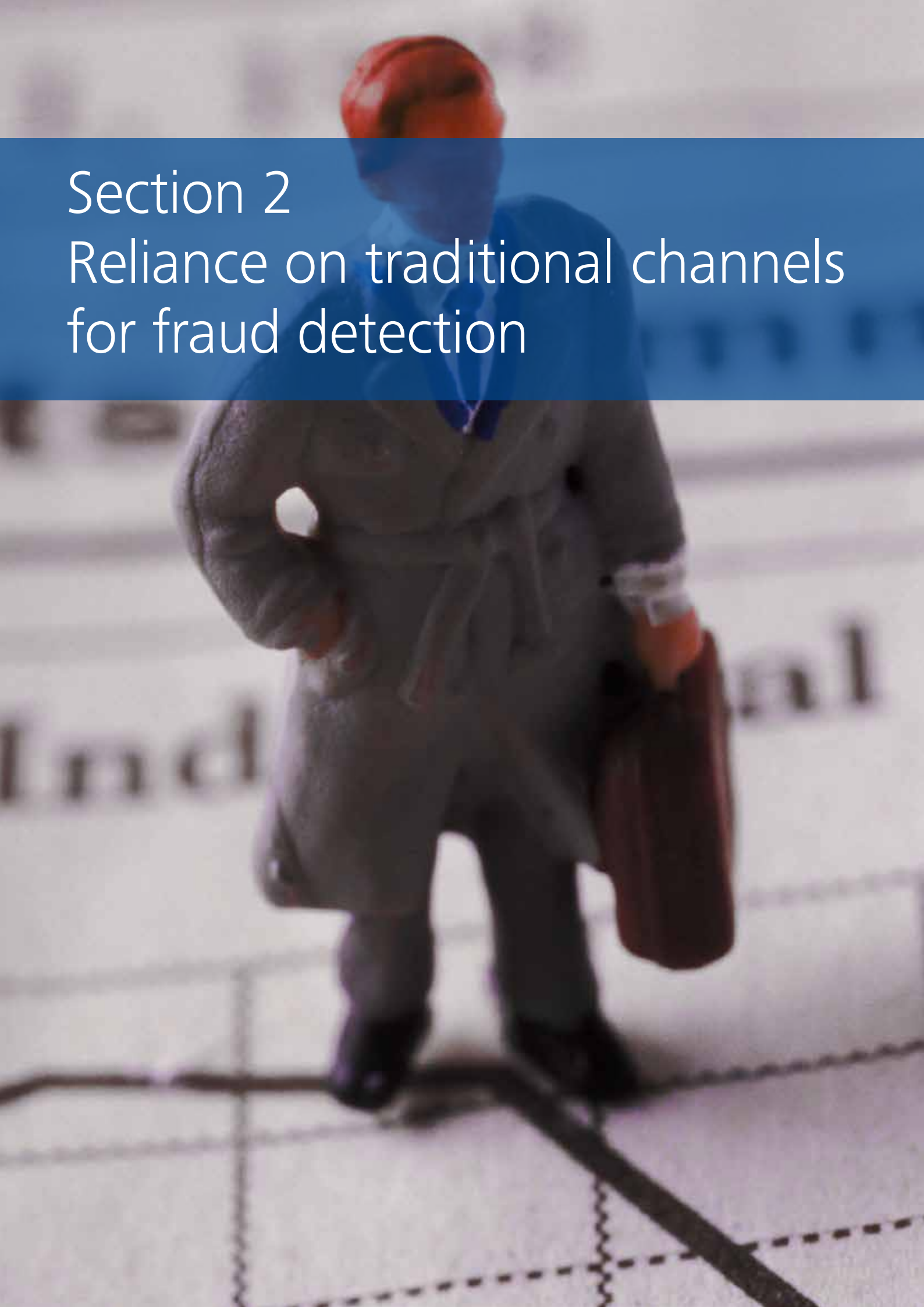
"…Any dent in the confidence of the stakeholders in the banking system will result in huge reputational and operational risks for the banks, adversely affect public perception and undermine faith in the financial system…."

Sashi Jagdishan
Finance Division
Corporate Office
HDFC Bank

Figure 5: What was the nature of the non-financial loss that your organization suffered, due to the impact/ incident of fraud?



Survey statistics also reveal that the frequency, volume and the gravity of instances of fraud has gone up over the past few years. More than half of the respondents indicated that they were able to recover less than 25 percent of the losses due to fraud. Combined with a rise in the number of fraud incidents and the loss incurred per incident, it is possible that fraud may be significantly impacting profitability and perhaps partially contributing to the rising NPA levels.



Section 2
Reliance on traditional channels for fraud detection

Unearthing fraud

Although organizations can never eliminate the risk of fraud entirely, it is important to have controls that can effectively detect and prevent fraud. Efficient internal controls and data analytics can help identify frauds faster and thereby help banks limit the losses incurred.

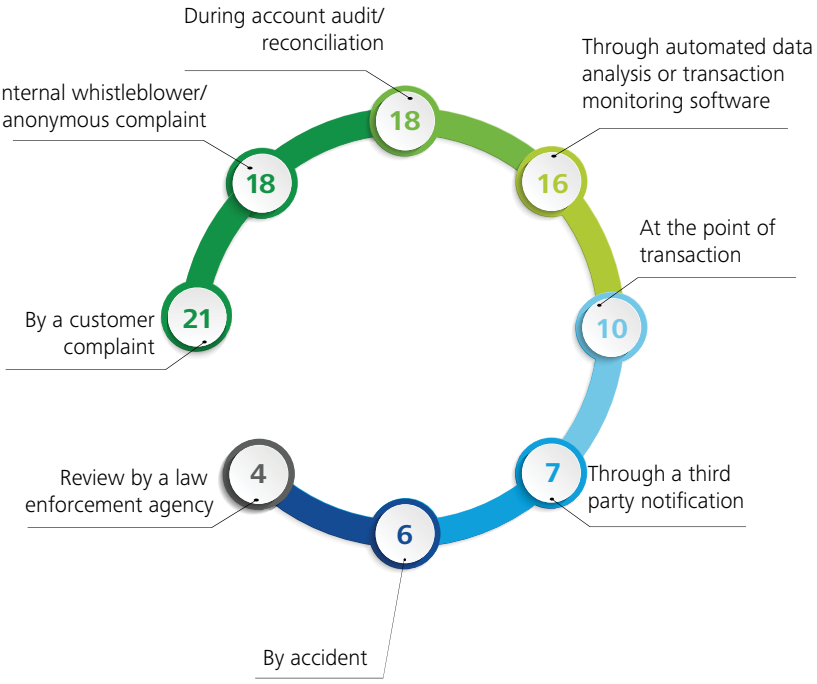
Survey respondents indicated that frauds in their organizations were most commonly detected through customer complaints, followed by an internal or external tip[3], which is in line with global trends.

The role of internal audit teams is expanding to include fraud risk management. An RBI circular on inspection and audit systems in banks[4] notes the failure of internal audit teams to highlight the existence of irregularities such as improper credit appraisal, disbursement without observing the terms of sanction, failure to exercise proper post-disbursement supervision, and suppression of information relating to unauthorized excess withdrawals. The circular has proposed a series of changes to the Internal Audit function to improve its effectiveness starting with expanding the coverage of the function itself. Internal Audit teams are expected to specifically report on the position of irregularities in branches, analyze and make in-depth studies of the corruption/ fraud prone areas,(such as appraisal of credit proposals, balancing of books, reconciliation of inter-branch accounts, settlement of clearing transactions, suspense accounts, premises and stationery accounts) during the course of their inspection; thereby leaving no scope for any malpractices/ irregularities remaining undetected. These appear to have borne some fruit as respondents have indicated that they rely heavily on audit/ reconciliation as one of their primary modes of fraud detection.

