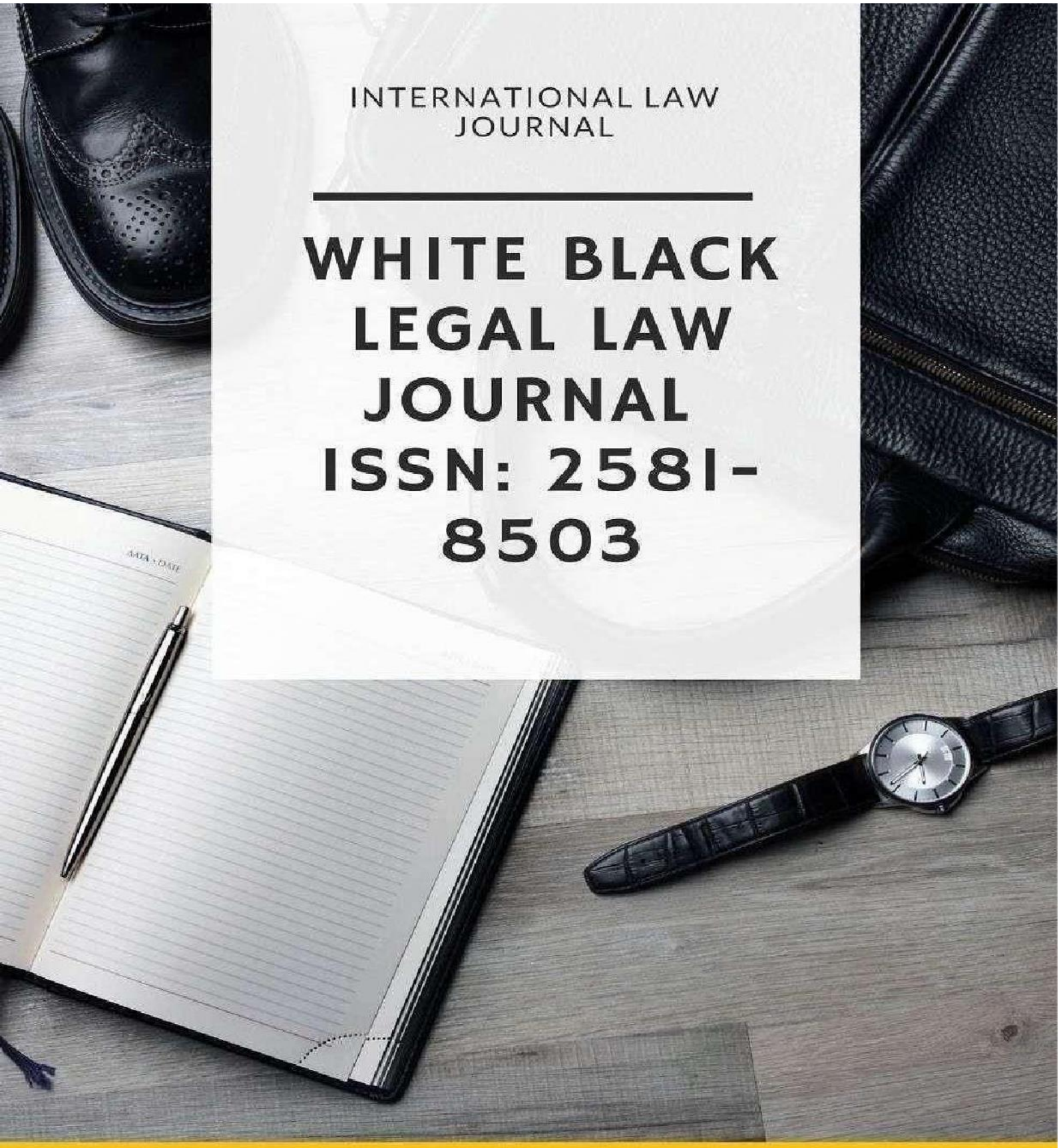


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

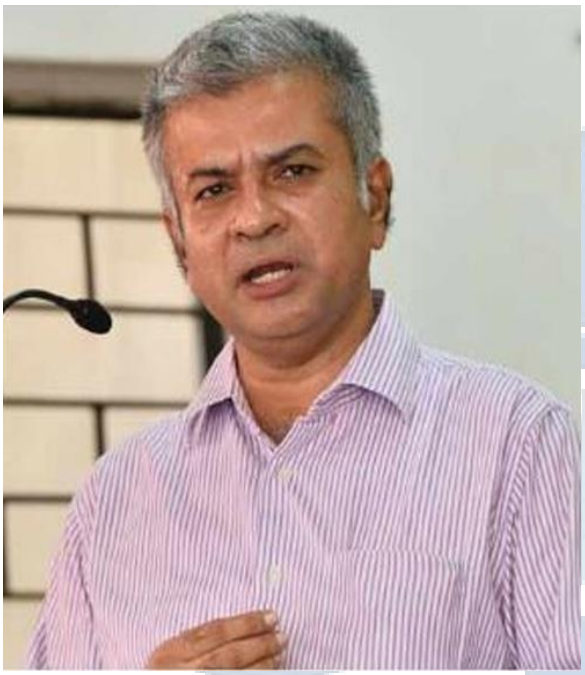
The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

 ISSN: 2581-8503

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | Feb 2025 ISSN: 2581-8503

"CORPORATE FRAUDS AND WHITE COLLER CRIMES IN INDIA"

AUTHORED BY - MS. SIMRAN RAKESH PARDESHI
LL.M. 1st, Sem-I, Roll No. 36
DES Shri. Navalmal Firodia Law College, Pune

