turnitin **Turnitin Raport privind originalitatea**

412 de Ecoforum 2016 / 1

De la Quick Submit (Quick Submit)

Procesat la 26-mai-2016 14:44 EEST
ID: 678564645
Numărul cuvintelor: 10252

Indice de similitudine	Similitudine în funcție de sursă	
61%	Internet Sources:	54%
	Publicații:	18%
	Lucrările studentului:	32%

surse:

1 8% match (Internet de la data de 23-nov.-2015)
http://www.business-and-management.org/library/2009/4_3--1-21-Khanna,Arora.pdf

2 6% match (Internet de la data de 30-nov.-2014)
http://www.eajournals.org/wp-content/uploads/AN-EMPERICAL-INVESTIGATION-OF-THE-RELEVANT-SKILLS-OF-FORENSIC-ACCOUNTANTS.pdf

3 3% match (Internet de la data de 18-sept.-2013)
http://psalegal.com/upload/publication/assocFile/BankingLawsBulletin-IssueXV.pdf

4 3% match (Internet de la data de 29-iun.-2009)
http://businessfinancemag.com/article/beating-back-fraud-0201?page=0%2C6

5 3% match (Internet de la data de 19-mai-2014)
http://www.acl.com/pdfs/DP_Fraud_detection_BANKING.pdf

6 2% match (Internet de la data de 16-mar.-2016)
http://www.virtusinterpress.org/IMG/pdf/RGC__Volume_4_Issue_2_2014_Continued1_.pdf

7 2% match (Internet de la data de 18-oct.-2015)
http://www.inc.com/keith-mueller/technology-shaping-the-fight-of-fraud-in-2015.html

8 2% match (lucrările studenților la data de 13-mar.-2016)
Submitted to University of Maryland, University College on 2016-03-13

9 2% match (Internet de la data de 01-aug.-2015)
http://www.pwc.in/en_IN/in/assets/pdfs/publications/2015/current-fraud-trends-in-the-financial-sector.pdf

10 2% match (Internet de la data de 12-dec.-2013)
http://ejbss.com/Data/Sites/1/marchissue2013vol12/ejbss-1208-13-corporateaccountingscandalatsatyam.pdf

11 1% match (publicații)
"Pvt banks see more fraud cases than public ones.", DNA (Daily News & Analysis), Jan 9 2012 Issue

12 1% match (Internet de la data de 28-oct.-2013)
http://www.accentureoutsourcing.ie/us-en/Pages/insight-protecting-customer-fighting-bank-fraud-new-environment.aspx

13 1% match (lucrările studenților la data de 08-sept.-2015)
Submitted to Nelson Marlborough Institute of Technology on 2015-09-08

14 1% match (Internet de la data de 29-aug.-2015)
http://www.ajbmr.com/current-issue/60

15 1% match (Internet de la data de 05-oct.-2014)
http://www.bjournal.co.uk/paper/BJASS_15_1/BJASS_15_01_02.pdf

16 1% match (Internet de la data de 22-mar.-2016)
http://ijarcsse.com/docs/papers/Volume_4/12_December2014/V4I12-0363.pdf

17 1% match (Internet de la data de 12-aug.-2015)
http://www.dnaindia.com/money/report-banks-no-safe-havens-for-your-money-2075581

18 1% match (publicații)

Quah, J.T.S., "Real-time credit card fraud detection using computational intelligence", Expert Systems With Applications, 200811

19 1% match (Internet de la data de 09-ian.-2016)
http://www.ey.com/Publication/vwLUAssets/Fraud_and_corporate_governance_changing_paradigm_in_India/$FILE/Fraud_and_corpora

20 1% match (Internet de la data de 28-mar.-2016)
http://marciegeffner.blogspot.com/2014_06_01_archive.html

21 1% match (Internet de la data de 04-ian.-2015)
http://www.ca.com/us/lpg/combat-bank-fraud.aspx

22 1% match (Internet de la data de 31-dec.-2014)
http://pgpbf.bsebti.com/news_fbs.html

23 1% match (Internet de la data de 13-mar.-2016)
http://trak.in/tags/business/2015/03/23/psu-bank-frauds-india/

24 1% match (Internet de la data de 15-oct.-2014)
http://anale.steconomiceuoradea.ro/volume/2012/n2/097.pdf

25 1% match (publicații)
Bielski, Lauren. "Keeping check fraud in check: recent report looks at the marketplace of fraud prevention.(Check frau", ABA Banking Journal, August 2004 Issue

26 1% match (Internet de la data de 13-iul.-2012)
http://onlinebankbanking.com/117830-Ten-ways-to-tackle-bank-frauds-in-India.html

27 < 1% match (Internet de la data de 17-nov.-2013)
http://www.forbes.com/sites/steveculp/2012/11/30/enlisting-customers-in-managing-cyber-fraud-risks/

28 < 1% match (lucrările studenților la data de 17-iun.-2014)
Submitted to Alliance University on 2014-06-17

29 < 1% match (lucrările studenților la data de 07-mai-2015)
Submitted to Gujarat National Law University on 2015-05-07

30 < 1% match (Internet de la data de 09-apr.-2014)
http://www.business-standard.com/article/finance/fraud-at-public-sector-banks-a-rampant-occurrence-113112700132_1.html

31 < 1% match (Internet de la data de 22-nov.-2013)
http://deloitteblog.co.za/tag/corruption/

32 < 1% match (Internet de la data de 17-oct.-2015)
http://www.seair.co.in/dData/RBI/156628.pdf

33 < 1% match (Internet de la data de 18-mar.-2014)
http://loansforbadcreditinstantdecision.fastloansnocreditchecktoday.com/posts/direct+loans+gov.html

34 < 1% match (lucrările studenților la data de 28-oct.-2015)
Submitted to Stefan cel Mare University of Suceava on 2015-10-28

35 < 1% match (Internet de la data de 15-apr.-2016)
http://indianjournals.com/ijor.aspx?article=002&issue=1&target=ijor%3Ajcmt&volume=5

36 < 1% match (lucrările studenților la data de 26-apr.-2014)
Submitted to University of Maryland, University College on 2014-04-26

37 < 1% match (Internet de la data de 08-ian.-2016)
http://www.customerxps.com/financial-fraud-newsletter.php?mid=8&yid=2015

38 < 1% match (lucrările studenților la data de 27-mar.-2007)
Submitted to University of Glamorgan on 2007-03-27

39	< 1% match (Internet de la data de 16-iun.-2015) http://www.newslookup.com/Asia/India/page1513
40	< 1% match (lucrările studenților la data de 09-dec.-2006) Submitted to University of Maryland, University College on 2006-12-09
41	< 1% match (Internet de la data de 07-sept.-2012) http://www.oppapers.com/essays/Fraud-Management/515742
42	< 1% match (Internet de la data de 24-dec.-2015) http://docslide.us/documents/white-collar-crimes-5584511cd6323.html
43	< 1% match (lucrările studenților la data de 01-feb.-2015) Submitted to Manipal University on 2015-02-01
44	< 1% match (lucrările studenților la data de 28-mar.-2014) Submitted to Nottingham Trent University on 2014-03-28
45	< 1% match (Internet de la data de 30-dec.-2014) http://ijern.com/Editorial-Board/1001.pdf
46	< 1% match (lucrările studenților la data de 24-mar.-2014) Submitted to Amity University on 2014-03-24
47	< 1% match (publicații) Banks, David G., "The fight against fraud: a look at best practices used in the effort to defeat corporate fraud.(Cove", Internal Auditor, April 2004 Issue
48	< 1% match (lucrările studenților la data de 01-feb.-2016) Submitted to University of Glamorgan on 2016-02-01
49	< 1% match (Internet de la data de 21-sept.-2015) http://www.dynamicciso.com/blog-details/5f2c22cb4a5380af7ca75622a6426917.html
50	< 1% match (Internet de la data de 24-iul.-2015) http://dc.asianage.com/business/banking-sector-frauds-have-gone-over-10-cent-deloitte-796
51	< 1% match (Internet de la data de 25-oct.-2012) http://www.ijera.com/papers/Vol2_issue2/DU22738742.pdf
52	< 1% match (Internet de la data de 11-nov.-2014) http://news89.com/indian-economy-lost-rs-6600-cr-due-to-frauds-in-fy12-ey/
53	< 1% match (Internet de la data de 05-mar.-2016) http://m.scirp.org/papers/OJAcct/30220
54	< 1% match (lucrările studenților la data de 31-iul.-2012) Submitted to Utica College on 2012-07-31
55	< 1% match (lucrările studenților la data de 12-feb.-2016) Submitted to University of Bedfordshire on 2016-02-12
56	< 1% match (lucrările studenților la data de 20-mar.-2014) Submitted to University of Durham on 2014-03-20
57	< 1% match (Internet de la data de 21-sept.-2015) http://www.ca.com/ae/en/news/press-releases/na/2014/using-big-data-and-analytics-to-combat-fraud-loss.aspx
58	< 1% match (Internet de la data de 13-apr.-2016) http://www.ijcaonline.org/archives/volume111/number5/19533-1181
59	< 1% match (lucrările studenților la data de 21-sept.-2014) Submitted to Southern New Hampshire University - Distance Education on 2014-09-21

60 < 1% match (lucrările studenților la data de 31-aug.-2013)
Submitted to Higher Education Commission Pakistan on 2013-08-31

61 < 1% match (Internet de la data de 19-apr.-2015)
http://www.business-and-management.org/issue.php?volume=4&issue=3

62 < 1% match (Internet de la data de 18-iul.-2012)
http://www.ey.com/Publication/vwLUAssets/Proactive_fraud_monitoring_for_banks_in_India/$FILE/Proactive_fraud_monitoring.pdf

63 < 1% match (lucrările studenților la data de 20-mai-2016)
Submitted to Strayer University on 2016-05-20

64 < 1% match (Internet de la data de 12-oct.-2010)
http://www.shuchita.com/pdf/Appendix/CS%20Excutive%20Programme%20Module%20II%20(New%20Course)%20Appendix%20Final%

65 < 1% match (publicații)
Bhasin, Madan Lal, and Junaid M. Shaikh. "Voluntary corporate governance disclosures in the annual reports: an empirical study", International Journal of Managerial and Financial Accounting, 2013.

