

**Deloitte.**



## Protecting your business in the Banking sector

For Private use only

# Forensic

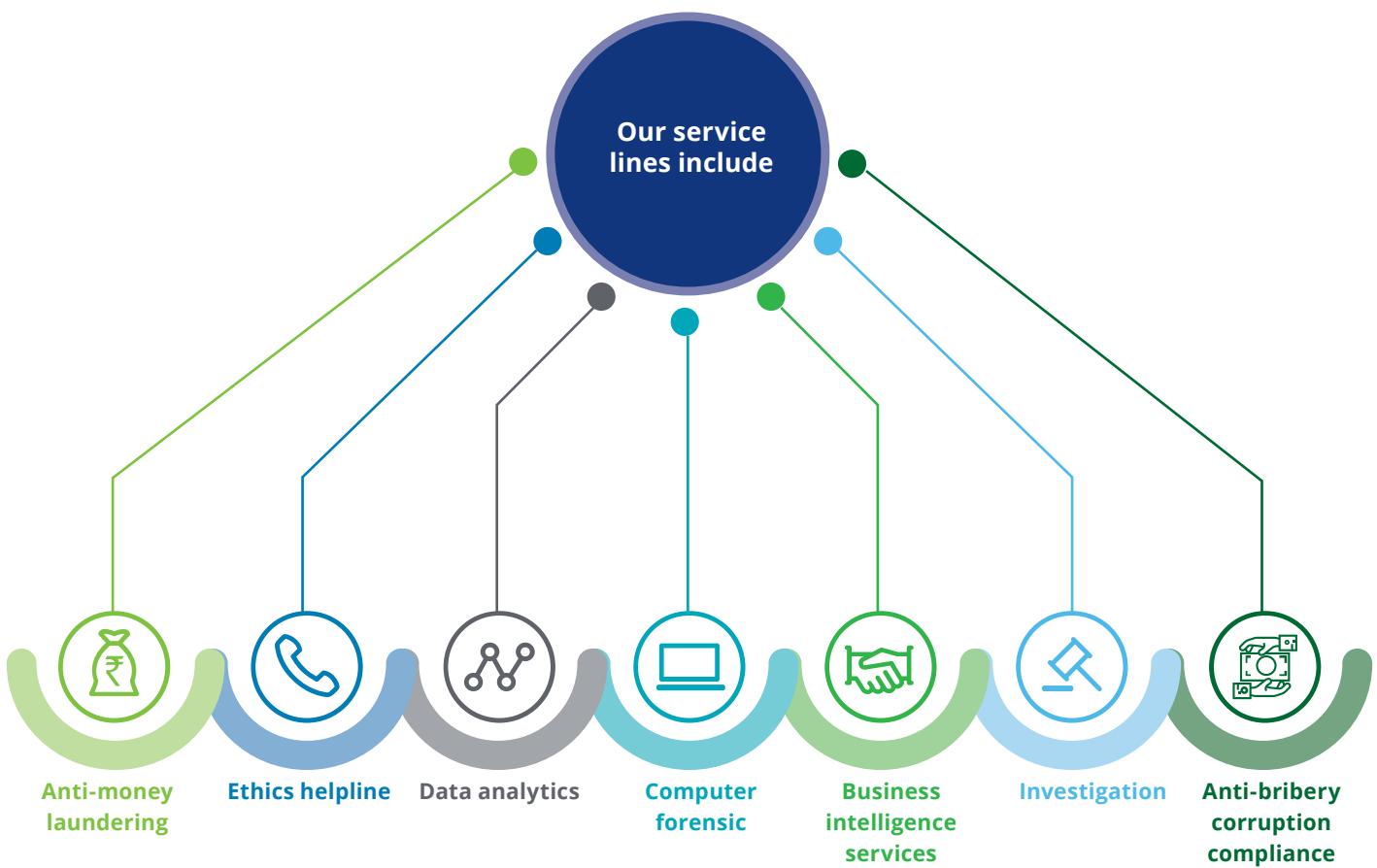
Banks are facing an increasingly difficult scenario with increased fraud incidents and low recoveries compounded by a tidal wave of compliance regulations in India and abroad, thereby directly affecting their bottom-line and increased cost of compliance. With increased regulatory scrutiny, banks are under greater pressure to implement best practices. Compliance is therefore not an option but the need of the hour.



**Source:** India Banking Fraud Survey, Edition II (2015)



# How can we help?





## Fraud risk management

In the wake of increasing incidents of frauds in the financial service sector, the Reserve Bank of India (RBI) introduced guidelines vide circulars for a comprehensive Fraud Risk Management (FRM) system for banks pertaining to fraud prevention and the management's function in the organization to prevent fraud.

### Key questions banks should look into:

- Who is responsible for the organization's fraud risk management programme?
- Which products are most vulnerable to fraud?
- Which processes are most vulnerable to fraud?
- What is the number of fraud incidents encountered by the organization in the last few years? Has it increased?
- What steps are being undertaken to improve fraud controls based on the root cause analysis of fraud incidents?
- How many processes are outsourced and what controls are in place to mitigate the outsourcing risk?
- Does the organization have capabilities to identify "Red Flags" proactively?
- Does a formal incident response mechanism and process exist for responding to fraud?



## Anti-money laundering

Negative publicity, damage to corporate reputation and loss of goodwill, legal and regulatory sanctions and adverse effect on the bottom line – are all possible consequences of an organization's failure to manage the risk of money laundering.