Despite these changes, the inherent nature of internal audits tends to be limited, relying on scrutinizing a small sample size for fraud and irregularity. In such cases, fraud may continue to be perpetrated, if the related transactions fall outside of the audit sample, making it difficult to detect. In our experience, frauds detected primarily through internal audit have existed on an average for 12-18 months, prior to detection, significantly increasing the fraud loss amounts and making recovery difficult.

Internal auditors should therefore, while planning their

Figure 6: How is a fraud incident involving your organization typically detected?



[3] Source: ACFE 2014 Global Fraud Study
[4] Source: RBI Master circular on Inspection and Audit Systems in Primary (Urban) co-operative banks, 2013

annual audit plan, consider the assessment of fraud risks and review the management's fraud mitigation capabilities periodically. They should also regularly and closely communicate with those responsible for risk assessment(s) in the organization to ensure that action, if required, can be taken in time. Internal auditors, other than spending adequate time and attention to evaluating the framework and internal controls related to fraud risk management, should also have a well-defined response plan to handle potential frauds uncovered during an internal audit assignment.

Around 30 percent of our survey respondents have indicated that it took them 6-24 months to detect fraud. Close to 22 percent of survey respondents said they could recover only up to 25 percent of the fraud loss amount. These statistics indicate a move towards reliance on multiple channels, including technology based channels, to detect fraud, as indicated by a significant percentage of respondents.

In this context it is interesting to note the use of whistleblowing channels by banks to detect fraud. According to the Association of Certified Fraud Examiners (ACFE), organizations with whistleblower hotlines experience frauds that are 41 percent less costly, and are able to detect frauds 50 percent faster compared to organizations that do not have such a channel[5]. However, in our experience we have observed that Indian companies tend to approach whistleblowing with a 'tick in the box' mentality, often resulting in ineffective and poorly managed whistleblower programs.

The success of a whistleblowing program lies in its adoption by employees and third parties such as customers and business partners. For Indian banks operating across different geographies, it becomes paramount to invest in a robust whistleblowing program that is not confined to one language, limited operating hours and selectively accessible to certain employees (e.g. only mid-level employees). Further, banks must institutionalize training programs to encourage employees to blow the whistle when they see or hear anything suspicious or seemingly unethical.

"The fraudster is always ahead of the controls or risk mitigants which will be put in place by the Banks. However, Banks have to be agile and think ahead of the fraudsters and put in place control measures quickly. The cat and mouse game has been going on in the past and will continue to be in future, but Banks have to devise ways to be ahead."

Sanjeeva Murthy
Executive Vice President
- Compliance
Kotak Bank

[5] Source: ACFE 2014 Global Fraud Study

Deloitte Point of View
Forensic Data Analytics - The new frontier to detect fraud

With banks facing heightened regulatory and public scrutiny in many countries, using advanced analytics to help identify potential fraud, committed by employees, customers, and third parties may be a strategic and operational imperative. Analytics has the potential to help banks refine the way they perform monitoring that will allow them to detect and identify potential fraud prior to the launch of a formal investigation/ inquiry.

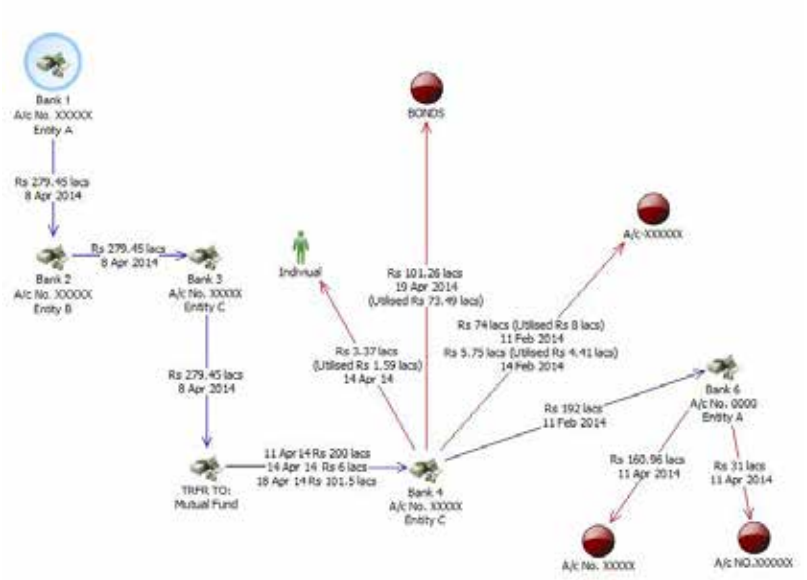
Banks can reshape their fraud detection efforts using advanced analytics and related tools, software and applications to obtain more efficient oversight. These steps can not only help enhance fraud deterrence, but also show regulators an enterprise-wide commitment to enforcing an effective anti-fraud strategy. The below chart shows some key methodologies and actions that banks can consider:

Methodology	Action	Benefits
Risk-based	• Define specific analytic tests based on results from risk assessments • Focus analytics on high-risk products and portfolios	• Management of exposed areas through targeted testing • Improved fraud mitigation planning
Constantly evolving	• Incorporate feedback from periodic reviews • Perform statistical analysis to create custom thresholds and apply sensitivity analysis for alert tuning	• Reduced false positives and risk of missed violations • Less human effort needed in the long-run
Predictive	• Use profiling and association of algorithms to couple high-risk entities with nature of fraudulent activity • Apply results from visual and text analytics to train models	• Enhanced ability to predict fraud and parties involved • Improved effectiveness of pattern recognition
Integrated	• Enhancing central datasets with data from additional departments • Combine structured and unstructured datasets in a single platform	• Greater insights and holistic view of operational data • Improved risk-scoring of analytic tests

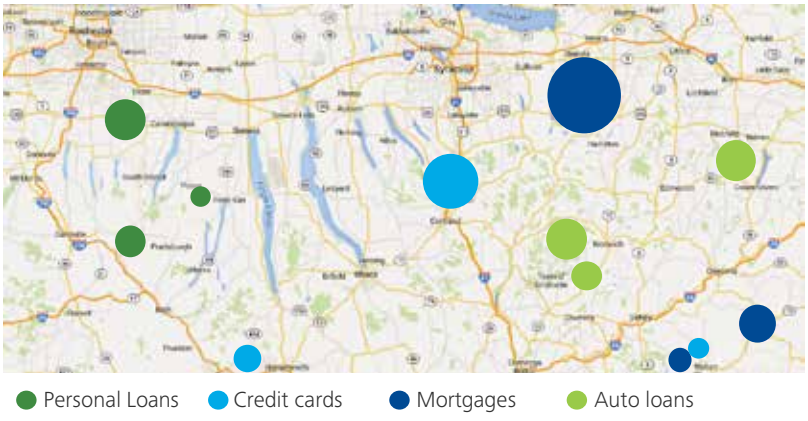
Another emerging tool that banks can use to detect frauds is data visualization. We are seeing global adoption of these technologies in leading banks. Built on the premise that human beings assimilate information better in visual format, than numerical format, this tool provides a visual representation of data patterns and outliers to translate multidimensional data such as frequency, time and relationships into an intuitive picture. This can be useful in identifying hidden and/ or indirect relationships, demonstrating complex networks involving multiple layers and/ or several intermediaries and tracking the movement of money especially in anti-money laundering investigations and diversion of funds by borrowers. Data can also be represented geo-spatially, to show interactions between data such as financial transactions, asset information, customer data and contracts, references to places, names and addresses.