66 < 1% match (lucrările studenților la data de 21-sept.-2014)
Submitted to Bridgepoint Education on 2014-09-21

67 < 1% match (Internet de la data de 29-oct.-2014)
http://www.isca.in/IJMS/Archive/v2/i7/4.ISCA-RJMS-2013-062.pdf

68 < 1% match (Internet de la data de 28-apr.-2012)
http://www.tlainc.com/articlsi12.htm

69 < 1% match (Internet de la data de 04-aug.-2015)
http://ethisphere.com/ac-categories/data-trends/

70 < 1% match (Internet de la data de 29-apr.-2014)
http://www.dataconsulting.co.uk/Files/DP_Fraud_detection_BANKING.pdf

71 < 1% match (Internet de la data de 29-nov.-2015)
http://www.ijmsbr.com/Volume%203,%20Issue%202%20Paper%209.pdf

72 < 1% match (Internet de la data de 29-iun.-2013)
http://webcache.googleusercontent.com/search?q=cache:FJOQ4kjlu88J:www.nysscpa.org/c

73 < 1% match (Internet de la data de 09-mai-2015)
http://www.irmbrjournal.com/papers/1405506805.pdf

74 < 1% match (Internet de la data de 21-sept.-2015)
http://businessperspectives.org/journals_free/bbs/2015/BBS_en_2015_02_Dzomira.pdf

75 < 1% match (Internet de la data de 01-nov.-2012)
http://www.onlinesbs.in/2012/01/mumbai-is-number-one-for-banking-fraud-in-india.html

76 < 1% match (publicații)
"Deloitte says bank frauds in India have increased.", Global Banking News (GBN), April 23 2015 Issue

77 < 1% match (lucrările studenților la data de 13-apr.-2016)
Submitted to Queen Mary and Westfield College on 2016-04-13

78 < 1% match (Internet de la data de 18-ian.-2014)
http://www.arabianjbmr.com/pdfs/AC_VOL_1_1/1.pdf

79 < 1% match (Internet de la data de 01-mai-2010)
http://www.icai.org/resource_file/9935588-594.pdf

80 < 1% match (Internet de la data de 26-mai-2012)
http://www.ajbmr.com/articlepdf/ajbmr_v01n01_02.pdf

81 < 1% match (Internet de la data de 03-nov.-2015)
http://papers.ssrn.com/sol3/JELJOUR_Results.cfm?form_name=journalBrowse&journal_id=1346520

82 < 1% match (publicații)
Madan Bhasin. "Disclosure of intellectual capital in the annual reports by the IT companies: an exploratory study of India", International Journal of Managerial and Financial Accounting, 2011

83 < 1% match (Internet de la data de 03-mai-2011)
http://www.mendeley.com/research/crimes-analysis-software-pins-in-maps-clustering-and-bayes-net-prediction/

84 < 1% match (Internet de la data de 24-dec.-2015)
http://www.hindustantimes.com/india/rbi-chief-wants-pmo-to-act-against-bank-frauds-worth-rs-17-500-crore/story-aSc2tkwhac4I2HDTfnq4HP.html

85 < 1% match (lucrările studenților la data de 31-mar.-2013)
Submitted to University of Bradford on 2013-03-31

86 < 1% match (lucrările studenților la data de 10-nov.-2015)
Submitted to Universiti Tenaga Nasional on 2015-11-10

87 < 1% match (lucrările studenților la data de 10-sept.-2015)
Submitted to Kenyatta University on 2015-09-10

88 < 1% match (lucrările studenților la data de 18-ian.-2016)
Submitted to Federation University on 2016-01-18

89 < 1% match (Internet de la data de 16-mar.-2015)
http://iosrjournals.org/iosr-jbm/papers/Vol16-issue3/Version-3/A16330107.pdf

90 < 1% match (Internet de la data de 30-apr.-2016)
http://maaw.info/BibliographyK-3.htm

91 < 1% match (publicații)
Mhamane, Sunil S, and L.M.R.J Lobo. "Internet banking fraud detection using HMM", 2012 Third International Conference on Computing Communication and Networking Technologies (ICCCNT 12), 2012.

92 < 1% match (lucrările studenților la data de 30-mar.-2015)
Submitted to Mid-America Christian University on 2015-03-30

93 < 1% match (lucrările studenților la data de 09-mar.-2015)
Submitted to Segi University College on 2015-03-09

94 < 1% match (lucrările studenților la data de 08-mai-2015)
Submitted to University of Southampton on 2015-05-08

95 < 1% match (Internet de la data de 31-mar.-2015)
http://icmrr.org/November_2013/IJFRR/11132008.pdf

96 < 1% match (Internet de la data de 19-sept.-2012)
http://www.bus.lsu.edu/accounting/faculty/lcrumbley/jfia/Articles/FullText/2010v2n2a2.pdf

97 < 1% match (Internet de la data de 06-apr.-2014)
http://www.hindustantimes.com/Search/search.aspx?q=psu%20banks

98 < 1% match (Internet de la data de 31-mar.-2010)
http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=694806

99 < 1% match (Internet de la data de 31-mar.-2014)
http://www.rabizservs.co.uk/downloads/RA_World_Class_Internal_Audit.pdf

100 < 1% match (Internet de la data de 31-mar.-2010)
http://www.nabard.org/FileUpload/DataBank/Newsletters/Newsletter%20%20November%202009%20web.pdf

101 < 1% match (Internet de la data de 18-apr.-2016)
http://indianjournals.com/ijor.aspx?article=001&issue=3&target=ijor%3Asjdm&volume=7

102 < 1% match (Internet de la data de 19-apr.-2013)
http://www.mydigitalfc.com/economy/economy-may-have-lost-rs-6600-cr-due-frauds-fy12-ey-117

103 < 1% match (Internet de la data de 08-iul.-2015)
http://ijbssnet.com/journals/Vol_5_No_6_1_May_2014/10.pdf

104 < 1% match (Internet de la data de 14-iul.-2006)
http://mba.iiita.ac.in/augsept05/brainwave_1.htm

105 < 1% match (Internet de la data de 16-ian.-2013)
http://www.escortsmutual.com/newsupdate%2017th%20september.html

106 < 1% match (Internet de la data de 20-ian.-2016)
http://savingwala.com/banks/frauds-in-banking.html

107 < 1% match (Internet de la data de 13-apr.-2016)
http://cmrindia.com/f5-bfsi-chat-room/

108 < 1% match (Internet de la data de 31-iul.-2013)
http://fareastjournals.com/files/FEJPBV9N2P2.pdf

109 < 1% match (publicații)
Bhasin, Madan Lal, and Junaid M. Shaikh. "Corporate governance through an audit committee: an empirical study", International Journal of Managerial and Financial Accounting, 2012.

textul lucrării:

THE ROLE OF TECHNOLOGY IN COMBATTING BANK FRAUDS: PERSPECTIVES AND PROSPECTS

14**Abstract Banks are the engines that drive the operations in the financial sector,** money markets **and growth of an economy. With the** rapidly **growing banking industry in India, frauds in banks are also increasing** very fast, **and fraudsters**

have started using innovative methods.

14**As part of the study, a questionnaire-based survey was conducted in** 2013-14 **among 345 bank employees to know their perception towards bank frauds and evaluate the factors that influence the degree of their compliance level. This study**

21**provides a frank discussion of the attitudes, strategies and technology that specialists will need to combat**

frauds in banks. In the modern era, there is “no silver bullet for fraud protection; the double-edged sword of technology is getting sharper, day-in-day- out.” The

57**use of neural network-based behavior models in real-time has changed the face of fraud management all over the world. Banks**

12**that can leverage advances in technology and analytics to improve fraud prevention will reduce their fraud losses.**

78**Recently, forensic accounting has come into limelight due to rapid increase in financial frauds** or **white-collar crimes.**

Key words: Combatting frauds;

> 14**Banking industry; RBI; risk management; use of technology;**

current scenario, future challenges. JEL Classification: M41 I. INTRODUCTION It is universally accepted that for the smooth functioning of a money market and economic growth of a country, an efficient and good banking system is a must.

