Current fraud trends in the financial sector

June 2015





Contents

Financial services megatrends	U ²
Transformation through technology: The advent of a new world of financial services	08
Frauds in financial institutions: Understanding the types and modus operandi	10
Regulatory and legislative landscape	19
Global trends in fraud prevention and detection	2 1

Message from ASSOCHAM

In the globalised and liberalised business environment of the last few years, we face a drastically increasing volume of frauds, especially in the financial sectors in India. The Indian financial services sector has witnessed exponential growth in the last decade—a growth that has not been without its pitfalls, as incidents of fraud have also been on the rise. Fraud results in significant losses to the public exchequer, thus adversely affecting service delivery.

Financial fraud is big business, contributing to an estimated 20 billion USD in direct losses annually. Industry experts suspect that this figure is actually much higher, as firms cannot accurately identify and measure losses due to fraud. The worst effect of financial frauds is on FDI inflows into India.

The time has come for financial services organisations to pursue a more strategic approach to fraud management within. To overcome this challenge, they need strict and focussed steps. There needs to be transparency at all levels in organisations to reduce frauds.

To provide a holistic outlook with good understanding of the current financial sector scenario, regulatory viewpoints, anti-fraud resources, tools, knowledge and best practices, **ASSOCHAM along with PwC India** has drafted this paper, in an attempt to understand and establish sound business practices for reputation enhancement and growth, by equipping organisations against fraud.

I am sure this study will provide rich insight and adequate knowledge to all stakeholders.

With best wishes.

D S Rawat

Secretary General ASSOCHAM

Foreword

In 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 organised 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.

In this paper, we share our perspective on the trends in frauds in the financial sector, the changing regulatory landscape and the ways for fraud prevention and control. We hope these insights will help the financial services industry combat fraud and other forms of economic crime.

Best regards,

Dinesh Anand

Partner and Leader, Forensic Services PricewaterhouseCoopers Pvt Ltd. India

Financial services megatrends

New technologies reshaping financial services

Whether it's financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the financial services sector. Most financial institutions are therefore insisting on cashless and paperless transactions.

Susceptibility to fraud: Flipside of technology breakthroughs

The new technologies adopted by financial institutions are making them increasingly vulnerable to various risks such as phishing, identity theft, card skimming, vishing, SMSishing, viruses and Trojans, spyware and adware, social engineering, website cloning and cyber stalking.

Younger generation as a new market for financial institutions

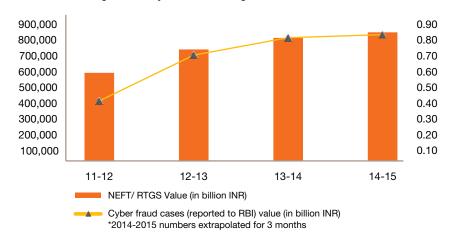
At the start of the century, Ray Kurzweil,¹ Futurist and Chief Engineer at Google, rightly predicted that "20,000 years of evolution would be crammed into the next 100."

In 2020, the average Indian will be 29 (lower than the average age in China and Japan). India's workforce will be the largest and youngest in the world.²

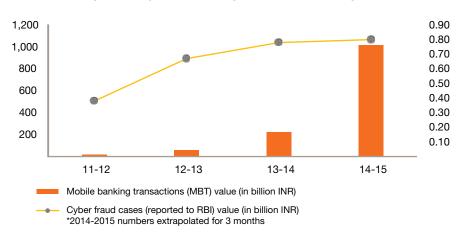
The younger generation in India today has financial and social independence. They are not only driven by high aspirations but are also technology savvy, well informed and connected through social media.

Hence, financial institutions are eager to tap into this new market by offering services and products that are tailored to their requirements.

Growing trend of cyber frauds with growth in NEFT/RTGS transactions



Growing trend of cyber frauds with growth in mobile banking transactions



Source: https://www.rbi.org.in/scripts/NEFTView.aspx

The Economic Times, 4 March 2015



- According to RBI records, 22 million of the 589 million bank account holders use mobile banking apps.
- The volume of mobile banking transactions has risen from around 18,190 million INR in 2011–12 to approximately 1,018,510 million INR in 2014–15.

^{1.} http://www.kurzweilai.net/the-law-of-accelerating-returns

^{2.} https://www.pwc.in/en_IN/in/assets/pdfs/publications/2014/indian-workplace-of-2022.pdf

Evolving regulatory framework driving increased compliance among financial institutions

- Regulations governing financial institutions are set to have a huge impact.
- The reporting requirements of the financial sector have never been this stringent.

The regulatory framework in India is continuously evolving. Driven by the need for stricter regulatory compliance and the global standards of delivering financial products and services, the regulators can be seen as becoming more aggressive and stringent in enforcing the existing regulations. At the same time, they are also striving to constantly evolve these legislations and statutes to keep up with the international technology and service standards.

According to the RBI, the primary responsibility of preventing frauds lies with banks themselves³ (Circular No. DBS. FrMC.BC.No.1/23.04.001/2013-14).

Customer at the forefront

Changing technology and rapid flow of information have placed the customer at the centre. It is critical for every financial institution to understand customer needs and expectations and offer customised services.

As the world shrinks, financial institutions need to set new standards for product and service delivery that not only satisfy customers but also ensure regulatory compliance and help them stay ahead in their business.

Financial inclusion to spur growth

Keeping in mind the twin objectives of financial stability and customer protection, the government has taken meticulous steps for financial inclusion, wherein banks have been advised to devise financial inclusion plans congruent with their business strategies and comparative advantages to make them an integral part of their corporate business plans.

According to RBI governor Raghuram Rajan, "financial inclusion refers to universal access to a wide range of financial services at a reasonable cost. This includes not only banking products but also other financial services such as insurance and equity products."

The following schemes have been introduced as part of this initiative:

- Pradhan Mantri Jan Dhan Yojana
- Pradhan Mantri Suraksha Bima Yojana
- Pradhan Mantri Jeevan Jyoti Bima Yojana
- Atal Pension Yojana

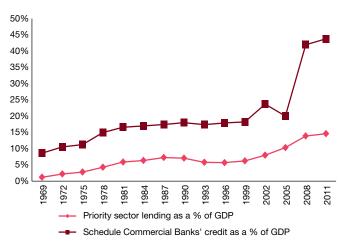
Changing landscape of financial services

- In India, the financial services sector operates as an arrangement of institutions—formal and informal—that facilitates the flow of surplus funds in the economy to deficit spenders.
- The institutional arrangement in the financial services sector consists of scheduled commercial banks (SCBs), insurance companies, non-banking financial companies (NBFCs), mutual funds, specialised foreign institutional investors (specialised FII), urban co-operative banks (UCBs), regional rural banks (RRBs), national pension scheme (NPS) fund and other smaller financial entities.
- Like many developing economies, India has an informal financial system consisting of loan brokers, NGOs helping self-help groups (SHGs), share brokers and traders, pawnbrokers, etc. Given the heterogeneous nature of entities and activities, no consistent database of customers and transactions is available. Informal financial agencies are also not considered very reliable in terms of customer protection.

Spread of bank branches for scheduled commercial banks: Decadal growth

	Rural	Semi- urban	Urban	Metro
1980–81 to 1989–90	7.26%	3.55%	4.4%	4.63%
1990–91 to 1999–2000	-0.91%	3.3%	3.7%	6.24%
2000–01 to 2009–10	-0.37%	3.78%	5.77%	7.19%
Total	0.93%	2.67%	3.69%	4.55%
Bank branches as of March 2014	44,699	31,298	21,310	19,143

Deployment of aggregate and priority sector credit



Evolving risks in the financial services sector

While some of the risks in the financial services sector have always been there, they keep changing with the constantly evolving technology standards and regulatory framework.