Today, regulators are already beginning to use proprietary risk analytics to identify inconsistent investment returns, fraudulent valuations, and improper use of assets. While many banks may already be using analytics to uncover frauds, they can most likely benefit by expanding their capabilities to implement a fraud detection and deterrence strategy with a larger scope to include certain methodologies mentioned above.

Sample 1- Link analysis depicting fund movement/ transactions that reflect a money trail through multiple banks and bank accounts



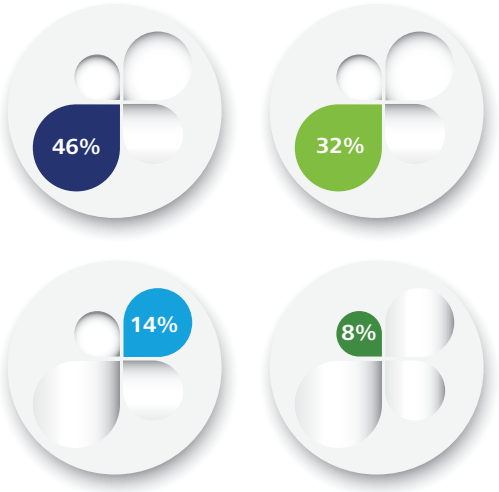
Sample 2 - Geo spatial data representation showing select locations with defaults across different product categories



Response to fraud

An organization's response to fraud is crucial as it has the ability to prevent future occurrences. Any response to fraud should be swift and effective so as to percolate the right message to employees. An RBI circular dated September 2009[6] requires banks to investigate frauds of large values with the help of skilled manpower in order to effectively take internal punitive action against the staff in question along with external legal prosecution of the fraudsters and their abettors, if required.

Figure 7: In your organization, what is the typical response to a fraud incident?



In line with RBI's recommendations, the majority of the survey respondents indicated that upon the detection of fraud, they carried out internal investigations, while others reported the incident to a law enforcement agency. It is interesting to note that only 8 percent of survey respondents indicated using an independent consultant to carry out investigations. While the responses received in our survey indicate that banks have set up a dedicated fraud investigative cell (elaborated in the next section), it appears to be hampered by the lack of dedicated technology tools for investigation. A little over 40 percent of survey respondents indicated they had not started implementing dedicated forensic technology tools for investigation, whereas, 20 percent of respondents had partially implemented these tools. Only 20 percent indicated that they had implemented forensic technology tools for investigation, and that these tools were effective (elaborated in the next section).

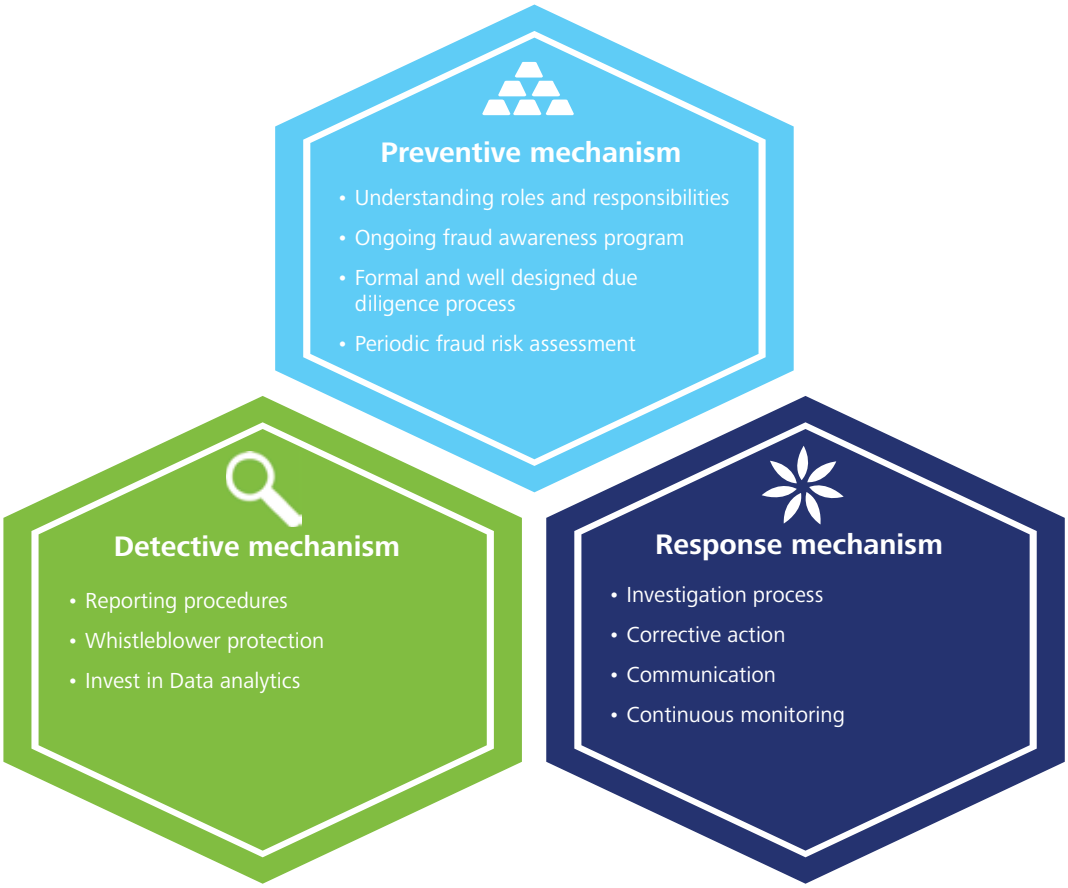
It is important to understand that fraud investigation requires specific skill sets like forensic accounting and technology to collect adequate evidence. While the evidence unearthed by a fraud investigation can vary on a case-to-case basis, typically, it needs to be relevant and comprehensive to be admissible in a court of law. Certain additional aspects such as the source of the evidence, a legitimate witness, electronic evidence and data etc., can all add credibility to the case. In the absence of these, organizations may not have the confidence to take legal recourse or action on the fraudster which could be one of the reasons why banks may not be reporting all the cases to law enforcement agencies.

[6] Source: RBI circular dated Sept 16, 2009 titled 'Fraud Risk Management System in banks – Role of Chairmen/ Chief Executive Officers': http://rbidocs.rbi.org.in/rdocs/notification/PDFs/DRAC160909.pdf

Section III
Fraud risk management at Banks

The current status of anti-fraud programs

The key to any anti-fraud program is to have a framework in place that will not only prevent fraud but also be able to detect fraud incidents in real time. However, the task of developing and maintaining such a robust enterprise-wide anti-fraud program with proactive monitoring components can be daunting for any organization. The key features which should necessarily be part of any organization's fraud risk management program include the following:



An effective fraud risk management solution can help banks manage fraud risks in a manner consistent with regulatory requirements, as well as with the entity's business needs and marketplace expectations. Through this survey, we asked banks about the various anti-fraud measures that they had adopted.