> 33**Banking industry in India has traversed a long-way to assume its present stature**

in the 21st century. According to Singh (2005), “The

> 33**Indian banking** industry **is unique and has no parallels in the banking history of any country in the world.** After independence, **the**

banking sector has passed through three stages:

> 33**character-based lending to ideology-based lending to competitiveness-based lending.”**

Similarly, Kumar and Sriganga (2014) stated, “Banking sector of India accommodates 1175,149 employees, with

> 16**total of 109,811 branches in India (and 171 branches abroad), and manages an aggregate deposit of** Rs. **67,504.54 billion**

> 16**and bank credit of** Rs. **52,604.59 billion.”**

Indeed, PSBs

> 11**have a 75% market share, but the number of** funds **by private banks is** 5 **times of PSBs. The**

> 41**phenomenal spread of branches, growth and diversification in business, large-scale computerization and networking, have collectively increased manifold the operational risks faced by** the **banks.**

Unfortunately, it is also true banking industry has to face many types of frauds and scams.

> 105**The Reserve Bank of India (RBI)** is **the** central policy making **and**

national-level regulatory body by keeping an eye over the entire banking industry.

> 9**Regulations and laws governing the financial services sector in India are continuously evolving.**

AS Bhasin (2011) sums up, “Some of the important regulatory drivers for the financial sector in India are as follows: (a)

> 64**Reserve Bank of India Act, 1934; (b) Securities and Exchange Board of India Act, 1992; (c) Companies Act,** 2013; **(d)** Prevention **of**

> 77**Money Laundering Act, 2002;** and (e) **The Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015.”**

The PwC’s Survey

9identified that suspicious transaction reporting, effective fraud risk management measures, whistleblowing processes and tip-offs helped financial services organizations to detect most frauds.

II. MEANING AND TYPES OF BANK FRAUDS

92Fraud is a worldwide phenomenon that affects all continents and all sectors of the economy.

23As per RBI, fraud can be "loosely" described as "any behavior by which one person intends to gain a dishonest advantage over another."

5Fraud encompasses a wide-range of illicit practices and illegal acts involving intentional deception or misrepresentation. The Institute of Internal Auditors' "International Professional Practices Framework (IPPF)" (2009) defines fraud as: "Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage." In

this context, Bhasin (2011a) remarked,

5"Fraud impacts organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. In fact, the losses to reputation, goodwill, and customer relations can be devastating." As fraud can be perpetrated by any employee within an organization or by those from the outside, therefore, it is important to have an effective fraud management program in place to safeguard your organization's assets and reputation.

3Banks can secure and preserve the safety, integrity and authenticity of the transactions by employing multipoint scrutiny: cryptographic check hurdles. In addition, banks should rotate the services of the persons working on sensitive seats, keep strict vigil of the working, update the technologies employed periodically, and engage more than one person in large-value transactions.

Of course,

47internal auditors can continue to win the battle against frauds and scams through the continued application of fundamentals, such as education, technological proficiency, and support of good management practices.

17Close attention and vigilance on the part of both banks and customers is, therefore, the best deterrence.

According to Freddie Mac (2015), "Fraud Mitigation Best Practices" include: (a) Fraud Risk Management Policies and Procedures, (b) Regulatory Compliance, (c) Ethical Conduct, (d) New Employee Awareness, and (e) Training. One of the most challenging aspects in the Indian banking sector is to make banking transactions free from electronic crime (Pasricha and Mehrotra, 2014).

5Fraud detection in banking is a critical activity that can span a series of fraud schemes and fraudulent activity from bank employees and customers alike.

It may be noted at the outset that

26**all the major operational areas in banking** industry offers **a good opportunity for fraudsters, with growing**

fraud and financial malpractices

26**being reported under deposit, loan, and inter-branch accounting transactions (including remittances).** As Bhasin **(2012),**

observed, “Frauds generally

26**take place in a financial system when safeguards and procedural** controls **are inadequate, or when they are not scrupulously adhered to,** thus, **leaving the system vulnerable to the perpetrators.”**

Most of the time,

28**it is difficult to detect** frauds well **-in- time, and even more difficult to book the offenders because of intricate and lengthy legal requirements and processes. In the fear of damaging the banks reputation,**

these kinds of incidence are often not brought to light. Historical

38**evidence shows that whether the agency (or individual) committing the fraud works for the bank or deals with it, the culprit** usually **does** very **careful** and detailed **planning before he** finally **attacks the system at its most vulnerable point.**

Table 1 shows some of the

107**common types of frauds in the** Indian **banking sector.**

In

9**today’s volatile economic environment, the opportunity and incentive to commit frauds have both increased. Instances of asset misappropriation, money laundering, cybercrime and accounting fraud are only increasing by the day. With changes in technology, frauds have taken the shape and modalities of** organized **crime, deploying increasingly sophisticated methods of perpetration. As financial transactions become increasingly technology-driven, they seem to have become the weapon of choice when it comes to fraudsters.**

Table 1: Ty pes of Frauds Commonly Prevalent in the Indian Banking Industry Bribery and corruption Cybercrime Multiple funding Counterfeit cheques Terrorist Financing Data Security Identity theft Tunneling Money Laundering Loan loss Internet banking frauds Absence of collaterals Tax Evasion Fraudulent documentation Incorrect sanctioning Mobile Banking Risks

9**According to the PwC Global Economic Crime Survey 2014, “cybercrime was one of the top economic crimes reported by** organizations **across the world, including India.”**

According to Accenture (2015), “”The key trend being seen across the banking industry is integration and optimization of fraud management tools and capabilities” including the followings: ? Integration of

12**IT security and fraud management** capabilities **to address the increasingly technical nature of fraud attacks,**

as well as the impact of innovations in the banking sector, such as mobile applications and payments. ? Greater

> 54**use of social network analysis and cyber data mining to identify the propensities of both new and existing customers to participate in fraudulent activities.**

? Updates to international payment fraud controls. ? Consolidation of legacy systems, including cross-financial crime prevention toolkits. ? Strengthening of Fraud Control Framework for outsourcing contracts and off-shored services. ? Increased industry coordination and improved fraud reporting. ? Development of pan-channel solutions for customer on-boarding and ongoing ID&V. ? Desire to move to global solutions to deal with fraud and anti-money laundering problems, to reduce the cost of financial crime prevention. There is

> 4**no simple way to squash fraud, but by implementing the right mix of technologies and prevention techniques, treasury executives can greatly reduce their organization's risk. As Accenture's Santoro puts it, "A solid portfolio of solutions with multiple layers of protection and controls can go a long way toward providing the necessary protection. If you put enough deadbolts at the door, thieves are going to give up and look elsewhere."** According **to**

Accenture (2015),

> 12**"changing customer demographics, the expansion of banks into new markets, and the adoption of new technologies and channels present new challenges in fraud protection. Rapid technological and social changes alter the relationship between banks and their customers in a way that creates new opportunities for fraudsters."**

> 6**It is an endless game of "cat and mouse" between banks and** cyber-criminals. **There is a virtual arms race taking place online between financial institutions and** cyber criminals, **who as soon as the bank deploys a new process or technology to prevent online fraud, they find a weakness to exploit (ACI, 2013;**

Dzomira, 2014).

> 12**In addition, customers expect to be protected from fraud, but also want anti-fraud tools to look at them holistically, assessing the fraud risk of transactions based on their individual profiles.**

Five ways to combat bank frauds are highlighted below as:

> 4**1. Adopt appropriate technologies: An inclusive mix of strong authentication systems; analytics software; and bank services, positive pay and payee verification, for example, can greatly reduce an organization's exposure to fraud. It** is **important to have layers of protection.**

> 4**2. Beef up your internal controls: Sarbanes-Oxley mandates that companies pay strict attention to their internal controls. But even the most thorough Sarbanes-Oxley compliance effort** cannot **provide comprehensive protection against fraud. Proactive organizations will want to put additional controls in place, including rigorous approval procedures and careful separation of duties. That** is **especially true of disbursement processes, such as wire transfers. 3. Screen job applicants carefully: One of the biggest security problems** company's **face is fraud perpetrated by trusted insiders. Key finance functions such as treasury must conduct background checks on potential hires, and companies should also consider drug testing and honesty testing. It** is **the first line of defense.**

4**4. Educate your workforce: Employees need to understand how damaging fraud can be to the organization. They must be able to recognize signs of fraudulent activity and know how to report it. In addition, treasury employees will need to be trained in the correct use of the company's fraud-protection tools and technologies. 5. Prosecute thieves: Many organizations fire employees who are caught stealing but avoid prosecuting them for fear of bad publicity. A zero-tolerance policy goes a long way toward reducing the risk of illegal activity. Likewise, managers should immediately turn over any evidence of suspected fraud to law enforcement agencies.**

III. MAGNITUDE OF FRAUDS IN BANKS: THE INDIAN BANKING INDUSTRY SCENARIO According to Ernst & Young Report

52**(E&Y** 2012), **"Different types of frauds caused Rs. 6,600 crore loss to** the **Indian economy in**

2011-12,

102**and banks were the most common** victims **in swindling cases;**

52**insider enabled fraud accounted for 61% of fraud cases."**

However, Soni and Soni (2013) concluded that

67**"cyber fraud in the banking** industry **has emerged as a big problem and a cause of worry for this sector."**