 Cybercrime: A majority of the banks in India offer online and mobile banking services. Most of the transactions are conducted via payment cards, debit and credit cards, and electronic channels such as ATMs. Consequently, both private and public banks as well as other financial institutions in India are becoming increasingly vulnerable to sophisticated cyberattacks.

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

 Identity theft: With the proliferation of mobile devices and online platforms, the nature of identity theft has changed in today's world. According to an RBI report,⁴ provisioning for loan losses is a critical component of effective financial reporting and prudential supervision. However, provisioning reduces an institution's reported net income for the period in which it is recognised.

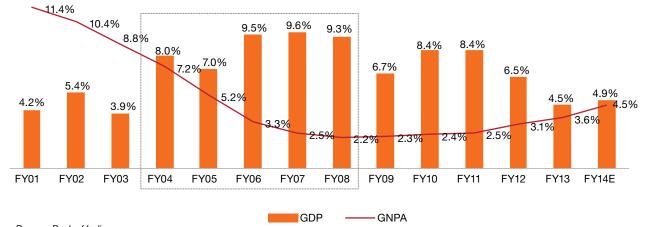
•••••

- Money laundering: India has
 witnessed numerous terror attacks
 and remains a potential target for
 such strikes. Stringent regulatory
 requirement and media scrutiny
 have made it mandatory for financial
 institutions to perform strict
 compliance checks to prevent the use
 of money laundering to fund terrorist
 activities.
- Black money: According to the Global Financial Integrity Report, 5 the total amount of illicit money moving out of India rose to 439.59 billion USD (28 lakh crore INR) from 2003 to 2012. In 2012, India ranked third globally, with an estimated 94.76 billion USD (nearly 6 lakh crore INR) in illicit wealth outflows. With the passing of the new Black Money (Undisclosed Foreign

- Income and Assets) and Imposition of Tax Act, 2015, financial institutions are under growing pressure to eliminate this malignancy.
- Loan loss: The risk of loan loss is high in India. Due to lack of appropriate due diligence and monitoring of loans, the number of loan defaults has increased in recent years. The non-performing assets are growing in last few years while the GDP has been declining.

According to the 2013 Norton Report, ⁶ India ranks among the top 5 countries in terms of number of cybercrime incidents such as ransomware, identity theft and phishing attacks.

Gross NPA vs GDP in India



Source: Reserve Bank of India

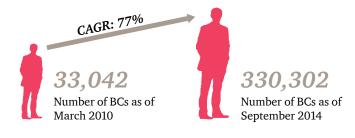
^{4.} http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DDP033012FL.pdf

^{5.} http://www.gfintegrity.org/reports/

^{6.} http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013



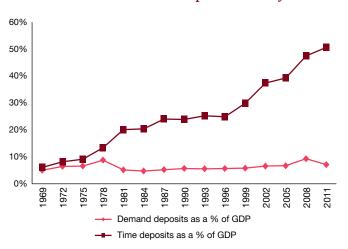
Growth in banking outlets via business correspondents (BCs)



Access to bank accounts

~ 296.1 million adults had access to bank accounts in 2011 ~ 425 million adults had access to bank accounts in 2014

Scheduled commercial banks' deposits as a % of GDP



Number of basic saving bank deposit accounts (BSBDAs)



Total growth of deposits and credit of scheduled commercial banks (1980–2010)



Sources: RBI – Statistical tables relating to banks in India; RBI – Trends and progress of banking in India reports; Madras School of Economics research; World Bank Findex; Census 2011; Planning Commission; PwC analysis

Transformation through technology: The advent of a new world of financial services

The Digital India dream

- The Digital India programme is a transformed version of the already running National e-Governance Plan.
- The project aims to provide thrust to nine pillars identified as growth areas.
- These pillars include broadband highways, everywhere mobile connectivity, Public Internet Access Programme, e-Governance, e-Kranti (which aims to give electronic delivery of services), information for all, electronics manufacturing, IT for jobs and early harvest programmes.

Source: Logging into Digital Banking

7.9 42,300 billion INR Wi-Fi in 400 Villages to universities and be provided public places in 25 universal mobile cities by June 2015 access by 2018 320 10 million billion INR persons in towns and Cost of establishing villages provided rural broadband in with IT services or 2.5 lakh villages by business training March 2017 1,130 billion INR Total investment in Digital India

programme

Policy and market trends

In August 2014, the government of India announced a planned investment of 1,330 billion INR in the Digital India project that aims to provide universal mobile phone access, broadband access in 250,000 villages and Wi-Fi hotspots in every city with a population of 1 million plus by the year 2020.

As per Celent's banking practice study, total bank IT spending across North America, Europe and Asia-Pacific will grow to 196.7 billion USD in 2015, an increase of approximately 4.6% over 2014.

The majority of the growth is expected to come from banks in the Asia-Pacific region: The spending of banks in this region is expected to grow by 5.6% in

2015 to 70.3 billion USD. The IT spend by Indian banking and securities companies in 2015 will be 15% more than the 46,600 crore INR spent in 2014.

Mobile financial services

RBI issued the guidelines for mobile banking transactions

Nonbanks/NBFCs permitted to issue mbased semi-closed instruments Banks permitted to issue semi-closed instruments through agents/BCs

RBI Master circular on mobile banking transactions issued in July 2014

October 2008

April 2009

August 2009

September 2010

November 2010

July 2014

RBI issued guidelines on prepaid instruments

Immediate
payment services (IMPS)
launched in India

Draft guidelines for licensing of payment banks

Proliferation of social media

The internet is fast becoming the favoured mode for performing financial transactions—checking one's bank balance, requesting for bank statements and chequebooks, upgrading debit cards and even purchasing virtual goods. Also, financial institutions are increasingly using social media platforms to engage their customers and enhance their service offerings.

One of the largest private sector banks in India recently launched a multi-social payment app that allows customers to transfer money through social media channels.

Rewards vs risks: Is reliance on social media a double-edged sword?

While social media platforms have many advantages, they also carry inherent risks of security breaches. Financial transactions via social media channels, and especially those on mobile banking apps, are prone to malware attacks.

•••••

Modern banking

Currently, 74% of the Indian population has mobile phones. Mobile payment volumes have hence registered a steady rise.

A recent study on e-commerce in India by Accel Partners estimated that shopping through mobile phones grew by 800% in 2013. It is expected to show a compound annual growth rate of 150% by 2016.

Branchless banking: An upcoming trend

Connectivity is the backbone of digital banking. The high volume of ICT transactions through banking correspondents has motivated the institutions to develop a solution that combines a mobile phone and a card reader to function together as a micro ATM. This solution transfers data using USSD technology that does not require a smart phone or internet connection and is thus accessible by a larger population.

A banking correspondent (intermediary) can use this device to deposit or withdraw money for a customer in rural areas where banking facilities are scarce, thus integrating these regions into core banking systems.

Increased risk of fraud

Such technological solutions also expose customers as well as financial institutions to the risk of bank spoofing, hijacking of mobile phones and SIM card cloning.

As per the Minister of Communications and IT, Government of India, cyber fraud cases worth 497 crore INR have been reported by the RBI and CBI since 2011.⁷

Security of mobile banking a top concern

Recent innovative financial services such as mobile wallets have also been targeted by fraudsters. Similarly, money management tools are becoming increasingly susceptible to cyber threats and related frauds.

Emerging technologies

- Digitised and automated account opening procedures
- Biometric products for enrolment, storage and verification of documents

Other financial institutions

Like banks, mutual funds are also prone to risks posed by emerging technologies. Mutual fund houses received about 21,000 complaints from investors in 2014–158.

Unlike banks, customers of non-banking

finance companies (NBFC) prefer to bank offline. As per a recent article in Business Standard, though NBFCs are offering online services, not many customers have been using them.