Survey respondents have highlighted that they face certain challenges in maintaining the efficiency of anti-fraud security controls at an enterprise-wide level, such as struggling to work across channels and/ or finding it difficult to integrate with applications/ tools (such as integrating online transactions and ATM transactions, and integration between retail banking, corporate banking and private banking transactions); however, over 80 percent of them find their current controls to be largely effective. Further, in terms of the implementation status of various anti-fraud programs, it is heartening to note that banks have progressed across several parameters compared to the last edition of our ssurvey, taking cognizance of the impact of fraud on their organization.

Figure 8: What is the status of the following measures in your organization?

Around 43 percent of the survey respondents appear to have an effective intelligence gathering mechanism, compared to 28 percent from our previous survey in 2012. Such an intelligence gathering mechanism can enable banks to identify weaknesses inherent to their process, and also be used to identify new threats hitherto unknown.

Only half of the survey respondents indicated having an effective risk assessment program; however, more than two-thirds of the survey respondents indicated that they have effective fraud control strategy and policies in place. A fraud control plan describes an organization's approach to controlling fraud. It includes actions to be taken to reduce the fraud risks identified through the fraud risk assessment process and assigns responsibility for their treatment. In case the fraud risks are not identified, the fraud prevention controls will be rendered inadequate, posing a challenge to fraud risk strategy at banks.

A significant proportion of survey respondents have indicated that employee background checks, while implemented in the organization, are not effective. In our experience, more often than not, employees who engage in unethical behavior or commit fraud tend to have a history of dishonesty. Pre-employment screening helps reduce the risk of employing people with a checkered past or those who claim to have qualifications they do not possess. It allows organizations to have greater confidence in the work ethics of their employees. We recommend that banks undertake the following pre-employment checks at the minimum:

- Confirmation of identity
- Police check for any convictions
- Residence/ address check
- Verification of qualifications claimed, and
- Employment check with previous employers

A quick analysis of the survey findings also indicates that banks need to immediately focus and speed up their efforts in the following areas:

- **Conduct regular fraud risk assessments**
  Existing processes within the bank must be regularly challenged to unearth gaps in the controls environment. Once this is done, the fraud risk exposure should be assessed periodically to identify specific potential schemes and events that the organization needs to mitigate. A good fraud risk assessment should necessarily answer three questions.
  - Am I aware of all the fraud scenarios in my

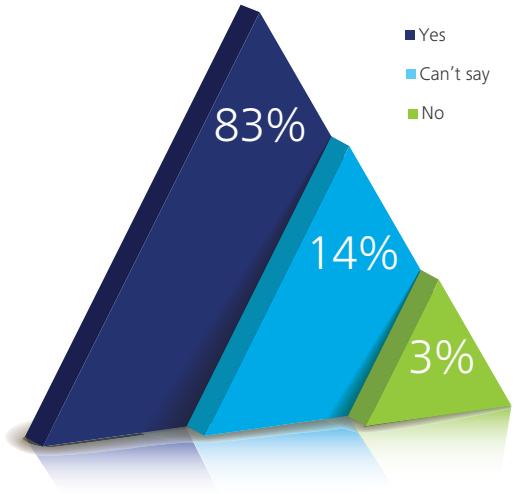
immediate environment?
- Do I have the necessary controls in place? And am I aware of how a potential fraudster can override or circumvent existing systems and controls?
- How is the effectiveness of controls monitored?

Further, a team of specialists can be instituted to collect information on the latest fraud schemes and test existing controls for vulnerability. Many banks may have such a team as part of their fraud investigation units.

- **Invest in an intelligence gathering mechanism**
  "Mystery Shopping" or "Market Intelligence" is an important element of fraud vulnerability assessment. This will enable banks to not only test the efficacy of controls to existing and new fraud scenarios but also have the ability to identify collusion, if any, which could result in circumvention of controls. This can also be leveraged in providing objective and accurate information on individuals and entities in the context of due diligence, litigation support, fraud, asset tracing and business investigations.

- **Use dedicated forensic tools during an investigation process**
  Today's business environment generates vast amounts of data. The key to a successful investigation is to not only manage this data and turn it into meaningful information, but also collect, preserve and analyze large and disparate data to support or refute facts and allegations of a case. Forensic tools can be used to navigate IT systems for evidence of malfeasance, such as information deletion, policy violations and unauthorized access. A wealth of information can be recovered from computers, including active, deleted, hidden, lost or encrypted files or file fragments which can be presented in a court of law. These include tools for forensic imaging, electronic discovery, data anomaly detection and records management which can help banks and their legal counsels in handling and analyzing large and complex data issues to help support their cases.

Figure 9: According to you, over the next two years, will the cost of anti-fraud measures (already adopted or to be adopted) in your organization increase?



Overall, a significant majority of respondents have indicated that they plan to invest in enhancing or implementing certain anti-fraud measures. While these costs largely cover elements that fall within a fraud risk management framework, it indicates that banks have realized that managing the risk of fraud is a continuous process that will need regular investment in order to meet current challenges as well as future fraud scenarios.

"In today's world, fraud is a continuous and rapidly evolving threat. There is no such thing as perfect security, so it is critically important that, we, the leaders in the field of financial crime prevention, work together to establish strong relationships and trust, to prevent, detect and respond to these threats effectively and efficiently."-

Dr. Sanjay Chougule
Global Head - Internal Audit
& Financial Crime Prevention
ICICI Bank Ltd.

Being proactive in managing the risk of fraud
To be or not to be, therein lies the question

Survey respondents indicated that the top three challenges faced by banks in preventing fraud were: lack of customer/ staff awareness; integration of data from various source systems; and inadequate fraud detection tools.

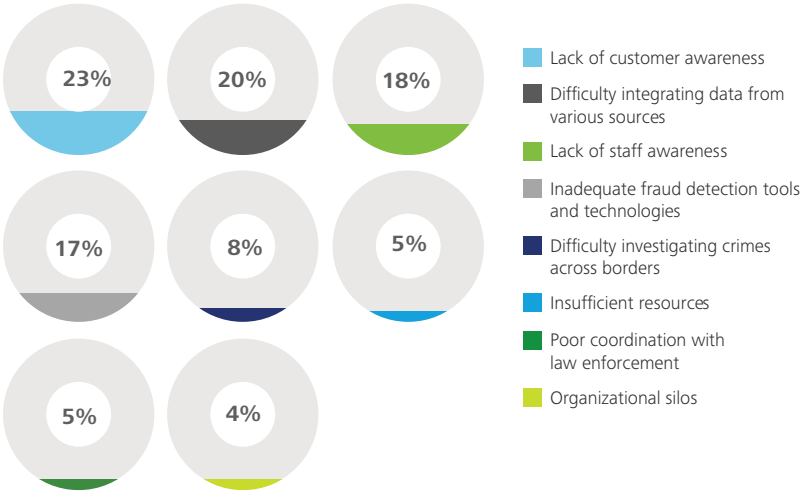
Employees are often the first ones to detect fraud. Organizations that have effective anti-fraud training programs experience less-costly losses, quicker resolutions of fraud cases, and an enhanced reputation for customer protection[7]. Targeted fraud awareness training for employees and managers is a critical component of a well-rounded program for preventing and detecting fraud. By implementing an effective fraud awareness program, management can harness the efforts of all staff members in its anti-fraud activities and can significantly reduce the cost of fraud within the organization. On a broad level, fraud awareness training should include following key topics:

- What is fraud and its effects on the organization
- Who perpetrates fraud and the fraud triangle
- How to identify fraud and the red flags to look out for (including behavioral signs)
- How to report fraud – the availability of channels and the process of dealing with complaints

As new regulations such as the Companies Act, 2013, place greater emphasis on the presence of a vigil mechanism to mitigate fraud risks, banks must ensure that their employees are aware of their organization's whistleblower program. In our experience, little effort is taken to sensitize employees on how their complaints are managed as well as how the whistleblower and suspect are dealt with throughout the investigation process. A clear and well-documented process for managing complaints can give greater confidence to employees to report suspicions.