Similarly, another survey conducted by Deloitte

42**(2012) shows that "banks have witnessed a rise in the number of fraud incidents in the last one year, and the trend is likely to continue in the near future." The**

106**Deloitte India Banking Fraud Survey Report Edition II**

(2015) added

76**"number of frauds in banking sector have increased by more than 10% over the last two years.** Banks witnessed rise **in**

50**level of sophistication with which frauds were executed."**

It is universally accepted that continued prevalence of frauds will have long-term bad consequences for banks, customers, investors, government and the economy in general. The year-wise details, beginning from 2000-01 to 2013-14, regarding the number and amount

22**of frauds reported by the** Indian **banking sector** to **the** RBI, are shown **in**

Table 2. As Pai and Venkatesh (2014) reported,

23**"As on March 31,** 2014 **banks reported total** loss **of Rs.** 169,190 **crore from 29,910 cases. In 2012-13, Rs. 13,293 crore of fraud was detected**

from 8646 cases." During Apr.-Dec. 2014, PSBs suffered losses of Rs. 11,022 crore from 2100 fraud cases involving Rs. one lakh or more. During same period,

23**46% more amount was lost due to frauds compared to last full-year.**

11**With the advent of mobile and internet banking, the number of banking frauds in the country is on the rise as banks are losing money to the tune of approximately** Rs. 2,500 **crore every year. While the figure for 2010-11 was** Rs. 3,500 **crore, for the current financial year (till September) it is about** Rs. 1,800 **crore. Further, state-wise list of information on banking frauds shows Maharashtra** (Mumbai) **reporting the highest number of cases to the RBI. In the last financial year, banks in the Maharashtra reported 1,179 cases with** Rs. 1,141 **crore being lost to such frauds. Maharashtra is followed by Uttar Pradesh with 385 cases during the same period.**

The

75**RBI requires banks to pursue fraud cases vigorously with the CBI or police authorities, and in court. The**

89**central bank has taken several steps to sensitize banks and curb frauds in the banking**

industry. The

62**evolving fraud landscape around banking and the increase in fraud-related losses requires automated detection systems and robust fraud defense processes**

(E&Y, 2010). Table 2: Number of Frauds and Amount Involved in Indian Banks Year ending 31st March Amount Involved (Rs. in Crore) Number of Fraud Cases Reported to RBI 2000-01 538.56 1,858 2001-02 470.37 1,353 2002-03 374.97 1,643 2003-04 823.61 2,193 2004-05 451.04 2,520 2005-06 1134.39 2,658 2006-07 844.76 2,568 2007-08 396.86 1,385 2008-09 1911.68 23,941 2009-10 2037.81 24,791 2010-11 3832.08 19,827 2011-12 4491.54 14,735 2012-13 8646.00 13,293 2013-14 169190.00 29,910

108**(Source: Compiled by the author from** various published bank **reports)** IV. REVIEW **OF**

LITERATURE

10**Jeffords (1992) examined 910 cases submitted to the "Internal Auditor" during the nine-year period from 1981-** 1989 **to assess the specific risk factors cited in the Treadway Commission Report. Approximately 63 percent of the 910 cases are classified under the internal control risks.** Similarly, **Calderon and Green (1994) made an analysis of 114 actual cases of corporate fraud published in the "Internal Auditor"** from **1986 to 1990. They found that limited separation of duties, false documentation, and inadequate or** nonexistent **control** account **for 60** percent **of the fraud cases. Moreover, the study found that professional and managerial employees were involved in 45** percent **of the cases.**

1**Ziegenfuss (1996) performed a study to determine the amount and type of fraud occurring in state and local government.**

1**Willson (2006) examined the causes that led to the breakdown of 'Barring' Bank, in his case study, "the collapse of Barring Banks". The collapse resulted due to the failures in management, financial and operational controls of Baring Banks.**

However, Bhasin (2007)

> 10examined the reasons for check frauds, the magnitude of frauds in Indian banks, and the manner in which the expertise of internal auditors can be integrated in order to detect and prevent frauds in banks. In addition to considering the common types of fraud signals, auditors can take several 'proactive' steps to combat frauds.

> 1One important challenge for banks, therefore, is the examination of new technology applications for control and security issues.

In another study, Bhasin (2012) examined in- depth the corporate accounting fraud perpetuated by the Satyam management team in collusion with the auditor. As per the survey conducted by Ganesh and Raghurama (2008),

> 1about 80 executive from Corporation Bank and Karnataka Bank Ltd of India, were requested to rate their subordinates in terms of development of their skills before and after they underwent certain commonly delivered training programs. Responses revealed that for the 17 skills identified, there was improvement in the skills statistically. The paired t-test was applied individually for the seventeen skills, and all these skills have shown statistical significance.

Moreover, another

> 61study to investigate the reasons for bank frauds and implementation of preventive security controls in Indian banking industry was performed by Khanna and Arora

(2009). The study "seeks to evaluate the

> 71various causes that are responsible for bank frauds. The result indicate that lack of training, overburdened staff, competition, low compliance level are the

main reasons for bank frauds." Mhamane and Lobo (2012) in their study attempted

> 91to detect and prevent fraud in case of internet banking using Hidden Markov Model algorithm.

Chiezy and Onu (2013)

> 15evaluated the impact of fraud and fraudulent practices on the performance of 24 banks in Nigeria during 2001-2011.

> 15Secondary sources of data were used for the study. The relationship between fraud cases and other variables were estimated using Pearson product moment correlation and multiple regression analysis was used. The

> 15paper recommended that banks in Nigeria need to strengthen their internal control systems and the regulatory bodies should improve their supervisory role.

However, Dzomira (2014) investigated the use of

> 6digital analytical tools and technologies in electronic fraud and detection used in the Zimbabwe banking industry.

He

6concluded that banking institutions should reshape their anti-fraud strategies to be effective by considering frauds detection efforts using advanced analytics and related tools, software and application to get more efficient oversight.

Similarly, Kumar and Sriganga (2014) highlighted the

16common insider frauds occurring in banks and also tried to categorize them into different types.

They focused

16on different generic data mining techniques and in specific, the techniques used for detecting insider frauds.

The

80foregoing discussion suggests that the literature on the

bank frauds

82in Indian-context is very limited and inconclusive. Thus, our study builds on the previous literature of

bank frauds in the Indian banking sector. The

80scope of the study has been confined to 21 banks in the

National Capital Region (NCR) of India. V. MATERIALS AND METHODS The present study is both descriptive and analytical in nature.

14As part of the study, in 2013-14 a questionnaire-based survey was conducted among 345 bank employees

of the National Capital Region (NCR) area. The questionnaire was structured into two parts. In fact, the first part comprised of several questions that attempted to know their opinions while working in a bank regarding training received,

1attitude towards the procedures prescribed by RBI, awareness level towards frauds and their compliance level under the following six heads: deposit account, loans and advances, administration of passbook and check book, drafts section, internal and inter-branch accounts, and credit-card section. Moreover, the

second part encompassed the issues about how to integrate technology in the banking industry

98in order to detect and prevent frauds in Indian banks. It also examined the

technology solutions available and how to integrate forensic approach to combat bank frauds in the Indian banking industry. All the respondents were selected through the random sampling method. There were 42 public sector banks in the area and finally, 21 banks were selected. The sampled employees comprising of Managers, Officers and Clerks of the branches were

1given the questionnaire by personally visiting them in bank. Out of all the employees,

296 employees responded, with an overall response rate of 85%. In all, there were 57 managers, 130 officers and 109 clerks as respondents and grouped

1on the basis of the following parameters (see Table

3). Table 3: Classification

1of Respondents into Categories based on Parameters Parameter Category/Group Compliance score of bank employee High Medium Low Attitude of bank employee towards procedures prescribed by RBI Favorable Moderate Unfavorable Training status Trained Untrained Awareness level of bank employees High Medium Low Hierarchical level Managers Officers Clerks VI. RESULTS AND

DISCUSSION The RBI, being the overall central regulatory agency,

1has developed many important guidelines for prevention of bank frauds,

which can help banks to prevent frauds. In the first part of the questionnaire, we focused on the compliance level of

46these security controls were measured under the following six heads— internal checks, deposit accounts, administration of check books and passbooks, loans and advances, drafts, internal accounts and inter branch accounts. The results of

this study

1indicate that the security control measures are not fully complied with.

As per a study,

1limited separation of duties, false documentation, and inadequate or nonexistent control account for 60% of the fraud cases. It found that professional and managerial employees were involved in 45% of the cases.

Thus,

85education, training and awareness programs are informal intervention measures that should be implemented to prevent frauds.