If NBFC customers do take the digital route in future, they are more likely to do so via mobile phones and not the online channel.

The insurance industry in India is also looking at adopting new channels of distribution that are already in place internationally. In one such initiative, a US auto insurance major installed Direct on the Spot Kiosks at public places with transactional capabilities. These kiosks allow customers to scan their driver's license in order to obtain quotes and walk away fully insured in less than five minutes.

Capital markets

The growing dependency of security exchanges on internet-based (IP) platforms has led to higher reputation, market and operational risks. Technological innovations have affected everything from software to system design and architecture. Some of these innovations are the use of extensible mark-up language (XML) as the industry IP language, straight through processing of data, pervasive or diffuse computing and grid computing, as well as the increased use of the internet and wireless technology.

According to a report published in ICFE Fraud Magazine,9 in 2013, 46% of the complaints or identity theft frauds reported globally involved breaches of government documents. Over 20% of all identity theft frauds or complaints were related to breaches of data of financial institutions (e.g. credit card, loan or other bank information).

RBI circular November 2014:¹⁰ It has been reported that in some cases even though the original cheques were in the custody of the customer, cheques with the same series had been presented and encashed by fraudsters.

National crime records bureau statistics11

- Total number of cases of cybercrime registered in India in 2013: 4,356
- Total number of arrests made: 2,098

Common types of identity theft frauds/Complaint percentages in 2013



Note: These percentages don't add up to 100 because some of the complaints include more than one type of identity theft.

- 7. http://www.freepressjournal.in/over-rs-490-cr-involved-in-cyber-fraud-cases-since-2011-govt/
- 8. https://www.amfiindia.com/
- 9. http://www.fraud-magazine.com/default.aspx
- 10. https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=9322

^{11.} http://ncrb.gov.in/

Frauds in financial institutions: Understanding the types and modus operandi

Evolution of fraud

1990-1999

- Hawala transactions
- Ponzi schemes
- Fake currency
- Cheque forgery
- Advancing loans without adequate due diligence
- Siphoning of investors' money through fictitious companies
- Use of fictitious government securities

2000-2015

- Tax evasion and money laundering
- Black money stashed abroad
- Cybercrime
- Debit/credit card fraud
- Identity theft
- Fake demat accounts
- Benami accounts
- Collusive frauds emanating kickbacks to employee of financial institutions
- Use of forged instruments such as stamp papers and shares
- Violation of Know Your Customer (KYC) norms



Overview of frauds in the financial sector:

Bribery and corruption: Corruption is one of the biggest challenges faced by the Indian economy. Various surveys and studies conducted by industry bodies like Transparency International have identified corruption as a key risk for Indian corporates.

India ranked 85 among the 170 countries included in Transparency International's Corruption Perceptions Index - 2014. This ranking has gone up by 9 points as compared to the country's rank of 94 out of 177 in 2013. Some of the key reasons for high corruption in India are the lack of a strong legal framework and enforcement of anticorruption laws, red-tapism and a result-oriented approach.

- Terrorist financing: It involves the raising and processing
 of assets to supply terrorists with resources to pursue their
 activities. While money laundering and terrorist financing
 differ in many ways, they often exploit the same vulnerabilities
 in financial systems that allow for an inappropriate level of
 anonymity and non-transparency in the execution of financial
 transactions.
- Money laundering: The goal of a large number of criminal acts is to generate a profit for the individual or group that commits the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process enables the criminal to enjoy profits without jeopardising their source.
- Tax evasion: The general modus operandi to evade tax include wrongly availing CENVAT credit, non-registration, short payment of taxes, wrong classification and undervaluation of services.

- *Cybercrime:* According to RBI, in 2012, 8,322 cases of cyber frauds amounting to 527 million INR were reported. Although the number of cases reported decreased from 15,018 in 2010, the total amount involved increased from 405 in 2012, implying that the average value per cyber fraud case has increased significantly.
- Data security: In addition to website defacement and distributed denial of service, hackers have been making use of social media to launch more sophisticated attacks. Hacking attacks are tailored to target a particular organisation or entity and are often focussed on gathering valuable sensitive data.

Fraud landscape: An overview

- Fewer instances but increased financial impact: According to the RBI, while the number of fraud cases has declined from 24,791 cases in 2009–10 to 13,293 cases in 2012–13

 — i.e. a 46% drop—the amount involved has increased substantially from 2037.81 crore INR to 8646.00 crore INR—i.e. an increase of 324% ¹⁴
- Pareto law applies: A granular analysis in this study reveals
 that nearly 80% of all fraud cases involved amounts less
 than 1 lakh INR, while on an aggregated basis, the amount
 involved in such cases was only around 2% of the total
 amount involved.¹⁵
- Major risk areas: Corruption and cash in hand are the most fraud vulnerable areas in the financial services sector.¹⁶
- Latest reported facts and figures: In India, frauds worth 11,022 crore INR were unearthed in public sector banks between April–December 2014; 2,100 cases of fraud were reported to the RBI.¹⁷

The extent of tax evasion can be evaluated from the fact that the Directorate General of Central Excise Intelligence (DGCEI) registered 1,144 cases of service tax evasion involving a revenue of 7,928.22 crore INR during 2013–14 as against 841 cases involving a revenue of 4,693 crore INR in 2012–13.13

13. http://www.business-standard.com/article/pf/ about-rs-8-000-cr-service-tax-evasion-detectedduring-2013-14-114040600173_1.html 14. https://rbio.org.in/scripts/BS_SpeechesView.

aspx?Id=826 15. https://rbi.org.in/scripts/BS_SpeechesView.

16. http://www.acfe.com/rttn/docs/2014-report-to

nations.pdf 17. http://rbidocs.rbi.org.in/rdocs/Speeches/PDFs/ DGKCAE200713.pdf

Fraud risks: Banking

Fraudulent documentation

Fraudulent documentation involves altering, changing or modifying a document to deceive another person. It can also involve approving incorrect information provided in documents knowingly. Deposit accounts in banks with lax KYC drills/ inoperative accounts are vulnerable to fraudulent documentation.

Some examples:

- An individual illegally obtains personal information/ documents of another person and takes a loan in the name of that person.
- He/she provides false information about his/her financial status, such as salary and other assets, and takes a loan for an amount that exceeds his eligible limits with the motive of non-repayment.
- A person takes a loan using a fictitious name and there is a lack of a strong framework pertaining to spot verifications of address, due diligence of directors/promoters, pre-sanction surveys and identification of faulty/incomplete applications and negative/criminal records in client history.
- Fake documentation is used to grant excess overdraft facility and withdraw money.
- A person may forge export documents such as airway bills, bills of lading, Export Credit Guarantee Cover and customs purged numbers/orders issued by the customs authority.

