



ECONOMIC
LAWS
PRACTICE
ADVOCATES & SOLICITORS



e - Frauds

ABOUT US

Set up in 2001 with the aim of bringing together a diverse set of professionals to deliver effective solutions for clients, Economic Laws Practice (ELP) is today a leading full-service law firm in India with 200+ professionals – lawyers, chartered accountants, cost accountants, company secretaries, sector experts and economists – assisting clients on transactional, advisory, litigation, regulatory, and tax matters.

OUR JOURNEY

- 2001** Start of our journey in Mumbai
5 professionals
- 2003** New Delhi office is set up
17 professionals
- 2007** Office opens in Ahmedabad
36 professionals
- 2008** Office opens in Pune
52 professionals
- 2013** Bangalore and Chennai offices open
ELP crosses the 100 mark and is home to 108 professionals
- 2015** Ranked in top-10 Indian law firms
156 professionals
- 2018** India -based member firm for Taxand network
- 2019** 6 offices pan-India
200+ professionals
Full-service offering with 14 practice groups & sector-focused teams

Setting the Context

- The internet, internet of things, artificial intelligence, big data and several new inventions have altered the way the world economically engages. Machine to machine communication, sensor technology, robotics, machine learning and cloud computing now form the very backbone of doing business.
- With data and information being key drivers of the economy, the paradigm of doing business has transformed. Not surprisingly, therefore, theft and frauds have increasingly started focusing on digital wealth and identity. Consequently, investigating crimes and frauds in the digital age have completely transformed.
- Going forward, digital forensics will increasingly play a crucial role in both law as well as in conducting business. The objective of digital forensics is to identify risks and preserve evidence while performing a structured investigation by collecting, identifying and validating digital information, for the purpose of reconstructing past events.
- The pace at which digitalization has exponentially grown, digital forensics are now sector and industry agnostic.

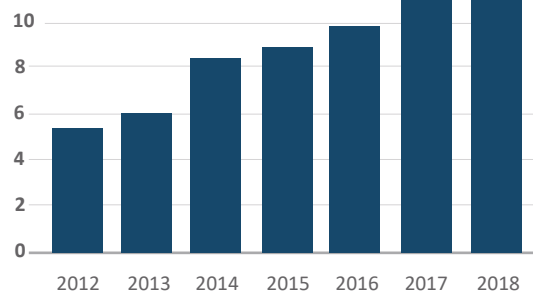
Investigations

- The rudimentary practices followed by local law enforcement and limited knowledge of emerging forensic technology have led to weak capabilities in investigating corporate crimes and bringing criminals to the fore.
- Mandatory risk assessment by a plethora of regulatory bodies and increasing accountability now being assigned to KMPs and Boards is an emerging concern.
- Various global legislations – such as US Foreign Corrupt Practices Act and UK Bribery Act – now require a mandatory investigation of fraud.
- Bribery and corruption infractions by suppliers or agents in other countries (like India) can also lead to liability on the company and its management, further underlining the need for robust internal prevention/detection structures as well as regular audits.
- Increasingly, most investigation agencies first seek and quarantine electronic footprint and records irrespective of the nature of crime – civil, economic or physical.
- The need for specialized integrated resources to help understand and manage incidents – from initial investigation all the way through the litigation process – is paramount.

LEVERAGING DIGITAL FORENSICS TO TACKLE FRAUD ACROSS THE BUSINESS LIFECYCLE

The average cost of a data breach in India rose nearly 8% Y-O-Y to INR 12 crore

The cost of a data breach in India has been on the rise
Average total cost
Rs12 crore



ATLAS Data : IBM Security and Ponemon Institute

- Between April 2017 and January 2018, over 22,000 Indian websites, including 114 government portals were hacked
- The Aadhaar database suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens (WEF report)
- Personal Information of more than 49 million Instagram users exposed after a social media marketing company left the data unprotected on an Amazon Web Services database
- Over 540 million records of Facebook users exposed
- Marriott International has been fined almost Euro 100 million over a major cyber attack which exposed personal data of 339 million guests
- In November 2018, tax reports of approximately 400,000 Amazon sellers were disclosed to other sellers due to malware
- Federation of Hotel and Restaurant Associations of India issued a notice to OYO India adducing a large number of data breaches
- WhatsApp experienced a security flaw that left people vulnerable to spyware
- In the aftermath of the crisis, the IL&FS board has initiated digital forensic investigations

Fraud, in the modern context, can manifest across different stages of business lifecycle encompassing operational, financial and regulatory aspects. In each of these instances, digital forensics – a set of tools that can help companies prevent and detect instances of fraud, which can then guide the formation of optimal response and containment strategies – can assist with the following:

Operational

- Compliance audits including Directors' liabilities
- Preventing/handling the aftermath of cyber attacks
- Investigating employees for violations of company policies/fraudulent actions
- Sexual harassment/defamation and harassment cases
- Accident investigations
- Assistance in data recovery
- Impact assessment of fraud
- Business continuity readiness

Financial

- Due diligence in M&A transactions/investments/exits
- Detecting economic espionage
- Money laundering
- Corporate fraud
- Insider trading

Regulatory

- Data theft and IP infringement
- Cartelization and competition law related investigations
- Breach of contract investigations
- Data protection and data theft
- Fraud related investigations

HOW WE CAN HELP

While there are different nuances to different types of fraud, generally speaking, most fraud incidents will have planning, launching and encashment as three constituent stages. ELP helps provide effective systems and protocols for all stages, including damage containment to create a robust fraud prevention and protection framework. These activities can be divided into four phases:

Prevention

Limit the opportunity to commit fraud through:

- Access restrictions
- Internal control systems (SOPs, access protocols, continuing recon)
- Training to sensitize users
- Threat of adverse consequences
- Signed code of ethics from employees

Detection

Continually identify and monitor key fraud indicators (such as weakening internal controls, inadequate processes) through:

- Regular audits and risk assessment
- Whistleblower reporting, protection (and reward) programs

Response

- Detailed evidence gathering, protection and preservation procedures
- Analyzing evidence to
 - assess liability
 - maintain admissibility
 - ensuring that investigation into the alleged incident is within legally permissible margins
- Thorough (independent/external) investigation
- Case preparation
- Asset recovery proceedings and/or litigation/complaints
- Asset recovery proceedings, damage assessments and/or litigation/complaints
- External reporting

Containment

- Building a crisis management team comprising of HR, Legal, IT and communication experts
- Managing adverse publicity and reputation damage to the business/brand
- Informed decision making and legal review of proposed organizational response

INVESTIGATIONS

Digital forensic investigations are still predominantly conducted in response to an incident. With this reactive approach, there is extreme pressure put on the investigation team to gather and process digital evidence before it is no longer available or has been modified. The rudimentary practices followed by local law enforcement and limited knowledge of emerging forensic technology have led to weak capabilities in investigating corporate crimes. The need for specialized resources to help manage incidents – from initial investigation all the way through the litigation process – is paramount.

HOW CAN WE HELP?

- An integrated approach combining proven expertise in investigations, legal strategy and enforcement
- An experienced cross-sectoral team of forensics specialists, retired law enforcement officials and IT experts
- Discretionary approach to investigations
- Customizing investigation techniques and technologies on a case by case basis
- Ensuring that the evidence gathering procedure is admissible in court



**ECONOMIC
LAWS
PRACTICE**
ADVOCATES & SOLICITORS

MUMBAI

9th Floor, Mafatlal Centre
Vidhan Bhavan Marg
Nariman Point, Mumbai 400 021
T: +91 22 6636 7000

NEW DELHI

801 A, 8th Floor, Connectus Tower, Bhavbhuti Marg
Opp. Ajmeri Gate Railway Station, Nr. Minto Bridge
New Delhi 110 001
T: +91 11 4152 8400

AHMEDABAD

801, 8th Floor, Abhijeet III
Mithakali Six Road, Ellisbridge
Ahmedabad 380 006
T: +91 79 6605 4480/8

PUNE

202, 2nd Floor, Vascon Eco Tower
Baner Pashan Road
Pune 411 045
T: +91 20 4912 7400

BENGALURU

6th Floor, Rockline Centre
54, Richmond Road
Bengaluru 560 025
T: +91 80 4168 5530/1

CHENNAI

No 18, BBC Homes, Flat-7 Block A
South Boag Road
Chennai 600 017
T: +91 44 4210 4863



elplaw.in



insights@elp-in.com



[/elplaw.in](https://www.facebook.com/elplaw.in)



[/ELPIndia](https://twitter.com/ELPIndia)



[/company/economic-law-practice](https://www.linkedin.com/company/economic-law-practice)

DISCLAIMER:

The information contained in this document is intended for informational purposes only and does not constitute legal opinion or advice. This document is not intended to address the circumstances of any particular individual or corporate body. Readers should not act on the information provided herein without appropriate professional advice after a thorough examination of the facts and circumstances of a particular situation. There can be no assurance that the judicial/quasi judicial authorities may not take a position contrary to the views mentioned herein.

© Economic Laws Practice 2020