Abstract

When trust is breached, we all foot the bill, with fraudsters as the collectors. The phrase, white collar crime introduced by American criminologist Edwin Sutherland in 1939, highlighted the distinctive clothing often worn by those responsible for these acts, who were typically individuals in the business world, top-level professionals, and politicians. Currently white-collar crimes encompass offenses like bank fraud, tax evasion, embezzlement, bribery, and money laundering which are governed by the Indian Penal Code, 1860, Income Tax Act, 1961, Prevention of Corruption Act 1988 , The Prevention of Money Laundering Act 2002 The Special Court Act 1992.However, the shifting landscape of white-collar crimes now includes white-collar cybercrimes as well according to Investopedia- White-collar crime is a nonviolent crime often characterized by deceit or concealment to obtain or avoid losing money or property, or to gain a personal or business advantage. EG.of white-collar crimes include securities fraud, embezzlement, corporate fraud, and money laundering. Entities that investigate white-collar crime include the Securities and Exchange Commission (SEC), the National Association of Securities Dealers (NASD), etc. Numerous laws aim to prevent corporate fraud and white-collar crimes, yet these offenses continue to occur. It's crucial to address the loopholes in these laws that allow such crimes to persist. In addition, Cyber fraud and cybercrime are reshaping the white-collar crime and corporate fraud landscape, highlighting the demand for comprehensive legal measures. Laws on white-collar cybercrimes are intricate, constantly changing, and often challenging to understand. Despite numerous laws designed to prevent corporate fraud and white-collar crimes, the authorities still face challenges in effectively addressing the ongoing offences. India's laws against financial fraud need to be strengthened to punish offenders as they currently exploit legal loopholes. The promotion of Digital India has led to a surge in cybercrimes, a type of white-collar crime. India lacks comprehensive cybersecurity laws to effectively address this issue. the researcher has taken this topic to understand changing dynamics of white-collar crimes and corporate frauds.

Key words - white-collar crimes, corporate frauds, Cyber frauds, stringent laws, changing dynamics, challenges.

A. INTRODUCTION

B. What is White-Collar Crime

Edwin Sutherland, a sociologist, and criminologist coined the term "white-collar crime" in 1939. These crimes are not violent, but they are not victimless. White Collar Crimes are the crimes which are committed by the men of high-class society during the course of their business or occupation. White-collar crimes can destroy a company, wipe out a person's life savings, cost investors billions of dollars, and erode the public's trust in institutions.

Examples of White-Collar Crime Health care fraud, Corporate Fraud, Money laundering Securities and Commodities Fraud, mortgage and financial institution fraud, Intellectual Property Theft/Piracy etc.

C. White-collar crimes and corporate fraud

The main differences between white collar and corporate crime are that corporate crime is usually committed by companies or their agents against the public and is generally carried out for the benefit of the company. In contrast, white-collar crime is generally committed against companies and is usually carried out for personal benefit. Corporate crime is a type of white- collar crime.

The Significance of White-Collar Crime in Corporate India: Emerging Trends and Characteristics White-collar crime has a profound impact on corporate India, with contemporary fraudsters primarily driven by greed and a pursuit of financial gain. Several noteworthy trends have surfaced, reflecting the evolving nature of these illicit activities:

a. Decreasing Age of Fraudsters:

The average age of individuals involved in white-collar crimes is on the decline, indicating a concerning shift toward younger perpetrators.

b. Rise in Whistleblower Reports:

Detection of fraud and wrongdoing is increasingly attributed to whistleblowers, highlighting the growing importance of individuals within organizations who expose malpractices.

c. Technology-driven Evasion:

Fraudsters now leverage technology, such as instant messengers and social media networks, as alternative communication channels to evade detection, moving away from traditional methods like emails.

d. Innovative Kickback Mechanisms:

White-collar criminals are adopting innovative methods for kickbacks and favors, demonstrating adaptability and sophistication in their illicit activities.

Corporate fraud involves the commission of illegal and deceptive actions by either a company or an individual. These actions often employ sophisticated accounting techniques with the aim of artificially boosting a company's reported profits. Detecting such fraudulent activities may take years. Misinformation in Prospectus, Manipulation of Accounting Records, Debt Hiding, False Accounting Entries, False Trades for Profit Inflation, Insider Trading, False Transactions to Attract Funding are some examples of corporate fraud.

White-collar crimes typically revolve around the misuse of trust and authority. When corporate executives manipulate prices to eliminate competitors, they are exploiting their positions unethically. Detecting white-collar crimes is often challenging because the losses incurred may not be immediately apparent to the victims. Moreover, these crimes frequently involve intricate schemes and attempts to conceal wrongdoing. Many white-collar crimes necessitate coordinated efforts among individuals involved in the criminal activity. For instance, a real estate fraud case may require the collaboration of an escrow officer, a buyer, an appraiser, and a bank officer—all willing to participate in signing false documents to carry out a fraud for personal gain.

D. Cybercrimes (corporate computer crime)

Corporate computer crimes are not much different from conventional white-collar crimes White-collar crimes have undergone significant changes over time, particularly with the advent of technology. This research illuminates the way in which digital revolution has redefined financial transactions, communication, and data management, consequently impacting the development of patterns in white-collar crime. The most notable transformation occurred with the introduction of the internet. The emergence of the internet has introduced a multitude of intricacies, giving rise to computer crimes or cybercrimes. This convergence has blurred the lines between traditional white-collar crimes and cybercrimes.

Here are some examples; Computer intrusion, Definition, Unauthorized Access, Manipulation of Information, financial Motivation, Personal Motivations, Cybersecurity Threat, Ethical Hacking.

It is important for individuals and organizations to be vigilant about cybersecurity, implementing measures such as strong passwords, regular software updates, and security protocols to minimize the risk of hacking incidents. Additionally, legal and regulatory frameworks are in place to deter and prosecute those involved in hacking activities.