Multiple funding/diversion/siphoning of funds

Siphoning of funds takes place when funds borrowed from financial institutions are utilised for purposes unrelated to the operations of the borrower, to the detriment of the financial health of the entity or of the lender. Diversion of funds, on the other hand, can include any one of the following occurrences:



- · Use of short-term working capital funds for long-term commitments not in conformity with the terms of sanction
- Using borrowed funds for creation of assets other than those for which the loan was sanctioned
- Transferring funds to group companies
- Investment in other companies by acquiring shares without the approval of lenders
- Shortage in the usage of funds as compared to the amounts disbursed/ drawn, with the difference not being accounted for



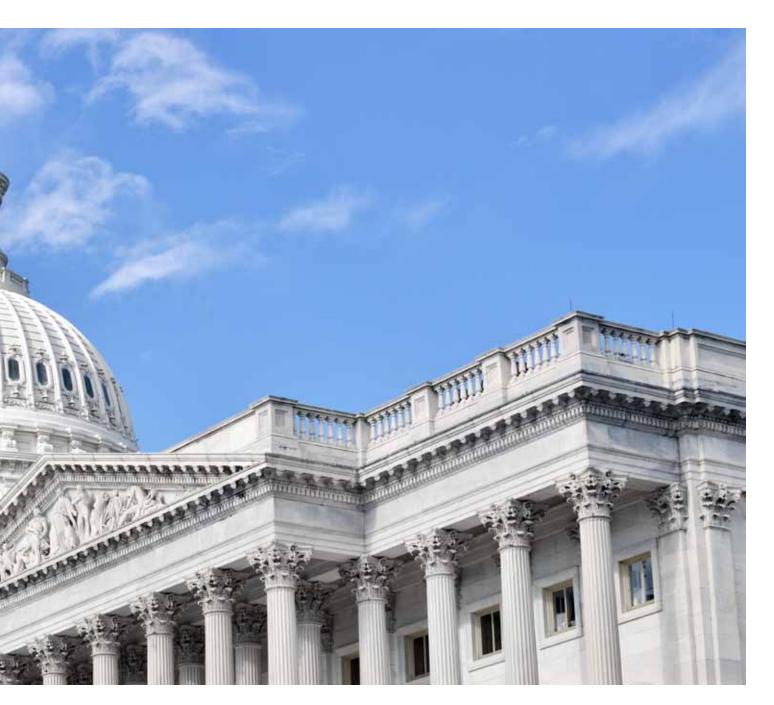
Identity theft

Fraudsters are devising new ways to exploit loopholes in technology systems and processes. In case of frauds involving lower amounts, they employ hostile software programs or malware attacks, phishing, SMSishing and whaling (phishing targeting high net worth individuals) apart from stealing confidential data.

In February 2013, the RBI advised banks to introduce certain minimum checks and balances such as the introduction of twofactor authentication in case of 'card not present' transactions. 18

Some examples:

- Unauthorised emails asking for account information for updating bank records are sent by fraudsters. The customer information is then misused for misappropriating funds.
- Access rights for making entries are given to unauthorised people.



- Bank employees keep original Fixed Deposit (FD) receipts with themselves and hand over phony FD receipts to customers. They then revoke FDs by forging signatures.
- *Lost/stolen card*: It refers to the use of a card lost by a legitimate account holder for unauthorised/illegal purposes.
- Account takeover fraud: An individual illegally obtains
 personal information of valid customers and takes control of
 the card account.
- Theft of valuables: Fraudsters open bank lockers to take key impressions of other lockers and then use duplicate keys to steal assets.

Internet banking and related frauds

Around 65% of the total fraud cases reported by banks were technology-related frauds (covering frauds committed through/ at an internet banking channel, ATMs and other payment channels like credit/debit/prepaid cards), whereas advance-related fraud accounted for a major proportion (64%) of the total amount involved in fraud.¹⁹

Some examples:

- Triangulation/site cloning: Customers enter their card details on fraudulent shopping sites. These details are then misused.
- *Hacking:* Hackers/fraudsters obtain unauthorised access to the card management platform of banking system. Counterfeit cards are then issued for the purpose of money laundering.
- Online fraud: Card information is stolen at the time of an online transaction. Fraudsters then use the card information to make online purchases or assume an individual's identity.
- Lost/stolen card: It refers to the use of a card lost by a legitimate account holder for unauthorised/illegal purposes.

- Debit card skimming: A machine or camera is installed at an ATM in order to pick up card information and PIN numbers when customers use their cards.
- ATM fraud: A fraudster acquires a customer's card and/or PIN and withdraws money from the machine.
- **Social engineering:** A thief can convince an employee that he is supposed to be let into the office building, or he can convince someone over the phone or via e-mail that he's supposed to receive certain information.
- Dumpster diving: Employees who aren't careful when throwing away papers containing sensitive information may make secret data available to those who check the company's trash.
- False pretences: Someone with the intent to steal corporate
 information can get a job with a cleaning company or other
 vendor specifically to gain legitimate access to the office
 building.
- Computer viruses: With every click on the internet, a
 company's systems are open to the risk of being infected with
 nefarious software that is set up to harvest information from
 the company servers.

Incorrect sanctioning or external vendor-induced fraud

According to PwC's Global Economic Crime Survey 2014,²⁰ external fraudsters are still the main perpetrators of economic crime for the majority of financial service organisations (57% in 2014 and 60% in 2011).

Financial institutions are prime targets for external frauds, given the amount of money fraudsters can potentially obtain as well as the sensitivity of data held by these organisations (credit card and personal identity details, for example).

The financial services sector also tends to be more strictly regulated and as a result, many business processes and functions have corporate controls in place. This makes it more difficult for frauds to be internally perpetrated without discovery. The absence of a proactive and robust monitoring framework, however, does not allow the entity to identify conflict of interest issues such as employees or agents having a close relationship with other entities.

Some examples:

- Falsified Valuations: External consultants advising loan borrowers to fabricate their valuation report and inflate the amount of funds that can be borrowed
- Corporate espionage: Sharing trade secrets or confidential customer information with the competitor for commercial benefits
- Merchant collusion: Merchant owners and/or their employees conspiring to commit frauds using their customers' accounts and/or personal information
- *Ponzi scheme:* A type of pyramid scheme, where money from new investors is used to provide returns to previous investors
- Off shore investing: External vendors convincing investors to invest in outside companies by showing higher returns when the companies don't exist in reality
- Bogus offerings: Investing in a bogus company (no operations, earnings or audited financial statements)
- *Misappropriation of loan disbursements*: Loans of lesser value being disbursed to farmers and funds being misappropriated by intermediators through false documentation



- Inflation of projected sales figures or past income: Large and unusual year end transactions resulting in profit for the enterprise.
- Others: Faking net worth of directors, faking CA certificates
 or financial statements, inflating sundry debtors or reducing
 sundry creditors, reference checks not being conducted,
 irregularities in repayments for loans availed from other
 banks, frequent start-ups, maintenance of a large number of
 small enterprises, etc.

Counterfeit cheques

Counterfeit or fake cheques that look too good to be true are being used in a growing number of fraudulent schemes, including foreign lottery scams, cheque overpayment scams, internet auction scams and secret shopper scams. Unsuspecting sellers get stuck when scammers pass off bogus corporate or personal cheques.

Tunnelling/phoenixing or asset stripping

Even though the above-mentioned terms are interchangeably used, in the banking world, asset stripping primarily implies taking company funds or assets of value, and leaving behind debts.



This can happen when a company's directors transfer only the assets of one company to another and not the liabilities. The result is a dormant company which has to be liquidated as it has large liabilities that cannot be met.

Some examples:

- Asset stripping: Fraudsters deliberately target a company or companies to take ownership, move the assets and then put the stripped entity into liquidation.
- Phoenixing: Directors of a company move the assets from
 one limited company to another to 'secure' the benefits of
 their business and avoid the liabilities. Most or all directors
 will usually be the same in both companies. This usually is a
 way of 'rescuing' the assets of a failing business rather than
 targeting a company.
- *Teeming and lading:* In order to maintain the liquidity situation artificially, amounts received from the subsequent debtor are credited to the earlier debtor's account so that one debtor's account does not show an outstanding balance for a long time. Such a process is continued till the time the original amount misappropriated is finally replaced or till the time the cashier is caught.

Overvaluation or absence of collaterals

Absence of stringent guidelines on the due diligence of professionals assisting borrowers at the time of disbursement of loans may result in valuation agencies or advocates facilitating the perpetration of frauds by colluding with the borrowers to inflate security valuation reports.