For instance, the processes required to establish allegations involving junior or middle ranking staff tend to be fairly straightforward across most companies. Either internal or external investigators are appointed to review the matter and report the allegations that are raised. Usually, an appropriate senior manager will then deal with the matter after seeking advice from the Legal and/ or HR teams. However, if the allegation is against a senior manager, the situation can become a little complicated. Companies without a robust policy for dealing with such a scenario, mostly, run the risk of such investigations becoming compromised by senior management involvement or of such allegations being ignored. Employees need to be made aware of these detailed processes around how their complaints will be handled, so that they can gain trust in the system.

Figure 10: What are your organization's biggest challenges to fraud prevention?



On the technology front, banks have been struggling with a number of legacy applications catering to various aspects of their operations. These systems often result in islands of information with limited data in a format that may be incompatible with the rest of the organizational data. Additionally with sophisticated anti-fraud solutions requiring varied types of data inputs for analysis, banks are realizing that they may not have been capturing the requisite information in their existing system, resulting in lack of sufficient data for meaningful analytics.

[7] Source: ACFE 2014 Global Fraud Study

Getting it right: Defining the role of technology

In the realm of fraud detection, the ability to reveal relationships, transactions, locations and patterns can make the difference between uncovering a fraud scheme at an early stage as opposed to having it grow into a major incident. From money-laundering schemes to anti-corruption laws, from manipulating financial statements by reporting fictitious revenues to inappropriate sanctioning; forensic analytical tools can help explore data and quickly identify errors, irregularities and suspicious transactions embedded within your day to day business, thereby providing clarity to concerns raised by managers and employees.

According to the responses received, a little over half of the survey respondents appear to have implemented a dedicated fraud detection/ analytics solution. However, interestingly only one in every three respondents who has implemented such a solution appears to be entirely satisfied with it. In our experience, banks are trying to leverage their existing transaction monitoring tools for fraud monitoring. Many are of the opinion that existing tools in the market are expensive/ ineffective with a few indicating insufficiency of data for non-implementation.

It was interesting to note that a large number of respondents sought technology to help them either highlight red flags where controls have been circumvented or where controls need to be enhanced. In our opinion, this could be because banks have realized that 'deviation from existing controls by line managers/ supervisors' is one of the major causes of fraud in the sector. With technology available which can help banks detect these deviations in controls, the internal audit team can also leverage this solution to undertake forensic based audits[8], which could go a long way in enhancing the efficiency of detecting frauds in time.

Figure 11: Have you implemented a dedicated fraud detection/analytics solution to identify red flags?

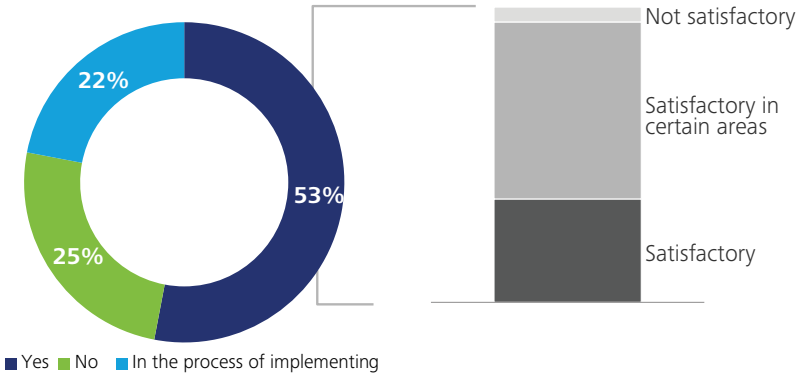
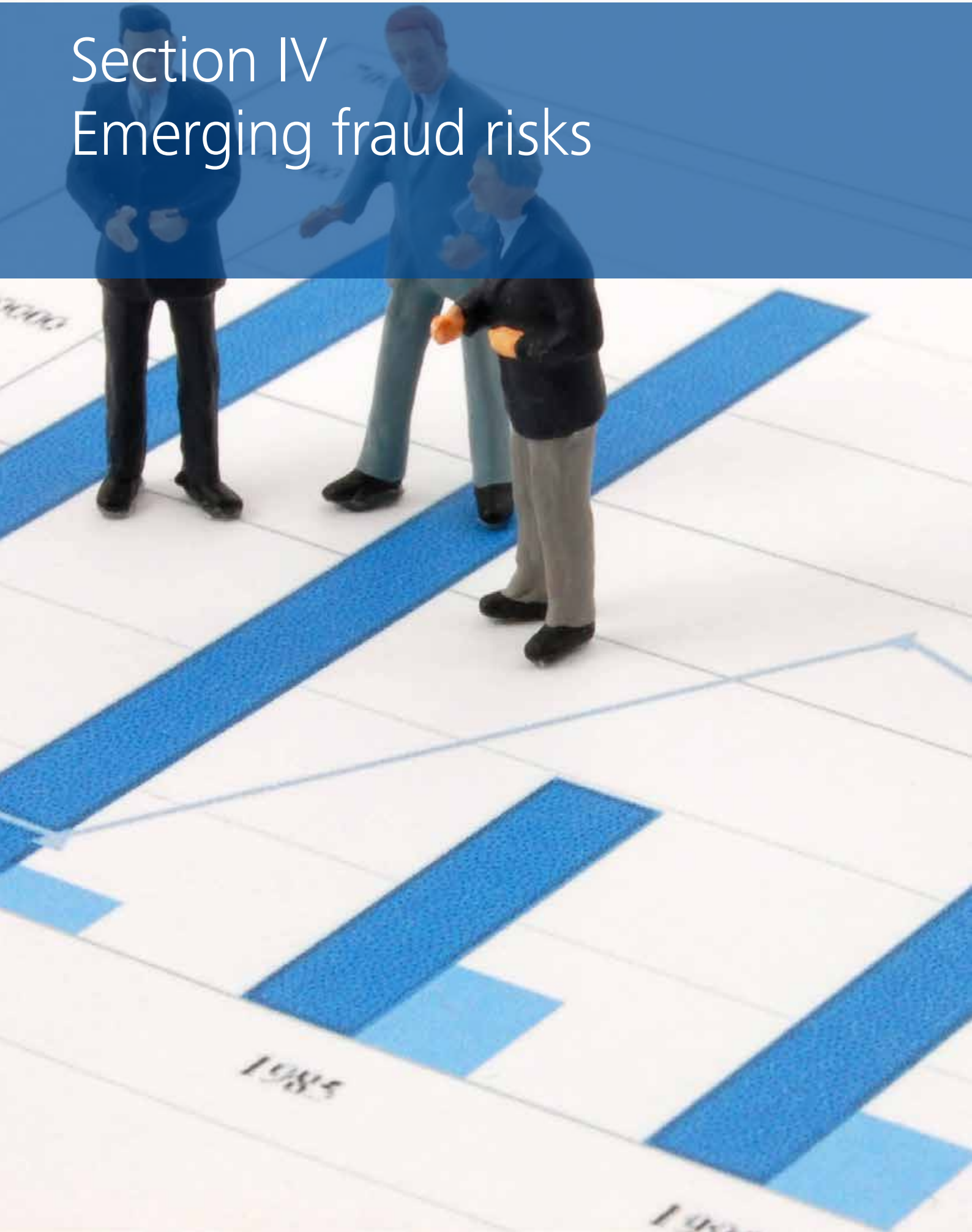


Figure 12: Which areas do you feel are the most important and are crucial to an anomaly detection solution?