White-collar crimes, therefore, encompass both corporate crime and cybercrime. Recently Finance Minister Nirmala Sitharaman said that to prevent con artists from abusing the system, people must become more conscious of cyber fraud and take control of technology. government regularly examines public sector banks and the regulator RBI checks its own systems in order to prevent cyber frauds, in which victims are tricked via phone or SMS. Insurance firms assess their own systems as well.

This research is focused on comprehending the changing dynamics of white-collar crimes in corporate fraud and digital transformation as cybercrime.

B. SIGNIFICANCE OF RESEARCH

This research is focused on comprehending the changing dynamics of white-collar crimes in corporate fraud and impact of digital transformation. it is highly beneficial for various stakeholders, including law students, lawyers, advocates, law researchers, law makers, and individuals seeking to enhance their knowledge in corporate frauds and frauds related to digital transformation. Here's how it could benefit each group:

Law Students:

a. Provides a valuable resource for academic studies, assignments, and research projects.
b. Offers real-world examples and cases related to corporate fraud and digital transformation, enhancing practical understanding.

Lawyers and Advocates:

a. Serves as a reference point for legal professionals dealing with cases related to corporate fraud and digital crimes.
b. Offers insights into evolving legal challenges in the context of digital transformations and corporate environments.

Law Researchers:

a. Provides a foundation for further research in the field of corporate fraud and digital transformation.
b. Offers a comprehensive overview of existing cases, legal frameworks, and emerging issues.

Law Makers:

a. Offers insights into the complexities of corporate fraud and digital crimes, aiding in the development of effective legislation.
b. Helps in understanding the legal gaps and challenges posed by digital transformation in the corporate sector.

Individuals Enhancing Knowledge in Corporate Frauds and Digital Transformation:

a. Serves as a valuable educational resource for anyone interested in understanding the legal implications of corporate fraud and digital advancements.
b. Provides practical insights and examples that are relevant to the current business landscape.

C. CURRENT LEGAL FRAMEWORKS AND REGULATORY AUTHORITIES

India's legal landscape encompasses several statutes, including the Indian Penal Code of 1860 (IPC) and the Indian Contract Act of 1872, which address a spectrum of offenses related to fraud. However, at the core of regulating corporate conduct in the country is the Companies Act 2013 (CA), serving as the primary legislation governing the corporate sector. The CA specifically outlines the framework for addressing corporate fraud in India, conferring authority upon the Serious Fraud Investigation Office to probe allegations of fraudulent activities involving companies and their officers.

COMPANIES ACT, 2013 DEFINES FRAUD;

Fraud: any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.

Section 36: Punishment for fraudulently inducing persons to invest money. Section 38; Punishment for personation for acquisition, etc., of securities.

Section 229: Penalty for furnishing false statements, mutilation, destruction of documents.
Section 251: Fraudulent application for removal of name.
Section 448: Punishment for false statements.

D. FRAUD REPORTING

Section 143 of the CA mandates internal auditors to report fraud to the central government within the prescribed time frame in certain situations, such as where the fraud involves an amount of at least 10 million rupees. The Ministry of Corporate Affairs, via the Companies (Auditor's Report) Order, 2020 (CARO), introduced stricter financial reporting requirements from 1 April 2021, which entails enhanced due diligence, disclosure requirements for auditors, and greater transparency in financial reporting and whistle-blower complaints.

The CARO now requires the auditor to consider any whistle-blower complaints received by the company during the year under audit. It also requires the auditor to report whether any fraud has been noticed or reported either on the company or by the company during the year and is not limited to frauds carried out by officers or employees of the company (as was the case previously).

Statutory auditors, through the CARO, have also been made subject to disclosure obligations within audit reports, if fraudulent transactions or conduct are observed. However, as per the 'Guidance Note on Reporting on Fraud under Section 143(12) of the Companies Act, 2013' issued by the Institute of Chartered Accountants of India in 2016, these disclosure obligations are only mandatory where the statutory auditor is the first to discover the fraud in question in the course of their duty. As per the Note, the auditor must use professional judgement to assess whether fraud has taken place, as well as review the steps taken by the company's management to report or mitigate the fraud. Furthermore, the Indian government has indicated that it intends to amend the CA to disallow statutory auditors from performing non-audit services for clients.

Under Section 134(5) of the CA, directors are required to disclose measures taken by the company to combat fraud, through a director's responsibility statement. Directors must attest to having taken adequate care for the maintenance of accurate accounting records, to detect fraudulent behavior or any other irregularities. Additionally, in listed companies, directors are required to list the internal financial controls deployed by the company and confirm that these

controls are sufficient and effective in combating fraud and other inconsistencies.

Further obligations on listed companies include a compliance certification, provided by the chief executive officer as well as the chief financial officer to the board of directors. These obligations are set out under the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Rules, which mandates that directors must notify the auditors and audit committees of any fraud in which the perpetrator has significant control over the company's system of financial reporting. Additionally, the listed entity must disclose to stock exchanges any instances of fraud by a promoter or key managerial person (or any arrest in connection with fraud) as soon as reasonably possible within a 24-hour window, along with any information regarding any fraud committed by directors or employees if the fraud is construed as a material event.

FUGITIVE ECONOMIC OFFENDERS ACT, 2018

The corporate world has faced many scams and frauds which affected the economy and society. To curb the fraud, Fugitive Economic Offenders Act, 2018 was enacted. The main objective of the Act is to discourage the fugitive economic offenders from violating the process of law in India by residing outside the jurisdiction of Indian courts to maintain the legal process and rule of law in a regular process.

The Act provides eligibility to declare any individual as a fugitive economic offender by the Special Court and subsequently to attach the property of the offender, disallow civil claims and bar the jurisdiction of the Civil Court. The FEO Act 2018 has the power to confiscate foreign properties with a letter of request to other foreign countries. The Act does not require a search warrant or seizure to investigate the matter or for any necessary investigation.