Some examples:

- Concealing liabilities: Borrowers concealing obligations such as mortgage loans on other properties or newly acquired credit card debts in order to reduce the amount of monthly debt declared on the loan application
- *Misstatement:* Deliberately overstating or understating the property's appraised value; when overstated, more money can be obtained by the borrower in the form of a cash-out refinance, by the seller in a purchase transaction, or by the organisers of a for-profit mortgage fraud scheme
- Cash back schemes: The true price of a property illegally being inflated to provide cash-back to transaction participants, most often the borrowers, who receive a 'rebate' that is not disclosed to the lender
- Shot gunning: Multiple loans for the same home being obtained simultaneously for a total amount greatly in excess of the actual value of the property

Mobile banking: Risks

There are two types of mobile financial services that are currently offered in the Indian market—mobile banking and mobile wallets. Being an easy and convenient mode of transacting, there has been a 55 times rise in value usage of mobile banking and 5.5 times rise in the volume of transactions between FY12 and FY15.

After the recent changes to RBI policy, customers of semi-closed pre-paid instruments (PPIs) can now do the following:

- Load up to 1,00,000 INR in wallets
- Transfer money from their wallet to any bank account

This move, on one hand, enhances the convenience and adoptability of a mobile wallet and on the other, makes it more susceptible to fraud risks.

Risks associated with mobile banking

- Mobile banking application being mapped to an incorrect mobile number: For bank customers who do not use mobile banking, an employee of the bank could attach an associate's mobile number to the bank account and install a mobile application on his mobile device. The customer's account is compromised by the associate and he or she does not get any notification about the same.
- Creating fake and non-existent users on the mobile financial services *platform:* Most of the banks appoint a third party vendor to develop a mobile application to be integrated with their core banking system. The vendor may create two unauthorised users with rights to initiate and verify transactions, and transfer funds from the organisation to his associates' wallets, effectively stealing money from the bank.
- Malware: The increase in the number of mobile banking users is accompanied by a rise in attacks through malware.
- Data theft: Mass attacks are possible through the theft of credentials which can be used for personal benefits.

- SIM swap: SIM swap means replacing the old SIM with a new one, when the old gets lost or damaged, or when one needs a differently sized SIM card. If a fraudster manages such a swap, he can carry out numerous fraudulent transactions using the mobile number of the victim. For instance, the valid mobile station international subscriber directory number (MSISDN) is moved to another handset. The user has no access to their account and receives no notification. The user with the other handset, on knowing the PIN, can transact in the account.
- Fake or similar interface apps: Fake applications, with exactly the same user interface as the original application, are being created to steal confidential information shared by the

Risks associated with mobile wallets

- Increased risk of money laundering: Transfer of money into and out of a mobile wallet from or to a bank account is now possible. Cash-in from the bank account of an individual and cash-out to a different bank account of another individual can be used as a platform for laundering unaccounted
- Unauthorised deductions from the wallet of a customer (especially a dormant or infrequent customer account): Employees of the mobile wallet service provider may misuse the balance stored in the wallet of a customer by making unauthorised deductions. Moreover, in case of a mis-happening to a customer with no nomination facility, the balance in the customer's account is not passed on to his family members and remains with the service provider, which ultimately becomes a low-hanging fruit for the fraudsters.
- Failure to conduct proper due diligence of merchants: If the merchant on-boarded by the service provider is a fraudster, and the payment is made by the customer for fictitious goods or services from the merchant, cash can be rotated with minimum transaction fees.
- No auto log off facility: An individual

usually opens the application on his mobile device for availing of the services and closes the application, instead of logging out. If the mobile device is stolen or lost and a fraudster opens the application, he can misuse the remaining balance in the service provider's wallet.

Fraud risks: Insurance companies

Large accumulations of liquid assets make insurance companies attractive for loot schemes. These companies are under great pressure to maximise the returns on investing the reserve funds, making them vulnerable to high-yielding investment schemes.

The insurance industry has witnessed an increase in the number of fraud cases over the last couple of years. A growing number of organisations are realising that frauds are driving up the overall costs of insurers and premiums for policyholders, which may threaten their viability and also have a bearing on their profitability. To keep these risks under check, a detailed framework for insurance fraud monitoring



has been laid down with effect from 2013–14 and is applicable to all insurers and reinsurers.

- Policy holder and claims fraud: Policy holder committing fraud against the insurer at the time of purchase and/or execution of an insurance product
- Intermediary fraud: Intermediaries committing frauds against the insurer and/or policyholders
- Internal fraud: Employees commit fraud suo moto or in collusion with external parties or amongst themselves against the insurer

Broad categories of fraud risks in the insurance sector

Misrepresentation: Misrepresenting critical information relating to a profile (incorrect income, educational qualification, occupation, etc)

Example: The proposal form mentioned that the client had a shop in the market, whereas investigations revealed that the client was a small-time vendor sitting on a footpath.

Forgery or tampering documents:

Forging the customer's signature in any document, proposal or any supporting document

Example: The client (staying in one city) and working as a surgeon was required to countersign the application form for some corrections. The form came back and it was found that the signatures were forged by the advisor, who was the client's brother.

Bogus business: Proposal forms submitted for non-existent customers

Example: A sales manager or broker logs in the proposal of a non-existing client

Cash defalcation: Agent collecting the premium but not remitting the cheque to the insurance company, owing to which the insured has no coverage

Example: The advisor had collected the premiums from the customer and had not deposited the same for almost a month; it came to the insurer's notice when the customer was sent the lapsed letter.

Mis-selling: A selling practice wherein the complete, detailed and factual information of a product is not given to the customer

(also called product misinformation); can include incomplete or incorrect representation of the terms and conditions such as guaranteed returns, rider features, charges, linked product vs endowment, facility of top-up vs regular premium, premium holiday, etc

Example: The customer was given a cover of 1 lakh INR and the premium was 5 lakh INR. This was a clear case of mis-selling as even the facility of a top-up was not explained to the client.

Pre-signed forms: Obtaining pre-signed blank forms and filling the address change request (ACR)/contact number change (CCR) without actually physically seeing the client or satisfying oneself about the client

Example: While the proposal form mentioned that the customers were working in an electronic agency, in reality they were working in some other business.

Doctor's nexus: Doctor being involved with the perpetrators in committing life insurance fraud

Example: A doctor gave clean medical reports, while the fraudster influenced the doctor to conceal the information.



Fraud risks: NBFCs

Incorrect KYC details

KYC details are collected and assessed by the institution at the time of customer on-boarding as well as during re-KYC. A fraudster can find an opportunity to use incorrect KYC details during the customer lifecycle to commit fraud.

Some examples:

- Tampering of KYC details
- PAN being provided by the investor, change in name and other personal details not being updated, leading to opportunities for fraudsters to remit money to incorrect bank accounts and dummy customers
- Units of different account holders with the same or similar name getting consolidated despite varying bank details and addresses in different folios
- Mismatch between folios (schemes) for consolidation as per the customer

Incorrect date and time stamp

A time stamp is a digital signature that establishes the integrity of a reference submitted by a subscriber on a specific date and at a certain time. In order to carry out time stamp when the SIP transmits it to a

The staff or broker providing preferential treatment to an investor by stamping the receipt of an application or redemption form with an incorrect time or date

Misappropriation, siphoning of funds by brokers or intermediaries

- The broker cheating the investor or account holder by taking a blank

Incorrect commission or incentives

Lax internal controls may give way to in order to avail of extraneous commission

Commission being paid on selfinvestment and withheld cases

Front running and insider trading

In order to pass on the benefit of windfall broker may resort to unethical practices such as front running and insider trading.