Undoubtedly,

1security controls prescribed by RBI, if followed with 100% adherence, can prevent frauds

to a maximum extent. Table 4:

1Average Compliance Scores of Various Heads of Bank Managers Section Internal checks Loans advances & Deposit account Admin. in check, pass book Draft section Internal & inter- branch account Compliance score 95% 91% 82% 65% 84% 83% Table 4 depicts the average compliance

score of Bank Managers under the various heads. The

1results show that Bank Managers compliance level is the lowest (65%) in administration of

check/pass book. In sharp contrast, the highest (95%) compliance is noticed in internal checks. The Managers gave

1second highest (91%) importance to loans and advances, and gave almost

equal importance to

the draft section (84%), internal and inter-branch account (83%), and deposit account (82%), respectively. But surprisingly, still there is lack of 100% compliance related to security controls under any of the above listed six bank heads. Thus, it is amply clear that till now, banks in India are not able to follow "zero-tolerance" policy. Table 5: Average Compliance Scores of Various Heads of Bank Off icers Section

1**Loans and advances Deposit account** Admin. **in** check, pass **book Draft section Internal**& branch account **inter- Compliance score**

65% 75% 60% 81% 86% Table 5 provides a snapshot of average compliance scores of Bank Officers under the various heads. The

1**compliance level of Officers is** the **"highest" in internal & inter-branch account** (86%), **followed by** draft section (81%) **and deposit account**

(75%). Surprisingly, Bank Officers gave the lowest scores to the following two areas viz., loans and advances (65%), and administration in check and pass book (60%) sections. Keeping in view the Bank Managers and Officers scores, we can draw a broad conclusion: nobody likes to perform the work especially in the administration of check and pass book section." Thus, there appears to be considerable differences

1**in compliance level of employees of various banks,**

most probably, on account of differences in the organizational culture, training provided, past experiences and their mental attitudes to strictly follow the RBI procedures. We feel that if the detailed

1**procedures and/** or **instructions** as **prescribed by** the **RBI, if fully complied with**

(both in letter and spirit), no doubt, it

1**can greatly reduce the incidences of frauds. But the** present **study revealed "very low** percentage **of respondents** display **highly-** favorable **attitude towards the procedures laid-down by RBI."** As **Table**

6 shows, a "very high proportion of respondent (98+113=211/296)

1**believe that they do not have sufficient staff to carry out the work meticulously,**

they are usually overburdened with work and hence,

1**not able to follow** the **procedures strictly. Since** this **attitude is based on the perception of bank employees towards adequacy of staff, it can be inferred that "if there is** an **adequate** number of bank **staff** hopefully **the compliance** level **will be more." Table** 6: **Frequency Distribution of the Responses of** the **Bank Employees on the basis of their Attitude** tow ards the **RBI Procedures Attitude towards RBI** procedures Favorable **Moderate** Unfavorable **Total Total number of employees**

85 98 113 296 From Table 7, we can conclude that "the

29**compliance level of the managers** (48%) **is higher than that of officers** (22%). **This** may **be due to the fact that managers are more** rigorously **trained and their attitude towards RBI's procedures is more** favorable **than that of officers and clerks.** Hence, Mangers **awareness level is high** as **they have increased level of responsibility.**

1**Table** 7: **Distribution of Managers and Officers according to their** Compliance **Level**

Position High Medium Low Manager 48 42 10 Officer 22 53 25 It is amply clear from Table 8 the

1**awareness level is very low,** both on **the** part of **Clerks and Officers**

in Banks. For example, only 9.17% of clerks and 13.07% of

1**officers belong to "high" category of awareness level.** However, **Managers** show **a little better**

awareness level. For example,

1**around 15.** 78% **of Managers belong to high category of awareness level.**

A careful study of the data contained in the table reveals shockingly that about 52% of

1**Clerks, 49% of Officers, and 47% of Managers belong to "low" category of awareness level.**

1**It is** very **disappointing to know that** the **awareness level of** Bank **employees about various types of frauds**

and losses suffered by the banks are very low. Hence, with this dismal scenario, how can we expect from them to follow detailed procedures and guidelines issued by the RBI and take pro-active actions to prevent frauds and mitigate bank losses? Table 8: Frequency Distribution of the Responses

1**on the basis of Awareness** Levels **Awareness** Category **High Medium Low Total Position Frequency % Frequency % Frequency % Managers** 9 **15.** 78 21 **36.** 84 27 **47.** 36 57 **Officers**

17 13.07 49 37.69 64 49.30 130 Clerks 10 9.17 42 38.53 57 52.29 109 Table 9 depicts the relative importance (on 10 point score) assigned by the Bank

1**Managers, Officers and Clerks to the reasons responsible for** the commitment of **bank frauds. Managers gave more weight-age to lack of training** (7), and **followed by overburdened staff**

(5). In sharp contrast to this, both Officers (6) and Clerks (7)

1**felt that overburdened staff is the main reason responsible for bank frauds,** which is **followed by lack of training**

for Officers (5) and Clerks (6), respectively. Table 9: Responses about the Key Reasons for Perpetration of Frauds in Banks

1**Position Lack of training Corrupt officer in-charge Overburdened staff Competition Managers**

7 3 5 4 Officers 5 5 6 5 Clerks 6 4 7 4 When we asked the bank employees and managers,

6**80% indicated that fraud detection tools and technologies** are **the most effective** ways **of**

combatting bank frauds. On the other hand,

643% of the respondents showed that real-time decision making tools are effective in preventing fraud,

while 22% respondents

6showed that monitoring of accounts is effective, whilst 77% indicated that customer awareness is most effective of preventing fraud, and finally, 76% of the respondents revealed that training of employee putting emphasis on identification and response to fraudulent activities is the most effective way of preventing fraud in organisations.

The response given by Bank Employees and Bank Managers are shown in Table 10. Table 10: Responses about Detection and Prevention of Frauds in Banks Monitoring accounts manually Training Employees of Customer Education Real-time decision- tools techniques Fraud detection 22% 76% 77% 43% 80% Based on how fraud incident is typically detected in bank, a large majority of 21% respondents gave the reason of complaint by a customer. However, the second important reasons given by 18% of respondents were internal whistle-blower and during audit of accounts or reconciliation process. Over 16% of respondents gave the reason “through automated data analysis or transaction monitoring software.” Moreover, other important reasons given by the respondents were: at the point of transaction (10%), through a third-party notification (7%), by accident (6%) and review by a law enforcement agency (4%), respectively. To conclude, as shown in Table 11, survey respondents indicated that frauds in their organizations were most commonly detected through customer complaints, followed by an internal or external tip, which is in line with global trends. Table 11: Response about How Fraud incident is Ty pically Detected in Banks Review by law enforcement agency By accident Through a third party notificatio n At the point of transaction Through automated data analysis or software During audit or reconciliat ion Internal whistle- blower By customer complaint 4 6 7 10 16 18 18 21 Banks response to fraud is critical 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. According to a 2009 Circular issued by RBI states, “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

100external legal prosecution of the fraudsters and their abettors,

if required.” In line with RBI’s recommendations, the

2majority 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 (see Table 12). The reasons given by respondents were: internal investigation is done (46%), incident reported to legal agency (32%), and forced to resign (14%). It is interesting to note that only 8% of survey respondents indicated using an independent consultant to carry out investigations. Survey respondents indicated that the top three challenges faced by banks in preventing fraud were: lack of customer awareness (23%); integration of data from various sources (20%); and inadequate fraud detection tools (18%). According to Bhasin (2016), “It is important to understand that fraud investigation requires specific skill sets like ‘forensic accounting and technology’ to collect adequate evidence, which can be admissible in a court of law.” In the absence of these, banks may not have the confidence to take legal resource 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. While the responses received in our survey indicate that banks have set up a dedicated fraud investigative cell, it appears to be hampered by the lack of dedicated technology tools for investigation. A little over 40% of survey respondents indicated they had not started implementing dedicated forensic technology tools for investigation, whereas, 20% of respondents had partially implemented these tools. Only 20% indicated that they had implemented forensic technology tools for investigation, and that these tools were effective. Table 12: Response about the Process Followed to Handle Fraud Incidents in Banks An internal investigation is carried out Incident is reported to law enforcement agency Individual in question is asked to resign External investigation by an independent consultant 46% 32% 14% 8% The second part of the questionnaire focussed very specifically about the use of technology in banks. Accordingly, we asked the Bank Employees and Bank Managers regarding the most effective methodologies used by them in banks to detect and prevent frauds. The response given by Bank Employees and Bank Managers are shown in Table 13. An overwhelming majority of 85% of the

6respondents indicated that they are planning to use in their bank intrusion

prevention technologies. However, 78% of the respondents expressed the opinion

6that fraud management system be planned for use. However, 68% of the respondents revealed that they intend to use strong encryption techniques in

future, and **70%**

6**indicated that they plan to apply neural net fraud detection technologies.**

As against this, 62% of the respondents plan to use strong

6**authentication, as on-going fraud prevention and detection program in future.**

Table 13: Response about Technologies Used by Banks to Detect and Prevent Frauds Fraud management system Strong authentication system Intrusion Prevention technologies Encryption System detection systems Neural fraud 78% 62% 85% 68% 70% According to the responses received, 53% of the respondents appear to have implemented a dedicated fraud detection/analytics solution. However, only one in every three respondents appears to be entirely satisfied with it. The following responses were given by the respondents, in order of response: ability to highlight red- flags where controls are being circumvented (29%), ability to identify where enhanced controls are needed (27%), provide enhanced tracking of high-risk customers (19%), provide case management abilities (13%) and provide audit trails (12%), respectively (see Table 14). Thus, it was interesting to note that 56% of respondents sought technology to help them either highlight red-flag areas (29%), where controls have been circumvented, or where controls needed to be enhanced (27%). We feel 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 this sector." Here, Bhasin (2012, 2015) stated, "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, which could