SECURITIES AND EXCHANGE BOARD OF INDIA (SEBI)

The Securities Exchange Board of India was established under the SEBI Act, 1992 to protect the interest of the investors in securities and to promote the development of and to regulate the securities market. The act aims to avoid the commission of crimes and scams and other manipulations in the securities and capital market in India.

E. ENFORCEMENT AGENCIES

Enforcement agencies play a crucial role in enforcing white-collar crime laws in India, ensuring accountability and maintaining the integrity of the financial system. These agencies, which include the Central Bureau of Investigation (CBI), the Serious Fraud Investigation Office and the Enforcement Directorate (ED), have been empowered with investigative and regulatory powers to combat financial fraud and economic offences.

The ED has been established by the Ministry of Finance to investigate contraventions of the Indian exchange control laws (FEMA) and anti-money laundering regulations. Cases investigated by the ED are adjudicated by adjudicating authorities specifically empowered under FEMA and PMLA as well as designated special courts set up under the Act. Additionally, there is a specialised Appellate Tribunal to hear appeals against orders of the Adjudicating Authorities under PMLA and FEMA.

The SFIO was established to investigate offences under the Companies Act, 2013 ("Companies Act"). SFIO investigations have been given priority, as all investigations by other investigative agencies must await the completion of the SFIO investigation. As part of its investigation, the SFIO can share information related to the commission of an offence with other investigating agencies in order to prosecute the offence outside its purview and is empowered to obtain information from other investigating agencies as part of its investigation. There are designated special courts notified to try cases under the Companies Act.

Their responsibilities encompass a wide range of activities, including conducting investigations, gathering evidence and prosecuting individuals and entities involved in white-collar crimes such as fraud, money laundering, insider trading and corruption. These agencies work in coordination with various stakeholders, including government departments, regulatory bodies and financial institutions, to identify and tackle complex financial offences.

The ED is reportedly developing the Core ED Operations System, a piece of software designed to allow information sharing and shared access between organisations such as the ED, the CBI, the Central Board of Direct Taxes and the Financial Intelligence Unit. Concurrently, the Reserve Bank of India (RBI) launched DAKSH, a web-based end-to-end workflow application to allow for more convenient and efficient fraud reporting mechanisms.

India, being the president of the G20 in 2023, hosted the first meeting of the G20 Anti-Corruption Working Group (ACWG) in February 2023, with Italy as co-chair. A second meeting of the ACWG was held in India in May 2023. The ACWG aims to present a united effort against global economic offenders, strengthening international cooperation and law enforcement with respect to financial crimes, promoting the integrity and effectiveness of public bodies and authorities, and strengthening asset recovery mechanisms.

F. CURRENT LEGAL FRAMEWORK FOR CYBERCRIMES

In India, regulatory and legal responses to digital white-collar crime are outlined in the Information Technology Act, 2000 (IT Act) and the Indian Penal Code (IPC). Key provisions include:

A) Information Technology Act, 2000:

Section 43: Imposes penalties for unauthorized access and damage to computer systems and data.

Section 66: Prescribes punishment for computer-related offenses and unauthorized access. Sections 66C and 66D: Address identity theft and cheating by personation.

Section 66E: Deals with the violation of privacy by capturing and transmitting private images.

B) Indian Penal Code (IPC):

Section 420: Pertains to cheating and inducing property delivery.

Sections 463 and 464: Address the making and possessing of counterfeit electronic records. Sections 468 and 469: Deal with forgery for cheating and its punishment.

Section 47: Addresses the use of a forged document as genuine.

These legal provisions are dynamic and adapt to technological advancements. Law enforcement agencies rely on them to investigate and prosecute digital white-collar criminals, ensuring justice in the digital realm.

I. CHALLENGES AND CONCERNS IN ADDRESSING CORPORATE FRAUD

a. Internal Investigation Capacities in Addressing Fraud and Corruption Challenges in India.

According to *A Survey On White-Collar Crime In India*, conducted by AZB &

PARTNERS published on 11th august 2023[1]

Not surprisingly, according to our respondents, **complex and layered shareholdings in companies and related party transactions are the most susceptible areas of corporate fraud and corruption,** and want statutory auditors to play a more proactive role (and believe further disclosures are required by auditors). Over 60% of the respondents believe that further regulatory enforcement actions are needed to curb the menace of fraud and corruption in India - these probably arise from delays in judicial process, legislative loopholes, and lack of comprehensive prosecution mechanism, and require a holistic review of the prosecution and settlement system. 70% of the respondents stated that while the investigative agencies are well-equipped to handle complex financial crimes, there is still scope for improvement, Over 70% of the respondents' state that social media and mainstream media have significant power to influence investigation on companies - however, over 60% of our respondents believe that Indian companies are reactive in these matters, and that they do not have a clear social media outreach strategy to deal with situations of regulatory investigations and allegations made in public domain.

Further, over 70% of the respondents feel that Indian companies do not have sufficient capabilities to undertake internal investigations, and that they are not comparable with global best practices in conducting internal investigations. This number is likely to reduce with time, as companies continue to put in place and strengthen their systems and processes.

Factors Contributing to Inadequate Investigation and Conviction Rates in Corporate Fraud Cases.

b. the Complexities and Obstacles in Probing Elaborate Corporate Crimes

Despite the involvement of high-ranking professionals and respected members of society, investigations must follow a systematic procedure involving step-by-step processes, thorough inquiries, well-coordinated efforts, and an analytical approach. Maintaining confidentiality throughout the investigation is crucial, necessitating precautionary measures.

However, the investigation process is often hindered by obstacles such as the financial

[1] https://www.mondaq.com/india/white-collar-crime-anti-corruption--fraud/1354210/emerging-trends-a-survey-on- white-collar-crime-in-india emerging trends A servey on white collar crime in india

influence of the offenders, political connections, and interlocutory petitions in the courts.