- Broking house being paid "under the table" in order to portray the company's stock as the favourite, causing the investor to buy the stock
- without any structured information that recommends the purchase
- company just before the broking house

Missing dividend payments or discrepancies

The investor may be lured by a broker or other intermediaries to put money in stocks with supposedly attractive returns. These intermediaries may collude with sham companies and cause a discrepancy in dividend payments to investors.

Some examples:

- Diversion of dividend payments to dummy customers
- Incorrect intimation of record date, dividend percentage and ex-dividend NAV by the AMC—excess or short pay-
- Dividend pay-out files not being or short pay-outs to investors



Regulatory and legislative landscape

On how to stay afloat in the sea of regulatory changes

Regulations and laws governing the financial services sector in India are continuously evolving. For any growing organisation, it is critical to keep up with the changing laws in order to mitigate risk and stay ahead.

By taking short-term steps to adapt to the regulatory amendments, we can avoid long-term consequences impacting the business future of a financial institution.

Banking

The RBI issued a master circular on 'Frauds – Classification and Reporting'. The circular has fixed the responsibility of preventing frauds on banks, exposing them to a completely new horizon of financial risks. Further, banks are now required to report to the RBI the "complete information about frauds and the follow-up action taken thereon".

With the shift from traditional ways of responding to frauds to new ways of robust reporting and risk monitoring systems, banks can now control financial and reputational risks more efficiently.

Mobile banking

With the rapid growth in users and wider coverage of mobile phone networks, mobile banking is increasingly coming up as a significant delivery channel for extending banking services to customers. Putting the onus on banks, the RBI has issued operative guidelines to regulate this channel, suggesting reporting of suspicious transactions to its financial intelligence unit.

Owing to the heavy reliance on telecom operators for its services, the prevention and detection of frauds in mobile banking have become even more complex.

To keep a check on frauds, banks need to incorporate a greater level of scrutiny, by deploying advanced tools and technology capable of protecting the customers against unethical activities.

Insurance

The Insurance Regulatory and Development Authority (IRDA) has issued an Insurance Fraud Monitoring Framework (IFMF) in order to guide the implementation of measures to minimise the vulnerability against frauds in the insurance sector.

IFMF mandates for the insurance companies to set up a risk management committee, followed by disclosure of adequacy of the systems in place to safeguard against frauds. In order to reduce the exposure, the IRDA has mandated that insurance companies have fraud risk management systems for reinsurers. Proficiently designed processes, continuous monitoring and management of fraud risk will go a long way in keeping a check. In addition to this, a well-established fraud risk management system will answer key questions related to complicated threats.

NBFCs

The NBFC sector has evolved considerably in terms of its size, operations, technological sophistication, as well as entry into newer areas of financial services and products. NBFCs are now deeply interconnected with entities in the financial sector, on both sides of their balance sheets. Being financial entities, they are as exposed to these risks as banks.

Acknowledging the risk factors applicable to NBFCs, the RBI has issued a master circular on reporting of frauds. The circular lays down a road map similar to the one for banks. Akin to the banking sector, the circular has fixed the responsibility of preventing frauds on NBFCs, subjecting them to uncertain financial risks. The RBI has further mandated the reporting of frauds by NBFCs in a prescribed format. This is expected to pose certain challenges to NBFCs and may require many to re-visit their business model. These regulations call for NBFCs to invest in upgrading their systems and processes and equip them with advanced tools to prevent as well as detect frauds in parlance with the emerging threats by way of technology.



Key regulatory drivers for the financial services sector

Regulator or law	Salient features
Reserve Bank of India Act, 1934 ²¹	 Is aimed at advising banks about fraud prone processes and the safeguards necessary for prevention of fraud Has made fraud reporting a mandatory process Mandates all banks to file suspected transaction reports Instructs them to follow KYC, AML and CFT guidelines Issues guidelines for the classification and reporting of frauds
Securities and Exchange Board of India Act, 1992 ²²	 Protects the interests of investors from fraudulent activities of corporates Empowers the regulatory authority to appoint an investigating authority to conduct investigations
Companies Act, 2013	 Empowers the Serious Fraud Investigation Office (SFIO) with powers to probe companies suspected of fraud According to the act, the SFIO's report filed in a court for framing charges is to be equivalent to a police report under the Code of Criminal Procedure, 1973 Authorises the auditor to act as a whistleblower and report fraud to the central government, audit committee or the board, depending on the quantum of fraud (as prescribed) Places the primary responsibility for prevention and detection of fraud on the company's board of directors and management
Insurance Regulatory and Development Authority Act, 1999 ²³	 Protects the interests of policy holders and secures fair treatment for them Prescribes the IFMF to address and manage fraud risks According to this act, all insurance companies are required to have in place an anti-fraud policy, duly approved by their respective boards
Pension Fund Regulatory and Development Authority Act, 2013	 Directs an investigation into the affairs of intermediaries or persons associated with the pension fund Entrusts the Central Recordkeeping Agency (CRA) or the annuity service provider with managing the withdrawals from the national pension
Forward Contracts (Regulation) Act, 1952	 Makes provisions for investigation, enforcement and penalty in case of contravention of the provisions of the act
Prevention of Money Laundering Act, 2002	 Prevents money laundering and provides for the confiscation of property derived from, or involved in, money laundering and for related matters Requires banks and other specified institutions to maintain a record of clients and transactions, and furnish them to the prescribed authority; this record needs to include full-fledged money changers, money transfer service providers, and casinos under its reporting regime
The Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015 ^{24 25}	 Deals with the problem of black money (undisclosed foreign income and assets) Penalises the concealment of foreign income and makes attempting to evade tax in relation to foreign income a criminal liability Specifies the applicable tax rates or assets, scope of income to be taxed, tax authorities, penalty and prosecution in relation to undisclosed foreign income and assets
The Benami Transactions (Prohibitions) Amendment Bill, 2015 (to be passed)	 Defines a "benami transaction" as a transaction where a property is held by or transferred to a person, but has been provided for or paid by another person Seeks to amend the Benami Transactions Act, 1988 Aims to: Broaden the horizon of the existing Establish adjudicating authorities and an appellate tribunal to deal with such transactions Specify the penalty for entering into benami transactions
National Bank for Agriculture and Rural Development Act, 1981 ²⁶	Authorises banks to frame an internal policy for fraud risk management and fraud investigation
Small Industries Development Bank of India Act, 1989	 Instructs to form an audit committee in terms of RBI guidelines for reviewing cases of fraud and action taken thereon
National Housing Bank Act, 1987 ²⁷	 Issues guidelines on causes and remedial action in terms of incidence of frauds in housing finance Shares the modus operandi and causative factors of housing finance frauds (The Fraud Management Cell has been collecting such information from housing finance companies, the RBI, IBA, etc, and circulating the same to HFCs to enable them to take adequate precautions, exercise due diligence and initiate timely corrective actions to avoid such fraudulent incidences in future).

^{21.} Master Circular on 'Frauds – Classification and Reporting' DBS.CO.CFMC.BC.No.1/ 23.04.001/2014-15. Circular on 'Risks and Controls in Computers and Telecommunications' DPSS.CO.PD.No.1017/02.23.001/2014-2015

^{22.} Circular on Fraud Classification and Reporting for NBFC DNBS (PD).CC. No. 315 /03.10.42 /2012-13 SEBI (Prohibition of fraudulent and unfair trade practices relating to securities market) Regulations 2003

^{23.} Circular on Insurance Fraud Monitoring Framework IRDA/SDD/MISC/CIR/009/01/2013

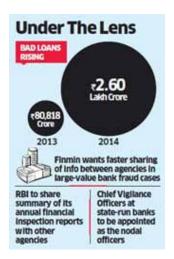
^{24.} http://www.prsindia.org/billtrack/industry-commerce-finance/

^{25.} http://www.prsindia.org/uploads/media/Black%20Money/Black%20money%20act,%202015.pdf

^{26. (}Ref.No.NB.DoS.HO.POL.CFMC/ 3662 /P. 78/2009-10 dated 10 November 2009. Circular No. 189 /DoS. 40 /2009)

^{27.} NHB(ND)/HFC/BP&P/2966/2005

Global trends in fraud prevention and detection



Source: Economic Times ET (Aug 8, 2015): CBI keen to be lead investigator of big ticket corporate loan default cases.