[8] A forensic based audit approach is aimed at identifying the health of internal controls to prevent the risk of fraud and to safeguard assets. A regular internal audit is aimed at providing assurance to the company that the financial statements, in all material respects, fairly state the company's financial position as of a certain date.

Section IV
Emerging fraud risks



The advancement of technology in providing innovative services, combined with the explosive growth in internet banking, has permanently altered the business landscape and how banks manage this risk.

While cybercrime as a trend is not to be ignored, the actual losses are, at times, not significant enough to a bank's financials. The potentially greater impact from cybercrime is on customer and investor confidence, reputational risk, and regulatory impact that together add up to substantial risks for financial services companies. These issues ultimately have the potential to impact the reliability of a bank and in extreme cases may lead to a systemic crisis.

With organizations increasingly depending on technology, it is perhaps not surprising to find that cybercrime continues to increase in volume, frequency and sophistication. This includes ATM skimming, phishing/ vishing and misuse of credit and debit cards. Additionally, when asked to select the top three areas which were giving 'sleepless nights to bankers', it was no wonder that Internet Banking/ ATM fraud, E-Banking and Identity fraud were the top culprits. Interestingly, in addition to the above as a future fraud concern, mortgage portfolio also appears to be increasingly vulnerable to the risk of fraud.

These concerns appear to be in line with overall statistics available in India as well as the global trend. India itself, has witnessed a massive surge in cybercrime incidents in the last ten years - from just 23 in 2004 to 72,000 last year. As per the government's cyber security arm Computer Emergency Response Team-India (CERT-In) 62,189 cybersecurity incidents were reported in just the first five months this year [9].

On a global level, the likely annual cost to the economy from cybercrime is estimated to be more than $400 billion[10] . Additionally, a global survey of corporate C-level executives and board members (conducted last year) revealed that cyber risk was now the world's third corporate-risk priority overall [11]. Interestingly, the same survey from 2011 ranked cybersecurity as only the twelfth highest priority; a rapid rise explained perhaps in part by the evolving nature of the risks themselves.

Figure 13 A. Current fraud risks that are of high concern to banks/ financial institutions

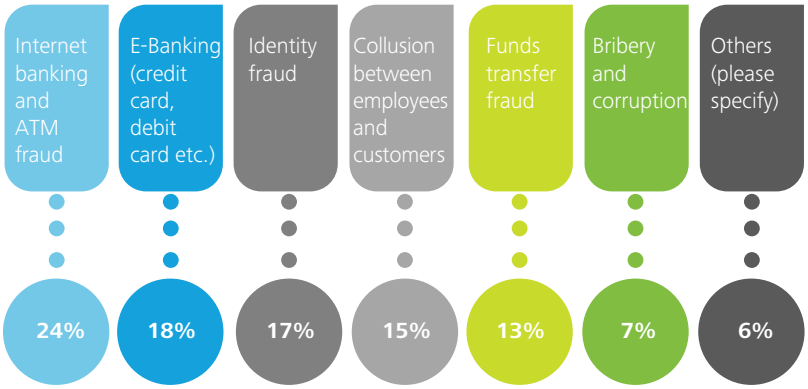


Figure 13 B.: New fraud trends that banks believe will be areas of concern in the next two years

Note: Out of the 15 options provided to the respondents, we have provided a synopsis of the top 4. Each individual option under 'Others' accounts for 3 to 4 percent each and has hence been clubbed.

- ATM/ ABM (skimming, ram raid etc.)
- Phishing/ vishing
- Mortgage
- Credit/ debit card
- Others (includes options such as third party POS skimming, account takeover fraud, IP theft, money laundering etc.)

[9] Source: Story reported on 17 Oct 2014 and published in The Times of India - http://timesofindia.indiatimes.com/tech/tech-news/Cybercrime-cases-shot-up-in-last-10-years-Telecom-minister/articleshow/44846265.cms

[10] Source: "Net losses : Estimating the global cost of cybercrime" published by McAfee in June 2014

[11] Source: "Risk Index 2013", Llyod's, July 2013

How are banks fighting this menace?

Business and technology innovations that the banking sector is adopting in their quest for growth are in turn presenting heightened levels of cyber risks. These innovations have likely introduced new vulnerabilities and complexities into the overall ecosystem. For example, the continued adoption of web, mobile, cloud, and social media technologies has increased opportunities for attackers. Similarly, the waves of outsourcing, offshoring, and third-party contracting driven by a cost reduction objective may have further diluted institutional control over IT systems and access points. These trends have resulted in the development of an increasingly boundary-less ecosystem within which banking companies operate, and thus a much broader "attack surface" for the threat actors to exploit[12].

It therefore becomes essential for organizations to try and keep pace with these new emerging threats. The root causes of cybercrime, according to the respondents, lie both internally as well as externally.

Cyberattacks on financial institutions are both increasingly diverse - and therefore unpredictable - and are also here to stay. Many of these continue to be driven, as we know, by financial gain, however the impact of cybercrime is not just financial, but also on the organization's reputation and customer confidence. With grave consequences such as these, financial institutions need to necessarily 'beef up' their security controls which currently, as per the responses received, appear to be focused on more traditional channels such as firewalls (and other perimeter controls), encryption including VPN, and anti-virus/ anti-malware solutions. Since the tactics used by cyber-criminals to target sensitive financial data are sophisticated and constantly changing. So, too, must the security controls financial institutions have in place, in order to not only stop the next cyber-threat, but also be resilient to such attacks.

An illustrative cyber threat landscape for the banking sector (Exhibit 2) suggests the need for firms to consider a wide range of actions and motives when designing a cyber-risk strategy. This requires a fundamentally new approach to the cyber-risk appetite and the corresponding risk-control environment.