Offenders, leveraging their financial affluence, can easily sway political parties to impede accurate investigations, resulting in a lack of convictions. They frequently attempt to manipulate evidence, prolong court trials, and extend the investigation process, creating obstacles and delays.

c. Investigations Stemming from the Technical Complexity of the Crime.

The deficiency in conducting thorough investigations into corporate crimes can be largely attributed to the technical intricacies inherent in these offenses. A significant proportion of the officers comprising the investigating team lacks the requisite expertise and skills to navigate the technical aspects involved. Insufficient training further exacerbates the challenge, leaving investigators ill-equipped to handle the complexities associated with corporate fraud.

It is a stark reality that investigators, tasked with unravelling intricate corporate frauds, often find themselves ill-prepared and inadequately trained for the task at hand. Compounding these issues is the presence of corruption and political entanglements among many investigating officials. Unfortunately, these factors hinder a comprehensive and in-depth exploration of the crimes, as some officials may be disinclined to pursue thorough investigations due to these external influences.

J. CHALLENGES AND CONCERNS IN ADDRESSING CYBERCRIMES.

Law enforcement faces unique challenges in detecting and preventing digital white-collar crimes, including the cross-border nature of many offenses and the jurisdictional complexities they present.

According to an official from the Data Security Council of India (DSCI), an organization established by the software industry lobby group NASSCOM to advocate for data protection, there is a concern that despite the government's investment in training police and other officials, the frequent transfers of trained individuals hinder cases from reaching their logical conclusion. The DSCI is also actively involved in providing specialized training to law enforcement agencies, prosecution lawyers, and members of the judiciary.

Speaking on the condition of anonymity, the official mentioned that government officials frequently lack awareness of their adjudicating powers granted by the Information Technology Act of 2008. The official highlighted that many state IT secretaries are not actively utilizing the quasi-judicial powers vested in them by the IT Act. Additionally, the official pointed out that adjudication cases often end up being redirected to police stations.

Another obstacle hindering investigations, as stated by the DSCI official, is the absence of a robust information-sharing model. The official explained that the lack of a comprehensive and well-defined collaboration and information-sharing model among investigating agencies results in inadequate preparedness for emerging threats.

Furthermore, the official pointed out that the absence of standardized procedures for the seizure and analysis of digital evidence contributes to fewer convictions in cybercrimes. The person emphasized that there are no documented standard procedures for searching and seizing digital evidence, as well as the lack of standard operating procedures for the forensic examination of digital evidence.

K. RECENT WHITE CALLER CRIMES AND CORPORATE FRAUDS 2023

Adani scandal: In January 2023, Hindenburg Research revealed that it had short positions in India's Adani Group, a close ally of Narendra Modi's administration,[463] and flagged debt and accounting concerns. Concurrently, Hindenburg released a report claiming that Indian conglomerate Adani Group "has engaged in a brazen stock manipulation and accounting fraud scheme over the course of decades." Soon after the report's release, Adani Group companies experienced an acute decline in their share prices. In a follow-up piece, *The Guardian* indicated that Hindenburg called on the Adani Group to sue if they believed the report was inaccurate. By the end of February 2023, the group lost $150 billion in value. Gautam Adani's personal net worth came down as he fell from 3rd richest in the world to 30th richest within a month after the report was published. The opposition leaders called it the "biggest scam" and Modi has been criticized for his lack of reaction towards the scandal.

2022

School Service Commission Job Scandal West Bengal:[2] On 23 July 2022, Education Minister of West Bengal and Secretary General of All India Trinamool Congress (ruling party of West Bengal State) Partha Chatterjee was arrested from his residence by the Enforcement Directorate in connection with the alleged State School Service Commission (SSC) recruitment scam cases along with his aide actress Arpita Mukherjee. He was admitted to SSKM Hospital after complaining of chest pains.[456] Later, he was shifted to AIIMS Bhubaneswar where doctors said that he suffers from chronic diseases but does not need immediate hospitalization. He is currently in the custody of the Enforcement Directorate.[457] As of 28 July 2022, the Enforcement Directorate has recovered ₹49.8 Crores cash, gold worth ₹5.07 Crores, ₹56 lakhs worth foreign currency and coded diaries from properties related to him and Arpita Mukherjee.[458] On 28 July he was expelled from the cabinet Ministries he was in charge of and suspended from the TMC.[459][460] On 5 August 2022, he and his aide Arpita Mukherjee were sent to jail custody.

2019

The Karvy Stock Broking (KSBL) scam[3]

The Karvy Stock Broking (KSBL) scam involved the illegal pledging of securities from the demat accounts of over 95,000 clients without their consent. KSBL raised over Rs 2,300 crore through loans against shares from various banks and financial institutions. The broking firm transferred inactive clients' shares to its own demat account and used them as collateral for loans. After the scam was exposed, the Securities and Exchange Board of India (SEBI) took action. In June 2019, SEBI issued a circular prohibiting brokers from pledging client securities for personal loans. Despite a deadline of September 30, 2019, for brokers to segregate client funds and securities, KSBL failed to comply. Investors complained to SEBI, prompting the National Stock Exchange (NSE) to investigate.In December 2019, SEBI, along with depository participants and stock exchanges, took measures to transfer securities of nearly 83,000 affected KSBL clients back to their respective demat accounts. This action aimed to rectify the unauthorized pledging and protect the interests of the affected investors.