Current scenario

Financial institutions are enhancing their processes, controls and fraud risk management frameworks to minimise the opportunities for fraud as well as reduce the time taken in their detection. Funding for fraud control initiatives, however, continues to compete with other business initiatives and is mostly challenged on a cost–benefit basis.

Many financial institutions are thus implementing their fraud control and reporting frameworks to generate information in a way that the level of fraud identified, prevented and actual losses incurred are identified. This approach has enabled the benefits of skilled resources and automated tools to be quantified more precisely.

The role of regulators

Regulators and investigative agencies are trying to gear up for the changed environment. In 2012, the Central Bureau of Investigation (CBI) announced that it is developing a Bank Case Information System (BCIS) to curb banking frauds. This database contains the names of accused persons, borrowers and public servants compiled from the past records.

The RBI has released a new framework to check loan frauds by way of early warning signals for banks and red flagging of accounts where defaulters shall have no access to further banking finance. It also plans to set up a Central Fraud Registry that can be accessed by all Indian banks. In addition, the CBI and Central Economic Intelligence Bureau (CEIB) will share their databases with banks.

Similarly, the IRDA is also in the process of setting up an insurance fraud repository in order to reduce monitoring costs, using advanced detection and prevention systems deployed at the industry level. The initiative is expected to identify fraudulent claims right at the processing stage, before the payment occurs, and is aimed to ensure better screening of proposals at the underwriting stage. This project aims at establishing an industrywide single fraud database that will eliminate the need for individual insurers to do the same, and targets to ensure better flow of information among the insurers

SEBI is in the process of getting its existing business intelligence gathering software, which is used for detecting fraudulent activities in capital markets, upgraded.

Industry-wide trends

Whilst the legal environment and regulators have pushed the financial sector in the right direction, individual institutions are also taking the lead in protecting their earnings and reputation.



% FS respondents

Source: PwC Global Economic Crime Survey 2014

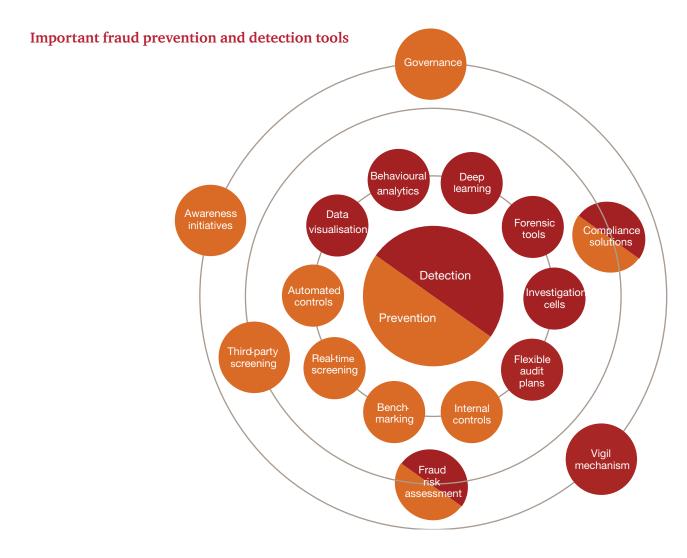
PwC's Global Economic Crime Survey 2014: Financial Services Sector Analysis identified that suspicious transaction reporting, effective fraud risk management measures, whistleblowing processes and tip-offs helped financial services organisations to detect most frauds.

Top trends

- Automated analysis tools: Today, the industry is increasingly aware of the need for automated analysis tools that identify and report fraud attempts in a timely manner. Solution providers are providing real-time transaction screening, third-party screening as well as compliance solutions.
- Sector-oriented benchmarking solutions: Solutions aimed at assessing the fraud vulnerability of financial institutions are now available. They help in formulating a targeted and cost-effective action plan against fraud risks.
- Data visualisation tools: These are being used to provide a visual representation of complex data patterns and outliers to translate multidimensional data into meaningful pictures or graphics.

- **Behavioural analytics:** This is helping businesses identify enemies disguised as customers. The data analytics implemented by the institutions to understand customer behaviour, preferences, etc are also helping in the detection of fraudulent activity either in real-time or post mortem.
- **Deep learning:** Internet payment companies providing alternatives to traditional money transfer methods are using deep learning, a new approach to machine learning and artificial intelligence that is good at identifying complex patterns and characteristics of cybercrime and online fraud.
- The internal audit function: This function is being altered to include fraud risk management in its scope. The changed technological landscape requires the old ways of internal auditing to give way to new, technologically equipped audit functions. Annual audit planning may no longer be fully effective and flexible audit plans are the need of the hour, as fraud risk assessments require extensive use of forensic and data analytics solutions.





Back to basics

Hiring reliable management and building relationships with genuine clients, suppliers and partners are of utmost importance. The lack of correct background information can lead to both reputation and business risks. Effective background checks of employees and associates are thus recommended.

It is difficult but also necessary to integrate data from various sources to be able to derive the benefits of analytics techniques. Financial institutions do face challenges in maintaining the efficiency of anti-fraud security controls at an enterprise-wide level. Challenges arise while integrating channels or within applications and tools (integrating online and ATM transactions,

retail banking and corporate banking or integrating subsidiary banks where different information systems are used).

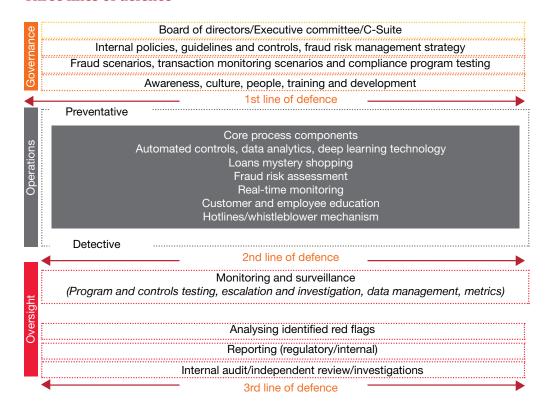
The three lines of defence can only be strengthened by technology and not replaced by it. The tone at the top is critical in the fight against fraud. Lack of customer and/or staff awareness can result in failure of even the best of technology solutions. It takes a concerted effort to be able to build, maintain and sustain an effective fraud risk management programme.

Organisations need to build awareness around the latest technological and procedural vulnerabilities and fraud schemes, to be able to remain one step ahead of the fraudsters.

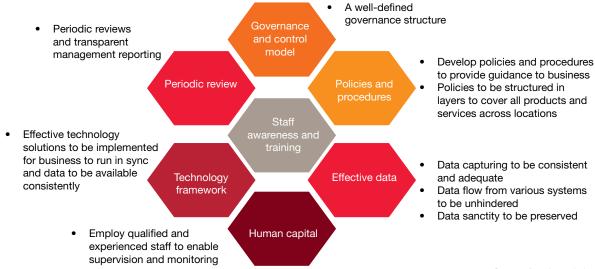
In addition, incident management procedures need to be well defined and comprehensive, in order to ensure that incidents of fraud are managed without exposing the organisation to any legal or reputational risks. Forensic tools can be used to navigate IT systems for evidence of malfeasance such as information deletion, policy violations and unauthorised access. These tools can help the company legal counsels to prepare for a suit to be filed against the fraudster.