Figure 14: Select the top three, out of the following, that you feel will be the greatest impact of a cybercrime attack

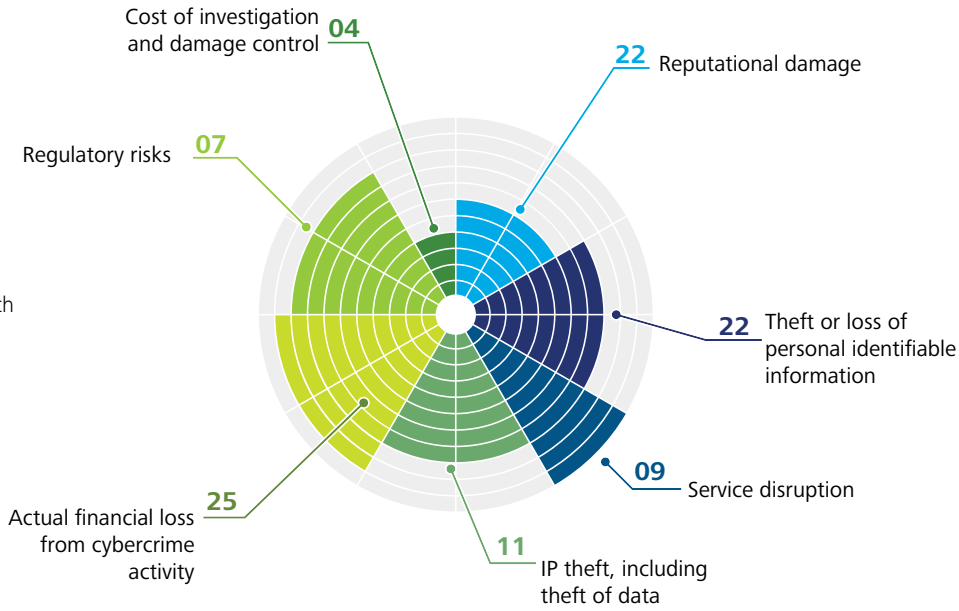


Exhibit 2: A diverse array of cyber attack actors and impacts

A typical cyber risk heat map for the banking sector

IMPACTS / ACTORS	Financial theft / fraud	Theft of intellectual property on strategy plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life / safety	Regulatory
Organised criminals	Very High	Low	Moderate	Moderate	Very High	Moderate	Very High
Hactivists	High	Low	Very High	High	Very High	Moderate	High
Nation - states	High	High	Very High	Very High	Very High	Moderate	Very High
Insiders	Very High	High	High	High	High	Low	High
Third parties	High	Low	Low	Low	Very High	Moderate	Very High
Skilled individual hackers	Very High	High	High	High	High	Moderate	High

Very High High Moderate Low

Source: Deloitte Center for Financial Services analysis

[12] Acknowledgment: "Transforming cybersecurity, New approaches for an evolving threat landscape", Deloitte Center for Financial services, Published in 2014

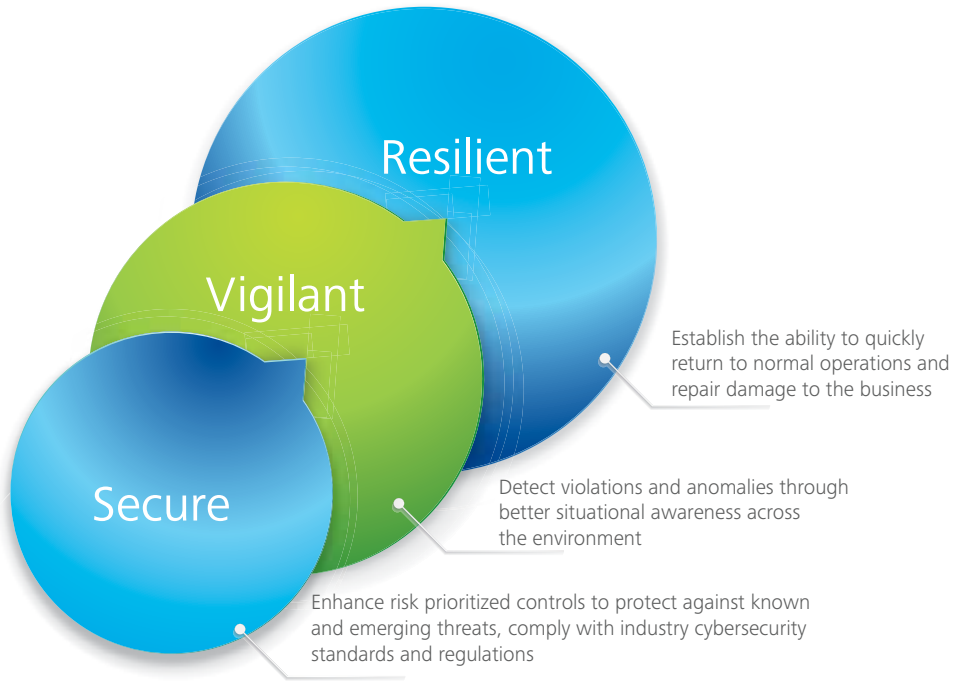
It was however encouraging to note that respondents have started actively addressing this threat on three fronts:

1. They are not only monitoring these threats by creating a separate in-house team of specialists, but also organizing regular awareness trainings/ workshops and periodic fraud risk assessments.
2. Additionally, banks are securing their boundaries by investing in firewalls, increased access management technology and database security tools including scanners. One of the reasons for increased spending in technology could be attributed to this.
3. Given the fact that banks have identified both internal and external factors as key culprits, one of the key risk management principles to consider is 'customer awareness'. While banks are undertaking customer education on the 'Do's and Dont's' of using internet banking and making transactions through credit cards/ ATM facilities, there needs to be a lot more awareness creation. RBI is cognizant of this fact and has insisted on twin factor authentication for all transactions over the internet, which can help lower frauds in online transactions. However, it would also have a positive impact to have an industry body undertaking such a program at a national level. This body can not only help in data dissemination (at an industry level) but also provide recommendations to banks on the issues faced by the industry including remedial measures. This is also important to ensure that customers feel safe while utilizing channels which have not only helped banks lower their overall cost on transactions but also in penetrating into newer markets through innovative products.

Deloitte Point of View – Managing cyber risks

The relationship between a fraudster and victim can be likened to a cat-and-mouse game, in which each side perpetually learns and adapts, leveraging creativity and knowledge of the other's motives to develop new offensive tactics and defensive postures. The relatively static compliance or policy-centric approaches to security found in many financial institutions may be outdated. Today's industry needs to create a dynamic, intelligence-driven approach to cyber risk management not only to prevent, but also detect, respond to, and recover from the potential damage that results from these attacks.

Banks have traditionally focused their investments on becoming secure. However, this approach is no longer adequate in the face of a rapidly changing threat landscape. Banks should consider building cyber risk management programs to achieve three essential capabilities: the ability to be secure, vigilant, and resilient



Source: Deloitte Center for Financial Services analysis

Being Secure

A good understanding of the known threats and controls, industry standards, and regulations can guide financial services firms to secure their systems by design and implementation of preventative, risk-intelligent controls. Based on leading practices, banks can build a "defense-in-depth" approach to address known and emerging threats. This involves a number of mutually reinforcing security layers both to provide redundancy and potentially slow down the progression of attacks in progress, if not prevent them.

Becoming vigilant

Early detection, through the enhancement of programs to detect both emerging threats and the fraudster's moves, can be an essential step towards containing and mitigating losses. Incident detection that incorporates sophisticated, adaptive, signaling, and reporting systems can automate the correlation and analysis of large amounts of IT and business data, as well as various threat indicators, on an enterprise-wide basis. Banks' monitoring systems should work 24/7, with adequate support for efficient incident handling and remediation processes.

Building resilience

Resilience may be more critical as destructive attack capabilities gain steam. Banks have traditionally planned for resilience against physical attacks and natural disasters; cyber resilience can be treated in the same way. Banks should consider their overall cyber resilience capabilities across several dimensions. First, systems and processes can be designed and tested to withstand stresses for extended periods. This can include assessing critical online applications for their level of dependencies on the cyber ecosystem to determine vulnerabilities. Second, banks can implement good playbooks/ guides to help triage attacks and rapidly restore operations with minimal service disruption. Finally, robust crisis management processes can be built with participation from various functions including business, IT, communications, public affairs, and other areas within the organization.