109**go a long way in enhancing the** efficiency **of**

detecting frauds in time." Table 14: Response about Most Important Areas Crucial to Anomaly Detection Solution Highlight Red flag areas Areas controls needed Tracking high- risk customers Case management Audit Trails 29% 27% 19% 13% 12% Moreover, Bhasin (2007) pointed out that "since banks are

69**increasingly depending on technology, it** is **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." Table 15 shows that ATM frauds ranked first with 23%, phishing and vishing attacks with 16%, mortgage with 114%, credit cards with 10%. Others (37%), includes options such as third-party POS skimming, account takeover fraud, IP theft, money laundering etc. Additionally, when asked to select the top three areas which were giving sleepless nights to bankers, it was no wonder that

50**internet banking/ATM fraud, E-Banking and identity fraud** were **the**

top culprits. Interestingly, mortgage portfolio also appears to be increasingly vulnerable to the risk of fraud. Table 15: Response about New Fraud Trends that will be of Concern in the Next Two Years ATM Phishing/vishing Mortgage Credit card Others 23% 16% 14% 10% 37% However, Bhasin (2015a) commented,

24**"As we know, the great financial scandals were based on accounting manipulation practices, but also on collaborations with** the **audit firms, which instead of acting as the 'guardians' of the financial markets have come to overlook, to hide, and even to participate to some of the greatest frauds in** the **history." Thus, reform measures for the companies'** Corporate **Governance systems were** also **imposed.**

According to a study conducted by Bhasin (2015b),

36**"It was equally revealed that one of the best ways to prevent the practice of Creative Accounting is to enforce both preventive, as well as, strong enough punitive measures on those that engage in** creative accounting **practice."**

Also,

96**we asked the respondents some questions about "the demand for forensic**

chartered **accountants**

(FCAs)

2**in the future—next five, ten and twenty years." As can be seen from Table** 16, **the majority of respondents felt that the demand for** FCAs **will increase well into the foreseeable future. In fact, ninety-four percent felt that the demand for** FCAs **would increase in the next 10 years. Respondents were also asked "if they felt that there will be enough** FCAs **available to meet the demand in the next five, or ten years, and beyond the next 10 years." As can be seen in Table** 17, **many participants were unsure if the supply of** FCAs **would be enough to meet the demand in the future.**

Table 16: Demand for the Forensic Chartered Account ants in the Future

2**Question Mean Standard Deviation The demand for forensic accountants in the next 5 years will: 4.46 (0.646) The demand for forensic accountants in the next 10 years will: 4.34 (0.651) The demand for forensic accountants in the next 20 years will: 4.20 (0.728) Table** 17: **Availability of Forensic** Chartered **Accountants** in the Future **Question** In **Percent (%) Will there be enough forensic accountants available to meet the demand in the next 5 years: Yes 13 No** 62 **Not Sure 25**

2**Will there be enough forensic accountants available to meet the demand in the next 10 years: Yes** 25 **No** 29 **Not Sure** 46 **Will there be enough forensic accountants available to meet the demand beyond the next 10 years: Yes** 32 **No** 16 **Not Sure**

52 Recently,

79**the banking industry around the world has undergone a tremendous change in the way business is conducted.**

As pointed out by Bhasin (2006),

51**"Leading banks are using Data Mining (DM) tools for customer segmentation and profitability, credit scoring and approval, predicting payment default, marketing, detecting fraudulent transactions, etc."**

2**Finally, the** sampled **respondents were asked, "In general, do** FCAs **needs to know computer-based forensic techniques?" Eighty-four percent of the respondents answered in "yes" to this question. Moreover, we asked the respondents "how important four different software tools are for** FCAs: **ACL, IDEA, Data Mining, and Digital Evidence Recovery." The scales were anchored at each end with the descriptors "extremely unimportant" and "extremely important," respectively. For the purpose of analysis, the descriptor "extremely unimportant" was given a weight of 1, while the descriptor "extremely important" was given a weight of 7. The mid-point of the scale "neither" was given a weight of 4. Table** 18 **shows the results.**

Bhasin (2013a) concluded as:

2**"The respondents rated each of these four tools as important, with data mining being rated as the most important with a mean score of 5.83."**

Table 18: Response about the

2**Ratings of the Importance of the Software Tools for** the **Forensic** Chartered Accountants Tools **Mean Standard Deviation ACL 5.45 (1.297) IDEA 5.24 (1.232) Data Mining 5.83 (1.240) Digital Evidence Recovery 5.82 (1.224)**

1**Discussion on frauds cannot be complete without analysis of human** behavior. **An employee in** a bank **is like a fish in** a small **ocean. Nobody can determine when and how much water a fish has consumed. Likewise a corrupt and dishonest person in** a bank **can commit frauds with impunity**

(ACFE, 1996). Unfortunately, most of the employees committing frauds get scot free, with the award of minor penalties, and the cases pending in courts keep on dragging for many years. As pointed out by Inamdar (2013), "The

30**time taken for cases to be ascertained as fraud was very high. It took over 10 years for 45% of the cases and between 5 to 10 years for 67% of the cases, creating a great disconnect between the punishment meted out and the offence." The**

RBI (on May 8, 2015) pointed out that "detection of fraud takes very

32**long-time,** and **banks tend to report an account as fraud only when they exhaust the chances of recovery. Delays in reporting of frauds** further delay **the alerting of other banks about the modus operandi through caution advices that may result in similar frauds being perpetrated elsewhere."**

Here, Bhasin (2103b) concluded,

72**"In the current environment, forensic accountants are in great demand for their accounting, auditing, legal, and investigative skills**

101**in order to detect and prevent frauds** and scams **in the**

Indian banking sector." There is lack of trained and experienced bank staff, and tremendous increase in banking business. By-and-large,

1**new recruits do not have adequate training or experience before they are put** into a **responsible**

position.

1**Ganesh and Raghurama (2008) believe that training improves the capabilities of employees by enhancing their skills, knowledge and commitment towards their work.**

1**Moreover, bank staff feels**"they are **overburdened** with work." **The life has become fast** and **the** bank staff **does not have enough time to scrutinize documents thoroughly.** Dilution **of**

93**system and non-adherence to procedures is** also **a significant reason for bank frauds.** This shows that **a** full-proof **system**

has not been developed and implemented to familiarize

1**the bank employees of various** types of **frauds that** take place **in banks every**

year.

> 17**"Most banks try to put in place robust systems and controls to prevent fraud and forgery—regrettably crooks and criminals use more and more sophisticated methods, especially where online fraud is concerned, to defraud banks," said Meera Sanyal, former CEO and Chairperson of Royal Bank of Scotland in India** (Pai, 2015). **The**

> 3**primary responsibility for preventing frauds lies with individual banks.**

> 1**Major cause for perpetration of fraud is laxity in observance in laid down system and procedures by supervising staff.**

However, the

> 3**RBI routinely advises banks about major fraud prone areas and the safeguards necessary for prevention of frauds. This is done so that banks can introduce necessary safeguards by way of appropriate procedures and internal checks. With growing usage and dependency on electronic forms of transaction, banks have employed more secured means and platform separate from the normal channels of communication. The authenticity and integrity of such a platform is ensured through usage of specific software, which ensures the validity of the bank's electronic documents**

(Dubey, 2013).

> 3**To keep the above frauds at bay, RBI prescribes that bank should conduct annual review of frauds and apprise its board regarding the findings;**

> 3**banks should have proper reporting mechanism in place to report to the RBI all information about frauds and the follow-up action taken.**

VII. Combatting Bank Frauds: What is the Role of Technology? Moreover, Bhasin (2015b) remarked,

> 40**"Technology is** like **a double-edged sword. On** the **one hand, perpetrators are using it to further fraudulent schemes; on the other hand, we are making some of our best progress using the same technology.**

Undoubtedly, technology can prove helpful in fraud detection and prevention in banks.

> 7**As technology becomes more advanced, fraudulent schemes will become more complex, while more sophisticated fraud solutions will be developed to combat hackers' best efforts."** But unfortunately, **the fraud**

> 25**takes on many forms to be handled with any 'single' application or approach.**

The cat and mouse game will continue.

> 7**As the landscape of fraud continues to shift, business leaders must be aware of trends and predictions that will allow them to implement internal/external controls and systems to help reduce the risk of fraud and keep them from becoming another statistic**

(Mueller, 2015).

5**Instead of relying on reactive measures like** whistleblowing, banks **can and should take a more hands-on approach to fraud detection. A fraud detection and prevention program should include a range of approaches—from point-in-time to recurring and ultimately, continually for those areas where the risk of fraud warrants. Based on key risk indicators, point-in-time (or ad** hock) **testing will help identify transactions to be investigated. If that testing reveals indicators of fraud, recurring testing or continuous analysis should be considered.**

5**By leveraging the power of data analysis software,** banks **can detect fraud sooner and reduce the negative impact of significant losses owing to fraud.**

83**Neural Networks have been extensively put to use in the areas of banking, finance and insurance.**

18**Usually such applications of neural networks systems involve knowing about the previous cases of fraud, to make systems learn the various trends. Fraud cases are statistically analyzed to derive out relationships among input data and values for certain key parameters in order to understand the various patterns of fraud. This knowledge of fraud trends is then iteratively taught to feed-forward neural networks, which can successfully identify similar fraud cases occurring in the future** (Quah **and**

Sriganesh, 2008). In

31**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

31**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 (Deloitte, Survey 2015).