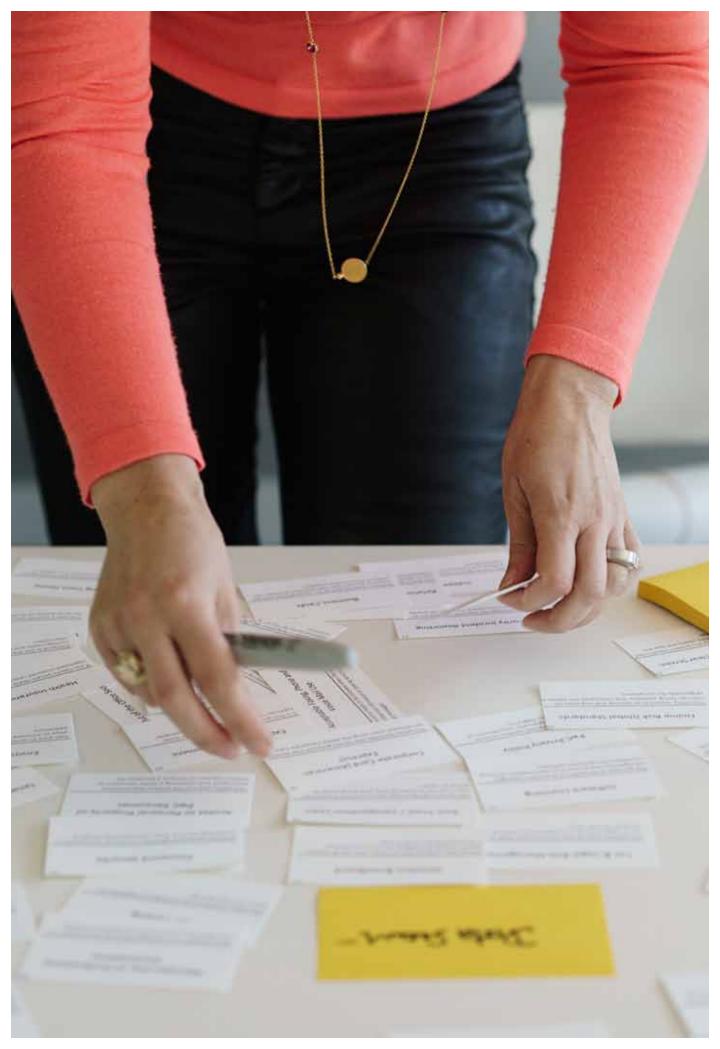
Apart from internal controls, financial institutions need to also educate the customers. Since the manoeuvres used by cyber-criminals to target sensitive financial data are sophisticated and constantly changing, financial institutions must look at existing security controls with a new approach and risk appetite.

Three lines of defence

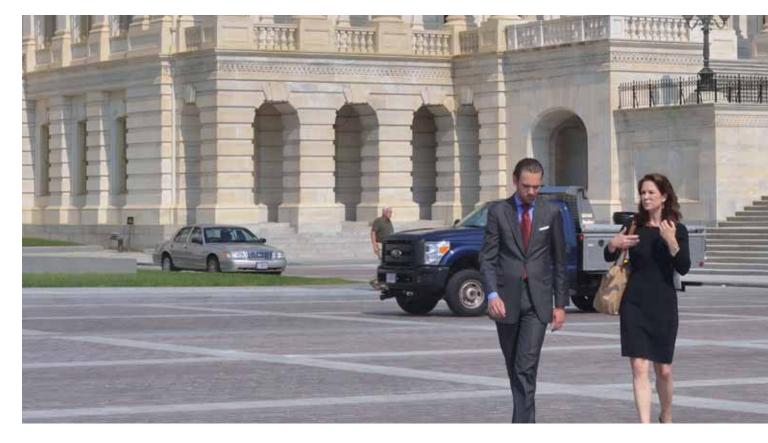


Key components of an effective anti-fraud programme





Notes



About ASSOCHAM

The knowledge Architect of Corporate India

The Associated Chambers of Commerce and Industry of India (ASSOCHAM), India's premier apex chamber, covers a membership of over 4 lakh companies and professionals across the country. ASSOCHAM is one of the oldest Chambers of Commerce which started in 1920. ASSOCHAM is known as the "knowledge chamber" for its ability to gather and disseminate knowledge. Its vision is to empower industry with knowledge so that they become strong and powerful global competitors with world class management, technology and quality standards.

ASSOCHAM is also a "pillar of democracy" as it reflects diverse views and sometimes opposing ideas in industry groups. This important facet puts us ahead of countries like China and will strengthen our foundations of a democratic debate and better solutions for the future. ASSOCHAM is also the "voice of industry" – it reflects the "pain" of industry as well as its "success" to the government. The chamber is a "change agent" that helps to create the environment for positive and constructive policy changes and solutions by the government for the progress of India.

As an apex industry body, ASSOCHAM represents the interests of industry and trade, interfaces with the government on policy issues and interacts with counterpart international organisations to promote bilateral economic issues. ASSOCHAM is represented on all national and local bodies and is, thus, able to pro-actively convey industry viewpoints, as also communicate and debate issues relating to public-private partnerships for economic development.

The road is long. It has many hills and valleys—yet the vision before us of a new resurgent India is strong and powerful. The light of knowledge and banishment of ignorance and poverty beckons each member of the chamber to serve the nation and make a difference.

Contacts

The Associated Chambers of Commerce and Industry of India (ASSOCHAM)

5 Sardar Patel Marg, Chankyapuri, New Delhi – 110021 Tel: +91-11-46550555 Fax: +91-11-23017008/9 Website: www.assocham.org

Southern Regional Office D-13, D-14, D Block, Brigade MM,

1st Floor, 7th Block, Jayanagar, K R Road, Bangalore – 560070 Telephone: +91-80-40943251-53 Fax: +91-80-41256629

E-mail: events.south@assocham.com, events@assocham.com, director.south@assocham.com

ASSOCHAM Western Regional Office

4th Floor, Heritage Tower, Bh. Visnagar Bank, Ashram Road, Usmanpura, Ahmedabad-380 014 Tel: + 91-79- 2754 1728 / 29, 2754 1867

Fax: + 91-79-30006352

Email: assocham.ahd1@assocham.com assocham.ahd2@assocham.com

Eastern Regional Office

F 4, "Maurya Centre" 48, Gariahat Road Kolkata-700019

Telephone: 91-33-4005 3845/41 Fax: +91-33-4000 1149

E-mail: kolkata@assocham.com

ASSOCHAM Regional Office Ranchi

503/D, Mandir Marg-C

Ashok Nagar Ranchi-834 002

Email: Head.RORanchi@assocham.com

Phone: +91-9835040255



About PwC

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 184,000 people who are committed to delivering quality in Assurance, Tax and Advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bangalore, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

You can connect with us on:

You can connect with us on:

facebook.com/PwCIndia

twitter.com/PwC_IN

in linkedin.com/company/pwc-india

youtube.com/pwc

Contacts

Dinesh Anand

Partner and Leader, Forensic Services M: +91 9818267114 Email: dinesh.anand@in.pwc.com

Gaganpreet Singh Puri

Partner, Forensic Services M: +91 9818756955 Email: gagan.puri@in.pwc.com

Dhruv Chawla

Leader, Financial Crime and Compliance M: +91 8130166550

Email: dhruv.chawla@in.pwc.com

Dhritimaan Shukla

Director, Forensic Services M: +91 9899038326

Email: dhritimaan.shukla@in.pwc.com

Data Classification: DC0 This publication does not constitute professional advice. The information in this publication has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this publication represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take. © 2015 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN: U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

AK 385 - June 2015 Current fraud trends in the financial sector .indd

Designed by: PwC Corporate Communications, India