### Key questions you should ask:

- What is the money laundering risk in each jurisdiction where you operate? Are your policies and procedures robust enough to mitigate these risks?
- What is your money laundering risk profile? Are your policies and systems benchmarked to leading industry practices?
- Is your AML programme fully implemented in practice and supported by the corporate culture?
- How well do you know your customers? Are you acquiring clients, agents or business partners that may be involved in facilitating money laundering?



## Ethics Helpline

An important aspect to encourage accountability and transparency within an organization is a mechanism to enable all individuals to voice concerns internally in a responsible and effective manner when they discover information which they believe shows serious malpractice.

Implementing an employee whistleblowing hotline gives your employees a voice to confidentially report workplace concerns

and enables you to identify and rectify problems before they damage your business and its reputation.

Deloitte Tip-offs Anonymous can act as a deterrent for unethical behavior that could lead to losses. It is also proved to be one of the most effective ways to detect fraud according to the Association of Certified Fraud Examiners (ACFE). Additionally, the presence of a whistleblowing helpline can boost staff morale by encouraging values such as trust, integrity and openness.



## Data analytics

With banks facing heightened regulatory and public scrutiny in many countries, using advanced analytics to help identify potential wrongdoing sooner may be a strategic and operational imperative.

### Key questions you should ask:

- Are you confident that your AML monitoring system has not missed transactions that should have featured in your STR?
- Do you have visibility to potentially suspicious customer behavior manifesting across different banking products and spread over 18 – 24 months?
- Are you certain that your de-dupe and UCIC program is identifying all potentially related parties?
- Do you know which of your customers defaulting on their loan payment is potentially fraudulent?
- Are you aware of hidden/ un-disclose relationships between your suppliers and employees?
- Do you think there are ghost employees on your payroll?
- Do you have an early warning preventive system that is able to identify potential fraudulent outliers or raise 'red flags'?



## Computer Forensic

Today's business environment generates vast amounts of data and information. However, hundreds of billions of dollars are lost every year due to fraud, financial mismanagement or other malfeasance such as information deletion, policy violations or unauthorized access, etc. Evidences mostly lie concealed in different digital media, in the form of active, deleted, hidden, lost or encrypted files, file fragments etc. Commercial investigations and litigations increasingly rely on this data to help tell the whole story. The key to managing such huge volumes is turning the array of data into meaningful information.

### We:

- Understand applicable legal requirements and policies
- Secure and collect evidence in a manner consistent with rules of admissibility
- Analyze the evidence with trusted and validated tools
- Present the evidence in an understandable manner



## Business intelligence services

Investment banks seeking to raise capital for their clients, either through public or private offerings, or advising clients on potential transactions, or a private equity investor investing in a company generally need an objective picture and understanding of the backgrounds of the parties involved. Such information can assist in mitigating reputational, legal, or commercial risks in the context of contemplated transactions. Just as strict anti-money laundering regulations have made it essential for financial institutions to practice "know your customer" due diligence, the need to "know your vendor" plays a similar role in mitigating fraud and regulatory risk for businesses.

### Key questions you should ask:

- Do we have the complete information about the prospective enterprise/ key decision makers?
- Has the fraud been examined from all possible angles and have we gone to the depth of the problem?
- Do we have complete knowledge of the fraudster, his businesses, assets and other interests?
- Are the subject parties involved in criminal activities or have links to organized crime?
- Do you have visibility on all your assets/ funds and their utilization/ ownership?



## Anti-bribery and corruption compliance

The upward trend in regulatory anti-corruption initiatives globally has meant that Indian financial institutions need to ensure their compliance programmes are robust and tested. This will help to minimize chances of prosecution and significant fines not only under Indian laws, but also under the more stringent global regulations like U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act (UKBA).

### Key questions you should ask:

- Have you performed a corruption risk analysis of your operations to identify potential high risk areas?
- Do you have an anti-bribery and corruption policy? Is your staff aware of anti-corruption measures?
- Does your staff receive regular, appropriate and specific anti-corruption training?
- Do you conduct sufficient, effective due diligence when entering into relationships with third parties?



## Investigation

Some of the common fraud incidents in retail and priority sector banking include incorrect sanctioning, multiple funding, over valuation of collateral and fraudulent documentation. Similarly siphoning of funds and external vendor induced frauds are prevalent in the corporate banking environment. In addition to this, the introduction of technology for internet and mobile banking are leading to newer types of frauds like phishing,

account takeover, hacking and cloning. Any response to fraud therefore, should be swift and effective. The RBI circular dated September 2009 required banks to investigate 'large value frauds' with the help of skilled manpower for internal punitive action against the staff and external legal prosecution of the fraudsters and their abettors.

# Our approach

Our approach and methodology has been developed based on numerous projects carried out in the financial services industry in India and across the world. Our approach is custom designed for each client to assist them in demystifying the issue, identifying the perpetrators and the root cause, tracing the assets as well as to help enhance their existing controls to prevent the occurrence of similar incidents in the future.

# Contact us

To know more, reach out to:

**Nikhil Bedi**

Partner, Leader, Forensic  
Deloitte India  
T: +91 22 6185 5130  
E: [nikhilbedi@deloitte.com](mailto:nikhilbedi@deloitte.com)

**KV Karthik**

Partner, Forensic  
Deloitte India  
T: +91 22 6185 5212  
E: [kvkarthik@deloitte.com](mailto:kvkarthik@deloitte.com)

# Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.