37**Whether it** is **financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the** banking **sector. Most** banks **are, therefore, insisting on cashless and paperless transactions. The**

substantially larger proportion of technology related frauds in the Indian banking sector

22**by number is only expected as there has been a remarkable shift in the service delivery model with greater technology integration in the**

banking industry. Even

22**though the incidence of cyber frauds is extremely high, the actual amount involved is generally very low.**

As Bhasin (2007a) stated, “The

9**new technologies adopted by** banks **are making them increasingly vulnerable**

to various risks, such as, phishing, identity theft, card skimming, vishing (voicemail), **SMSishing**

(text messages), Whaling (targeted phising on high net worth individuals),

9**viruses and Trojans, spyware and adware, social engineering."**

49**While some of the risks in the** banking **sector have always been there, they keep** on **changing with the constantly evolving technology standards and regulatory framework. For instance,**

check fraud is in decline while electronic fraud is on the rise, and the latter tends to be perpetrated by more sophisticated criminals. Cheque fraud has been around the globe since the ancient time,

25**but the pace of changing schemes has been** very **slow for** banks **to react with very good procedures—many of them** still **'manual'.**

According to Bhasin (2011), "Some of the technological innovations, which may be already in use in some banks, are, briefly summarized. As: (a) Two-dimensional Bar Codes, (b) Data Glyphs, (c) Biometrics, (d) Cheque Image Processing, (e) Data Mining (f) Data Analytics, etc."

25**Given this complicated fraud prevention picture,**

25**banks will need to figure out their own patterns of exposure and deploy tools with the best fit.**

20**Banks have more technology and more incentive than ever to combat fraud in electronic banking services. But whether they have enough technology and incentive to protect consumers from the headaches of a compromised account, payment card or identity is doubtful. Threats are escalating more quickly than what banks, or even just other businesses in general, can deploy in terms of defenses against those threats**

(Geffner, 2014). There is

13**no "one silver bullet" to stop all fraud forever. Rather, the pace of new threats "is not going to slow down and nobody (no bank, no retailer, no consumer) is ever 100% secure. What** is **needed instead is a combination of checks from a layered approach that banks will have to adopt and consumers will have to accept if they want to utilize electronic banking services. That suggests consumers should expect to see, and might want to welcome, an ongoing stream of new solutions that banks will employ to stay a step ahead of electronic banking fraudsters.**

It is most unfortunate that

13**the current system of usernames and passwords, with which consumers are familiar,** is **basically broken.**

Consequently, banks also have begun to deploy an array of other technologies, some of which are so exotic and sophisticated they might seem like science fiction. Here, is a summary of some of the technology that is on tap: ?

8**Device fingerprinting tracks a series of identifiable hardware and software attributes to recognize a user's (or fraudster's) device. ? Behavioral analytics monitor navigation techniques and other aspects of a user's online behavior to search for anomalies or suspicious activity. ? Malware detection searches for**

potentially fraudulent changes to a user's Web browser to assess whether it' s been compromised. ? Knowledge-based authentication presents a series of static or dynamic and supposedly secret questions to establish a user's identity. ? Password tokens give a user a one-time-only password that must be entered before it expires. ? Out-of-band authentication challenges a user to access a one-time-only password or code that is sent to another device, such as a mobile phone or land line. ? Transaction signing requires a user to digitally sign each transaction. ? Endpoint protection requires a user to download a one-time-only, secure browser to access a website. ? Voice printing records attributes of a caller's speech over time and matches those attributes against subsequent calls. Voice printing is an example of biometrics, which use unique physical traits, or characteristics to identify individuals.

7However, as technology advances, we are seeing a distinct proliferation of more complex fraud schemes. At the same time, we are seeing more breakthroughs in the use of technology to detect fraud. Strategies that we have used in just the past few years will become completely outdated, as a fresh set of tactics will debut

(Mueller, 2015). To

7minimize the potential damage of fraud, companies need to invest not just in more advanced technology but in people and policies for detecting attacks as quickly as possible. While the networks are just too large to prevent every attack from occurring, detection is crucial. Most companies do not have adequate protocols and staff in place to deal with incidents of fraud. While advanced technology serves as a great tool to combat fraud, the issue should be viewed as more than just an IT problem and looked at as a business problem.

VIII. CONCLUSION

35While the banking industry in India has witnessed a steady growth in its total business and profits, the amount involved in bank frauds has also been on the rise. This

35unhealthy development in the banking sector produces not only losses to the banks but also affects their credibility adversely

(Kaveri, 2014). According to Klein (2015), "The business firms lose

595% of revenue each year to fraud. When applied to the 2013 estimated gross world product, this revenue loss translates to a global figure of nearly

USD3.7 trillion." Accordingly, the Government of India has expressed serious concern over the sharp rise in cases of fraud and corruption in the Indian banking sector. Recently in April 2015,

39RBI chief Mr. Rajan has written to the PMO seeking "concerted action in the country's 10 biggest bank frauds allegedly involving prominent real-estate, media and diamond firms that are being probed by the CBI," (Baruah, 2015).

Moreover,

15fraud and fraudulent activities inflict severe financial difficulties on banks and their customers; they also reduce the amount of money available for the development of the economy.

Many banks and companies that have been victims of frauds are reluctant to share and publicize the facts of the fraud cases due to fear of ‘adverse’ impact on their reputation (Banks, 2004).

3**Inadequate measure to prevent banking fraud is the primary reason for widespread frauds.**

3**So, what should banks do to safeguard the interests of its customers?**

According to S. Chakrabarty, Deputy Governor of the RBI, (2013), “Banks should strengthen their reporting system, quickly report fraud cases, and fix staff accountability. There is urgent need for sharing practices of fraudsters and methods used by such criminals.” As Siddique and Rehman (2011) stated, “The

60**only promising step is to create awareness among people about their rights and duties, and** make **application of laws more stringent to check**

crimes.”

3**Banks should ensure that the reporting system is suitably streamlined so that frauds are reported without any delay** and **fix staff accountability.**

3**Banks must provide sufficient focus on the “Fraud Prevention and Management Function” to enable effective investigation of fraud cases.**

The

3**fraud risk management, fraud monitoring and fraud investigation function must be owned by the bank’s CEO, its Audit Committee of the Board and the Special Committee of the Board, at least in respect of large value frauds. Banks can also frame internal policy for fraud risk management and fraud investigation function, based on the governance standards relating to the ownership of the function and accountability for malfunctioning of the fraud risk management process in their banks.**

19**While it is not possible for** banks **to operate in a ‘zero’ fraud environment, ‘proactive’ steps, such as conducting risk assessments of procedures and policies can help them** to **hedge their risk of contingent losses due to fraud.** By leveraging **the** power **of**

70**data analysis technology** banks **can detect fraud sooner and reduce the negative impact of significant losses owing to fraud.**

Moreover, use of new technologies (such as, data visualization, fuzzy logic, social network analysis, data mining, encryption, dynamic account modeling, etc.) can prove handy to mitigate the fraud risk in banks. Although banks

19**cannot be 100% secure against unknown threats, a certain level of preparedness can go a long way in countering fraud risk.** At least, **it can** minimize the **damages and protect** their reputations. **The** use **of**

21**neural network-based behavior models in real time has changed the face of fraud management all over the world.**

21**Fraud prevention specialists are grappling with ever-mounting quantities of data, but in today’s volatile commercial environment, paying attention to that**

data is more important than ever.