[2] https://www.hindustantimes.com/cities/kolkata-news/wbrecruitment-scam-cbi-raids-premises-of-tmc-mla-councillors- cash-seized-101701356107689.html - HINDUSTAN TIMES
[3] https://timesofindia.indiatimes.com/city/hyderabad/karvy-scam-heres-how-it-unfolded/articleshow/85471866.cms the times of India

INX Media case against former Union Minister P. Chidambaram

the INX Media case involves alleged irregularities in the Foreign Investment Promotion Board (FIPB) clearance granted to INX Media during the UPA government. The Financial Intelligence Unit flagged a foreign direct investment of over Rs 305 crore by Mauritius-based companies in INX Media in 2008. The case was initially related to Foreign Exchange Management Act (FEMA) violations and later expanded. Documents discovered during an investigation into a company associated with Karti Chidambaram indicated payments from INX Media when FIPB approval was granted. The CBI registered an FIR in 2017, and the ED filed a money laundering case in 2018. P Chidambaram's plea for anticipatory bail was rejected in August 2019, leading to his arrest. He has been in CBI custody, with the Supreme Court set to pass an order on his plea challenging non-bailable warrants and subsequent remand orders.

L. OPINION OF THE JUDICIARY UP[4] ON CORPORATE FRAUDS IN INDIA[5][6]

The following are the Opinion of the Judiciary over Corporate Fraud in India:

The Supreme Court stated in ***Vimla v. State of NCT, Delhi*** that the concept of deception is a crucial component of fraud, although it did not go into detail. Deception and harm to the individual who was duped are two components of the term "defraud." Injury includes any harm committed to a person's health, intellect, reputation, or any aspects of their personhood other than economic loss, which is the deprivation of property, whether it be mobile or immovable, or of money. A gain or advantage for the deceiver nearly always results in a loss or disadvantage for the victim. The second requirement is met even in uncommon situations where the misled receives a profit or advantage without also suffering a comparable loss.

The petitioner in ***Vikas Agarwal v. Serious Fraud Investigation Office*** was called to court on charges of criminal conspiracy and violating Section 447 of the Companies Act, 2013. It was claimed that the company's mining operations were unlawful. It was also given an unsecured loan through trust. In this case, the Supreme Court said that the definition of fraud given in the explanation section 447 of the Companies Act, 2013 makes it apparent that the instance and also to other people who have in any way participated in the conduct of the offense to obtain an unfair advantage.

[4] Vimla vs State (Govt. Of Nct Of Delhi) on 31 May, 2017
[5] Vikas Agarwal vs Serious Fraud Investigation ... on 6 February, 2019
[6] State Of Maharashtra Trhu Cbi vs Vikram Anantrai Doshi & Ors on 19 September, 2014

M. SYED ASIFUDDIN AND ORS. V. STATE OF ANDHRA PRADESH AND ANR.[4]

Facts: The subscriber purchased a Reliance handset and Reliance mobile services together under the Dhirubhai Ambani Pioneer Scheme. The subscriber was attracted by better tariff plans of other service providers and hence, wanted to shift to other service providers. The petitioners (staff members of TATA Indicom) hacked the Electronic Serial Number (hereinafter referred to as "ESN"). The Mobile Identification Number (MIN) of Reliance handsets were irreversibly integrated with ESN, the reprogramming of ESN made the device would be validated by Petitioner's service provider and not by Reliance Infocomm.

Questions before the Court: i) Whether a telephone handset is a "Computer" under Section 2(1)(i) of the IT Act?

ii) Whether manipulation of ESN programmed into a mobile handset amounts to an alteration of source code under Section 65 of the IT Act?

Decision: (i) Section 2(1)(i) of the IT Act provides that a "computer" means any electronic, magnetic, optical, or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic, or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network. Hence, a telephone handset is covered under the ambit of "computer" as defined under Section 2(1)(i) of the IT Act.

ii) Alteration of ESN makes exclusively used handsets usable by other service providers like TATA Indicomm. Therefore, alteration of ESN is an offence under Section 65 of the IT Act because every service provider has to maintain its own SID code and give its customers a specific number to each instrument used to avail the services provided. Therefore, the offence registered against the petitioners cannot be quashed with regard to Section 65 of the IT Act.

Satyam computer scam (2006-2008)

Satyam Computer Services Ltd. was founded in the year 1987 by Ramalinga Raju and his brother Rama Raju and soon the company became a significant IT player .Also called the mother of all scams, Satyam Computers Scam broke in the year 2009 when the founder and CEO of Satyam Computers, Ramalinga Raju confessed that the company has been falsifying its accounts and overstating its revenues for years. On January 7, 2009, Ramalinga Raju sent a

5-page letter to the SEBI and stock exchanges admitting a fraud of Rs. 7000 crores. The company committed fraud by overstating its revenues, forging bank statements, and manipulating the books by non-inclusion of certain receipts. Over the period of 5-6 years, the company's revenue was overstated by Rs. 4783 crores and as per the SEBI's probe, misstatements to the tune of Rs. 12,320 crores were found. On April 9, 2015, the CBI Special Court sentenced Ramalinga Raju and 9 others to imprisonment for 7 years. A fine of Rs. 5.5 crores was imposed on the Raju brothers.

Harshad Mehta scam 1992

The man behind the massive Securities Scam in 1992 was the well-known and experienced stockbroker, Mr. Harshad Shantilal Mehta. Being a skilled broker, Harshad Mehta misused his knowledge of the stock market to cause manipulations and made huge profits. The scam involved the diversion of bank funds worth Rs 3,500 crore to a group of stockbrokers, led by none other than Harshad Mehta. These funds were then put into the stock market selectively, causing it to surge to over 4,500 points. The scam was first exposed by journalist Sucheta Dalal in April 1992.Thereafter, the banks realised that they were holding on to worthless bank receipts and the stock market too came crashing down. Harshad Mehta was charged with about 72 criminal offences including cheating, bribery, forgery, criminal conspiracy, falsification of accounts, etc., and over 600 civil suits were initiated against him. In September 1999, the Bombay High Court convicted Harshad Mehta and three others in an Rs. 380.97 million MUL fraud case (one of the many cases within the larger scam) and they were sentenced to rigorous imprisonment of 5 years.