Though financial institutions may acknowledge the magnitude of the problem that cyber risks pose, not just to them but also to the systemic stability of the market, this imperative is not always adequately recognized or accounted for across the enterprise. A deeper analysis of the successes and failures of cyber threat programs may suggest some of the following potential actions that leaders can take to develop a more comprehensive organizational approach to cyber risk management:

1. Address the organizational challenges with decisive actions that recognize cybersecurity as a strategic business problem, not just an "IT issue"
2. Cyber risk strategy to be driven at the executive level as an integral part of the core company strategy
3. A dedicated cyber threat management team to be established for a dynamic, intelligence-driven approach to security
4. A focused effort to be placed on automation and analytics to create internal and external risk transparency
5. People and culture - The "people" link in the defense chain can be strengthened as part of a cyber-risk aware culture.

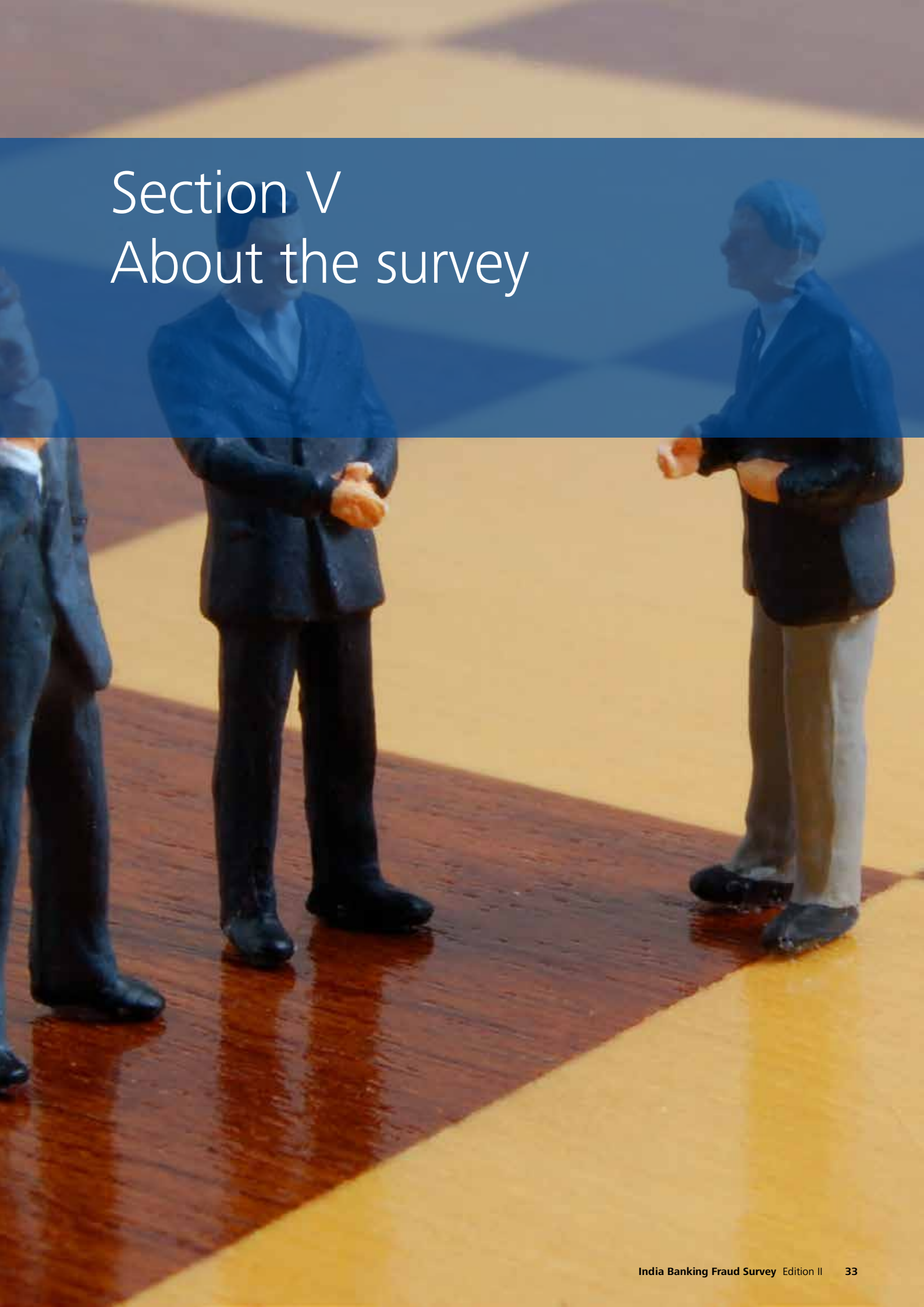
Conclusion

While fraud is not a subject that any organization wants to deal with, the reality is that most organizations experience fraud to some degree. The important thing to note is that dealing with fraud can be constructive, and forward-thinking, and can position an organization in a leadership role within its industry or business segment. Strong, effective, and well-run organizations exist because the management tends to take proactive steps to anticipate issues before they occur and to take action to prevent undesired results.

It should be recognized that the dynamics of any organization requires an ongoing reassessment of fraud exposures and responses in light of the changing environment an organization encounters. Especially given the unrelenting pace of regulatory change within the banking sector, these stricter regulatory requirements are demanding more attention from management, affecting the profitability of different lines of business, and increasing costs of compliance. Financial institutions therefore, should consider how their business models will be affected by current and potential future new requirements, and whether their risk management programs have the ability to respond flexibly to the ongoing process of regulatory change.

Financial institutions that have the ability to respond flexibly to the continuing series of regulatory changes, coupled with effective risk governance, strong analytical capabilities, and clear and consistent risk data, may be better placed to steer a steady course though the ever-shifting risk management landscape. A proactive approach to managing the risk of fraud is one of the best steps organizations can take to mitigate their exposure to fraudulent activities. Although complete elimination of all fraud risks is most likely unachievable or uneconomical, organizations can take positive and constructive steps to reduce their exposure. The combination of an effective fraud risk governance, a thorough fraud risk assessment, strong fraud prevention and detection strategies (including specific anti-fraud control processes), as well as coordinated and timely investigations and corrective actions, can significantly mitigate fraud risks. The important element to remember therefore is that with evolving fraud threats, banking institutions' defensive strategies also need to necessarily keep up. Firms that are able to institutionalize compliance in an effective and efficient manner could create competitive advantages, allowing them to best pursue their growth agenda.

Section V
About the survey



This report presents the key findings from the second edition of Deloitte's ongoing assessment of fraud and risk management practices survey in the financial services industry in India. The survey was conducted over two months from August 2014 to September 2014, to gather the views of key people/ senior management responsible for compliance and fraud risk management from varied financial institutions based in India.

- Financial institutions who participated in the survey included private, public and multi-national banks in India
- The institutions had total combined assets of more than INR 2 Lakh crore and represented a range of asset sizes. The majority of the respondents were primarily with an asset base of more than INR 5,000 crore.
- Responses were received from senior management responsible for compliance or managing the risk of fraud in their organization

The previous edition of this survey was released in 2012; where relevant, this report compares the current results with those from the 2012 survey.

Contacts

Rohit Mahajan
Senior Director and Head
Deloitte Forensic
Tel: +91 22 6185 5180
Email: rmahajan@deloitte.com

KV Karthik
Senior Director and FS Lead
Deloitte Forensic
Tel: +91 22 6185 5212
Email: kvkarthik@deloitte.com