Expressing concern over zooming up of the corporate fraud in the last 15 years, Mr. Ranjit Sinha (CBI Director), said on May 14, 2014 at an ASSOCHAM event, “Rising number of frauds in Indian banks are taking place due to collective failure of regulatory oversight system comprising of external auditors, audit committee, internal audit system, board of directors, independent directors, shareholders, etc. All regulatory and investigative agencies must work in close cooperation and share their inputs and databases with each other in order to prevent frauds.” Although banks

95**cannot be 100% secure against unknown threats, a certain level of preparedness can**

help to face with confidence fraud risks. Very recently, in March 2015, the RBI has “established Central Fraud Registry by sharing information about unscrupulous borrowers at the time loans are sanctioned by cross-checking their credentials, and thus, helping banks to control their bad loans. The

9**CBI and Central Economic Intelligence Bureau will** also **share their databases with banks.” The** regulators **also** stressed on prevention **of**

fraud through improved market intelligence. Now, we are hopeful that with the help of new initiatives, banking industry would be able to minimize the fraud losses, gain customer trust and improve their reputation. The top three fraud risks that are currently the highest concern to the banks are: (a) Internet banking and ATM fraud, (b) E-banking (credit card and debit card, etc.) and (c) Identity fraud. In addition, Bhasin (2007a) sums up the scenario as, “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. Similarly, Bhasin (2013a) stated, “Prior to Satyam (often called as India’s Enron) fraud,

2**most companies’ perceived fraud as largely an internal event, primarily pinching the bottom line. They now understand that fraud can have an impact not only on the reputation and business prospects but also on the survival of the firm. This concern has led to higher demand for**

forensic chartered accountants (FCAs) in

2**countries like India and China. The Ministry of Corporate Affairs in India has also established the Serious Fraud Investigation Office, which seeks the help of** FCAs. **The government recently proposed to give more teeth to the SFIO under the new Companies Bill by providing it statutory recognition and empowering it with more powers.**

“The FCA’s

2**being professional members of the** Corporate Governance **and Audit Committees, can play a far greater role in coordinating company efforts to achieve a cohesive policy of ethical behavior within an organization,** said **Bhasin** (2013b). **By helping companies to detect and prevent fraud,** FCAs can **create a ‘positive’ work environment, establish ‘effective’ lines of communication, and be vigilant as a corporate ‘watchdog’, the** FCAs **role can gradually evolve into a key component in the CG system. Let us hope that** FCAs, **through their specialized knowledge, training and skills, will be able to improve CG scenario, still a work-in-progress, across the globe.**

Last, but not the least,

27**effective customer education and communications programs–helping customers recognize how to prevent fraud, but also helping them understand**

their own responsibilities–should go hand-in- hand with sophisticated cyber security measures. Only by working in partnership with their customers can financial institutions develop truly effective fraud prevention efforts.

REFERENCES Accenture Analytics Innovation Center (2015),

12**"Protecting the Customer: Fighting Bank Fraud in a New Environment,"**

available at https://www.accenture.com, 1-9. ACL Services Limited.

94**"Fraud Detection using Data Analytics in the Banking Industry,"** Discussion paper, **available at www.acl.com/**

bankingfraud, 1-8. ASSOCHAM

9**(2015). Current fraud trends in the financial sector,**

joint study of

104**Associated Chambers of Commerce** and **Industry of India, New Delhi,**

and PWC, June. Available at www.pwc.in/ Banks, D. G. (2004). The Fight against Fraud," Internal Auditor, Volume 62 (1), April, 62-66. Available at www.highbeam.com. Baruah, S.K. (2015).

84**RBI Chief Wants PMO to Act against Bank Frauds Worth Rs. 17,500 crore,** The **Hindustan Times,**

April 24, available at www.hindustantimes.com.

68**Bhasin, M.L. (2006). Data Mining: A Competitive Tool in the Banking and Retail Industries, The Chartered Accountant, October,**

588-594. Bhasin, M.L.

87**(2007). Forensic Accounting: A New Paradigm for Niche Consulting, The Chartered** Accounting Journal, January, **1000-1010. Bhasin. M.L.**

(2007a).

45**Mitigating Cyber Threats to** the **Banking Industry, The Chartered Accountant, April,**

1618-1624. Bhasin, M.L. (2011),

45**Combating Cheque Fraud in Banks: The Role of Internal Auditor and Technology,**

Siddhant, Dec. 6, available at www.indianjournals.com.

65**Bhasin, M.L.** (2011a), **"Corporate Governance Disclosure Practices in India: An Empirical Study, International Journal of Contemporary Business Studies (IJCBS),** 2(4), **April,**

34-57. Bhasin, M.L. (2012). Audit Committee Scenario and Trends in a Developing Country, School of Doctoral Studies European Union Journal, 4, 53-70.

73**Bhasin, M. L. (2013). Corporate Governance and Forensic Accountant: An Exploratory Study, Journal of Accounting, Business** and **Management,** October,

20(

2), 55-75. Bhasin, M.L. (2013a).

48An Empirical Investigation of the Relevant Skills of Forensic Accountants: Experience of a Developing Economy, European Journal of Accounting, Auditing and Finance Research, 1(2), June, 11-52.

Bhasin, M.L. (2013b),

81"Audit Committee Scenario & Trends: Evidence from an Asian Country, European Journal of Business and Social Sciences, 1(11), February, 1-

23.

56Bhasin, M.L. (2013c), "Corporate Accounting Fraud: A Case Study of Satyam Computers Limited," Open Journal of Accounting, 2(4), April, 26-38. Bhasin, M. L. (2015). Menace of Frauds in

53the Indian Banking Industry: An Empirical Study, Australian Journal of Business and Management Research,

4(2), April, 21-33. Bhasin, M. L. (2015a). Creative Accounting Practices

53in the Indian Corporate Sector: An empirical study, International Journal of Management Sciences and Business Research,

October, 4(10), 35-52. Bhasin, M.L. (2015b). Creative Accounting Practices in the Indian Corporate

45Sector: An Empirical Study, International Journal of Management Science and Business

Research, 4(10), October, 35-52.

55Bhasin, M. L. (2016). Contribution of Forensic Accounting to Corporate Governance: An Exploratory Study of an Asian Country, International Business Management, 10(4),

479-492.

1Calderon, T. and Green, B.P. (1994). Internal Fraud Leaves Its Mark: Here's How to Spot, Trace and Prevent It, National Public Accountant,

39(2), August, 17-20. Chakrabarty, K.C. (2013). Inaugural Address,

22National Conference on Financial Fraud, organized by ASSOCHAM, New Delhi, July 26.

44Chiezey, U. and Onu, A.J.C. (2013). Impact of Fraud and Fraudulent Practices on the Performance of Banks in Nigeria, British Journal of Arts and Social Sciences, 15(1), 12-

25. Deloitte Fraud Survey (2015), The

50Deloitte India Banking Fraud Survey Report Edition II.

Available at www.deloittee.com/in. Deloitte Survey (2012). Indian Banking Fraud Survey-2012, Business Standard, February

748. Dzomira, S. (2014), Electronic Fraud Risk in the Banking industry, Zimbabwe, Risk, Governance & Control: Financial Markets & Institutions,

4(2), 17-27. Ernest & Young (2010). Proactive Fraud Monitoring For Banks in India. Available at www.ey.com/india. Ernest & Young (2012). India Fraud Indicator 2012, a study by E&Y's Fraud Investigation and Dispute Services. Available at www.ey.com/india. Freddie Mac (2015). Fraud Mitigation Best Practices, January, available at www.freddiemac.com.

1Ganesh, A. and Raghurama, A. (2008). Status of Training Evaluation in Commercial Bank-- A Case Study. Journal of Social Sciences and Management Sciences,

37(2), Sept.137-58. Geffner, M. (2014). How banks fight fraud in electronic banking, May 29, 1-2. Available at www.banrate.com.

99Institute of Internal Auditors (2009). International Professional Practices Framework, IIA.

1Jeffords, R.; Marchant, M.L. and. Bridendall, P.H. (1992). How Useful Are The Tread Way Risk Factors? Internal Auditor, June,

60-62.

66Kaveri, V.S. (2014). Bank Frauds in India: Emerging Challenges, Journal of Commerce and Management Thought, 5(1), 14-26.

28Khanna, A. and Arora, B. (2009). A Study to Investigate the Reasons for Bank Frauds

86in Indian Banking Industry, Int. Journal of Business Science and Applied Management, 4(3), 1-21.

90Klein, R. (2015). How to Avoid or Minimize Fraud Exposures, The CPA Journal, March, 6-

11.

2KPMG (2012), India Fraud Survey, available at www.

kpmg. Kumar, V. and Sriganga, B.K. (2014).

16A Review on Data Mining Techniques to Detect Insider Fraud in Banks,

16International Journal of Advanced Research in Computer Science and Software Engineering, 4(12), December,

370-380.

63Mueller, K. (2015). How technology is shaping the fight against fraud?

25 February. Available at

63www.inc.com/ keithmueller /technology-shaping-the-fight-of-fraud- in2015 .html.

1-6 Pai, S. (2015),

17Banks No Safe Havens for Your Money; Depositors Lost Rs. 27,000 crore in Last Five Years, DNA, April 8.

Pai, S. and Venkatesh, M. (2014).

97Frauds Ripped Public Sector Banks of Rs. 23,000 crore, Hindustan Times, January 30,

available at www.hindustantimes.com. Pan, S. (2015). An Overview of Indian Banking Industry,

103International Journal of Management and Social Science Research, Vol. 4, No. 5, May,

67-71.

88Pasricha, P. and Mehrotra, S. (2014). Electronic Crime in Indian Banking, Sai Om Journal of Commerce and Management,

1(11), November. PwC (2014),

10Global Economic Crime Survey 2014, available at www.pwc.

org. Sen, A. (2015), KPMG's Latest Fraud Survey Kicks up Some Dangerous Statistics, available at www.allianceonemumbai.com.

58Siddique, M.I. and Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector: an overview, International Journal of Business and Information Technology,

1(2), September, 159-164. Singh, M.K. (2005).

41Bank Frauds—What Every Banker Needs to Know,

IBA Bulletin, September, 3-7.

43Soni, R.R. and Soni, N. (2013). An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks, Research Journal of Management Sciences, 2(7), 22-27 July.

1Ziegenfuss, D.E. (1996). State and Local Government Fraud Survey for 1995. Managerial Auditing Journal, Vol. 9, November, p.49.