DHFL

DHFL was the first ever fraud in a housing finance company, which happened mainly due to active involvement of promoters in syphoning of funds and alleged money laundering.

How fraud was committed:

- Granting of loans to related parties of promoters
- Loans granted to parties, who were not credit worthy or were unknown having same addresses in obscure locations
- Evergreening of bad loans
- Creation of around 6 lacs dummy accounts at one branch, using name of borrowers who

had already repaid loans. These accounts were used to grant loans which were used to siphon funds to promoter companies. These loans ultimately turned out to be non-recoverable

- Utilization of borrowed funds for personal purposes, such as acquiring personal properties, yachts etc.
- Consequently, huge amounts were shown as recoverable in the balance sheet, which were not recoverable

The above-mentioned scams highlight a disturbing trend where individuals in positions of trust, often highly esteemed, manipulate stocks and investors' funds, disregarding laws and regulations.

It is evident that regulatory authorities may have shortcomings, either in detecting these crimes before they occur or in ensuring compliance beforehand. Various factors contribute to this, including legal loopholes, political influence, and sometimes insufficient resources for thorough investigations.

Additionally, inadequacies in training for law enforcement officers could also play a role. The consequences are significant, as innocent people place their trust in these individuals, only to have it betrayed due to a lack of effective oversight and preventative measures.

N. PWC'S GLOBAL ECONOMIC CRIME AND FRAUD SURVEY 2022:[7]

PwC surveyed 111 organizations across India from diverse industries. Amongst those surveyed, 71% belonged to the C-suite. Half the companies had a turnover over USD 1 billion.

According to the new frontier of fraud in India PwC's Global Economic Crime and Fraud Survey 2022: India Insights looks at the new frontier of economic crime – platform fraud, or fraud associated with social media, enterprise, e-commerce, and other kinds of platforms. Largely unrecognized for years, this insidious form of fraud has become more common since the start of the pandemic, owing to the rise in remote work and growth in e-commerce, delivery applications and contactless payments. And it is evolving and growing at a worrying pace,

[7] https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html PWC global economic crimes and fraud .

posing a new set of challenges for Indian companies. For the second report in this series, PwC surveyed 111 organizations across India from diverse industries such as technology, financial services, banking and capital markets, consumer products and retail, education, healthcare, hospitality and leisure, and industrial products and manufacturing.

What is the financial impact of fraud or economic crime on Indian organizations?

1. 40 % of Indian organizations lost between USD 50,000–1,00,000.
2. 17% lost between USD 1 million–50 million.
3. 5% incurred a loss of USD 50 million and above through the most disruptive incidents of fraud/crime.

N. RECENT AND PRESENT REFORMS UNDER THE COMPANIES ACT OF 2013

1) Advising the Serious Fraud Investigation Office on improving its investigation and prosecution procedures under the Companies Act

   The Serious Fraud Investigation Office (SFIO) is a statutory body recognized under Companies Act, for detecting and prosecuting frauds and other white-collar crimes under company law. While it was first established in the year 2003 in the aftermath of several corporate frauds involving Indian companies, it came into its own only recently by way of its new powers under the 2013 Act.

   From 40-plus amendments made in the Companies Act 2013, it comes across that the government is shifting the focus more on execution of the law. "If you see the amendments, the government is trying to make the execution very strict. They are increasing the penalties and offences bringing them in line with foreign laws," says Mamta Binani, Past President of The Institute of Company Secretaries of India (ICSI), a high court lawyer and an Insolvency Professional.

2) Making compliance stricter

   Among 40-odd amendments brought about in the Companies Act 2013, the most notable ones relate to better governance and measures to curb corporate frauds. One of the most significant of them is if the government is of the opinion that a fraud has taken place, and the company's directors, key managerial people or officers have taken undue advantage or benefits, the government can approach the NCLT for disgorgement of such undue advantage. The government can also ask the NCLT for holding such

directors, KMPs or officers personally liable without any limitation of liability. Repeated defaulters will now have to pay up to twice the penalty prescribed for the offences.

O. EXPERTS DECODE STEPS TO COMBAT FINANCIAL FRAUD IN THE DIGITAL ERA

Gopal Murli Bhagat, Deputy Chief Executive of the Indian Banks' Association (IBA) said "Fraud in Banking was there, is there and will be there but there are ways to identify profiles or identities of the borrowers which earlier was a big challenge. Cybercrime is on the rise. Then are we doing enough on technology adoption? The expenses on tech adoption are minuscule but are customers getting the benefit of this adoption in proper ways spread over a period of time?" Speaking in depth on tech adoption, he further commented on how the costs towards tech adoption is often underestimated and the need for banks to focus on this to a larger extent. The solution could be a single negative registry for fraudsters so that this database can he accessed by all banks.

The recent years have seen rapid digital transformation post the introduction of the Unified Payments Interface (UPI) in 2016 and the demonetization drive. "This transformation has led to a significant surge in financial as well as digital transactions. The exponential growth in digital transactions has, in turn, given rise to a corresponding increase in fraud incidents" said Durgadas Rege, Chief Internal Vigilance, RBI Bank.

However, regulators have taken proactive measures to address this growing concern. They have issued advisories and implemented regulations aimed at curbing fraudulent activities within the financial sector. Banks, as crucial players in this landscape, have been called upon to collaborate with regulator and employ various strategies to combat fraud effectively.

P. POSSIBLE SUGGESTIONS AND CONCLUSION FOR WHITE COLLAR CRIMES UNDER CORPORATE FRAUDS, AND FINANCIAL FRAUD DUE TO DIGITAL TRANSFORMATION.

1) Recommendations for Mitigating Corporate Crimes:

- Government and Organizational Initiatives

  To curb corporate crimes, both the government and organizations can take proactive

measures. Here are suggestions for what organizations can do

- Tone at the Top:

  Foster an ethical environment by ensuring that leadership sets a strong ethical tone. Executives should exemplify and promote ethical behavior throughout the organization.
- Lead by Example:

  Leadership should lead by example, adhering to ethical standards and principles. This sets a precedent for employees to follow suit.
- Corporate Code of Conduct:

  Establish and enforce a comprehensive corporate code of conduct that outlines ethical guidelines and expected behavior for all employees.
- Strict Rules for Reporting Unethical Practices:

  Implement stringent protocols for reporting unethical practices through a confidential and reliable reporting mechanism, encouraging employees to speak up without fear of reprisal.
- Robust Internal Control:

  Develop and maintain reliable internal control mechanisms to monitor and regulate organizational activities, ensuring adherence to ethical standards.
- Training Programs:

  Conduct regular training programs covering various aspects, including ethics, internal controls, fraud prevention, and adapting to technological and business changes.
- Specialized Training for Monitors:

  Provide specialized training for individuals tasked with monitoring and ensuring compliance, enhancing their ability to identify and address potential issues.
- Reference Checks for New Employees:

  Implement thorough reference checks on new employees to verify their backgrounds.
- Anti-Corruption & Anti-Bribery Practices:

  Adopt and rigorously enforce anti-corruption and anti-bribery practices, integrating them into the organizational culture and policies.
- New Code of Governance:

  Develop an updated and comprehensive code of governance that reflects the evolving landscape of corporate ethics and governance standards.

  By implementing these measures, organizations can create a culture of integrity, transparency, and accountability, mitigating the risks associated with corporate crimes

and fostering a more ethical business environment.

Q. POSSIBLE SUGGESTIONS FOR FINANCIAL FRAUD DUE TO DIGITAL TRANSFORMATION.

a) Dedicated fraud control unit

The government should establish a specialized and autonomous unit focused on fraud control, comprising personnel equipped with expertise and experience in managing fraud risks. It is crucial that the unit possesses comprehensive knowledge of all business divisions, products, services, and the intricate aspects of the business. Specifically, the staff should be well-versed in technology, fraud risk assessment, and security measures to effectively address the dynamic challenges associated with fraudulent activities. This dedicated unit must be proficient in understanding the complexities of various business operations and stay abreast of technological advancements to ensure a robust and proactive approach to fraud prevention and control.

b) Regular training and awareness

They should undergo consistent training and participate in awareness sessions focused on managing the risks associated with fraud. This training should encompass the following key areas:

c) Governance Framework, Policies, and Procedures:

Stay informed about the governance framework, policies, and procedures designed to prevent and detect fraud risks within the organization.

d) Updates on New Payment Channels:

Stay updated on the latest developments in payment channels and understand the specific risks associated with these channels, both traditional and emerging.

e) Traditional and Emerging Fraud Risks:

Gain knowledge about both traditional and emerging fraud risks, recognizing the evolving nature of fraudulent activities in the financial sector.

f) Technologies for Fraud Prevention:

Familiarize oneself with the technologies employed by Financial Institutions (FIs) for preventing and detecting fraud, ensuring a coprehensive understanding of the tools available.

g) Fraud Detection Methods and Techniques:

Acquire skills in various fraud detection methods and techniques, understanding how to

identify and respond to potentially fraudulent activities effectively.

h) Fraud Reporting for Compliance:

Understand the protocols and procedures for fraud reporting, considering both internal reporting mechanisms and regulatory compliance perspectives.

Participating in regular training and awareness sessions in these areas is crucial for individuals working in the financial sector. This ensures that they are well-equipped to navigate the evolving landscape of fraud risks, adopt preventive measures, and contribute to maintaining a secure and compliant financial environment.

R. CONCLUSION

This research aims to comprehend the evolving dynamics of white-collar crime within corporate frauds, particularly in the context of digital transformation. It seeks to gain insights into previously perpetrated frauds, analyses the recent trends in corporate frauds attributed to digital transformation, assess the impact of corporate frauds through surveys conducted by various corporate legal entities, and scrutinize the existing legal frameworks and regulatory authorities governing white-collar crime in corporate frauds and cybercrime. Ultimately, the research endeavors to provide viable suggestions to effectively address and mitigate the challenges presented by these scenarios.

S. REFERENCES

1. *Vimla vs State (Govt. Of Nct Of Delhi) on 31 May, 2017*
2. [2]*Vikas Agarwal vs Serious Fraud Investigation ... on 6 February, 2019*
3. [3]*State Of Maharashtra Trhu Cbi vs Vikram Anantrai Doshi & Ors on 19 September, 2014*
4. Adani scandal: In January 2023,
5. School Service Commission Job Scandal West Bengal: On 23 July 2022,
6. Satyam computer scam (2006-2008)
7. Harshad Mehta scam 1992
8. The Karvy Stock Broking (KSBL) scam
9. INX Media case against former Union Minister P. Chidambaram
10. DHFL

ARTICLES REFERRED

1. https://www.mondaq.com/india/white-collar-crime-anti-corruption--fraud/1354210/emerging-trends-a-survey-on-white-collar-crime-in-india emerging trends A servey on white collar crime in india
2. [1]https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html PWC global economic crimes and fraud.
3. https://www.lexology.com/library/detail.aspx?g=a815f6b0-048e-4d93-ba3d-28023e6f057f India white collar crime
4. https://www.fbi.gov/investigate/white-collar-crime federal Bureau of investigations
5. https://blog.ipleaders.in/white-collar-crimes/ I pleader
6. https://www.hindustantimes.com/cities/kolkata-news/wbrecruitment-scam-cbi-raids-premises-of-tmc-mla- councillors-cash-seized-101701356107689.html - HINDUSTAN TIMES