

## FINANCIAL SYSTEMIC FRAUDS IN BANKING SECTOR AND MONEY LAUNDERING CATAclySM: INDIAN REALISM WITS

**Ms. Nanda Pardhey** Assistant Professor (SG), School of Law, University of Petroleum and Energy Studies, Dehradun and Ph.D. Scholar of Department of law, Savitribai Phule Pune University, Pune.

*“It is well that the people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning.” — Henry Ford*

### Abstract

Financial systemic frauds are growing concern which directly affects the economy of country not only nationally but internationally. Today banking frauds are high in the country which leads question on banking regulatory system and initiative of monitoring and risk assessment. Another important concern is of money laundering by high profile culprits in sophisticated way indulging in illegal transactions. The focus of paper is mainly on issues of financial frauds in banking sector and money laundering analysis. Fraudster are exploiting vulnerabilities that has being opened during Covid -19 pandemic lockdown, increasing risks of cyber-attacks using various modus operandi. Covid -19 effect on banking sector and regulatory bodies concern relating to threats of evolving risks due to online transactions which is continuing threat of fraudster to victimize the not so techno-savvy lay man. During this entire pandemic FATF recommendation and statements particularly emphasizing on criminal activities alert to member countries wherein they advised to detect and report suspicious transactions of money laundering and terrorist financing risks. Customer due diligence (CDD) requisite which is laid down by RBI initiative to identify banking transactions for banking frauds, money laundering and terrorist financing. During the past one year RBI amended its master direction dealing with KYC norms for banking sector taking into account the pandemic situation. Pandemic became a favourable environment for financial criminality for fraudsters who have healthy ground to commit the crimes. Role of governing bodies to tackle and curb this financial systemic fraud and cases filed under various legislations will be analyzed. Key word: money laundering, financial fraud, banking fraud, CDD, covid-19

### Introduction

Financial Systemic frauds are arising rapidly in all segment of society wherein illegal activities are done by the criminals or white collar criminals using online and offline mode across the country that are crimes underlying antisocial elements which are both civil as well as criminal frauds. Frauds ranges in different forms and ways done by criminals like identity fraud, mass marketing fraud, dating fraud, high risk investment fraud, online banking fraud, online ticket fraud, plastic card fraud, telecommunications fraud, telephone banking fraud etc. in all this frauds the victims or the economy face financial loss due to such financial systemic fraud which also includes black money, corruption, embezzlement, forgery etc. Cohort of all this systemic financial frauds happens in some of vulnerable segment. If we look into the sources of this frauds they affect the economy of the country and bring to halt the economic activities of certain sector which are the source of finances doing important activities in the country which creates threat to the economy overall. These activities if we specifically look are specified sectors that are vulnerable one is systemic financial fraud like financial markets, banking sectors, international transactions leading to black money and also involving tax havens, ponzi schemes, jewellery markets etc.

Financial market is one of the important sector for generating economy, but if we see the financial market and their transactions they are involved in black money in diverse methods and forms, which may come through shell companies which are not actually doing any business but they are the one who manipulate the offshore companies and investors through the initial public offers which may escalate the trading that may be artificial in nature, due to which the ordinary investors suffers in such financial market transactions. Financial systemic frauds in various segments are scattered under different rules, regulation and governance under various bodies which are amended from time to time making it more stringent taking the economic into consideration to curb financial frauds. Even though we have the

regulations but they can be said to be failing due to lack of police investigations, employees as accomplice and investigating authorities who are not allowed to go in depth investigation involving high profile people's from industries, political background and businessmen, unless they have strong evidence and backing from higher authorities to investigate and nail the crimes of such frauds.

In the first six months of 2020, the Central Bureau of Investigation (CBI) has registered 40 cases of bank frauds and is probing bad loans worth over Rs 14,400 crore<sup>1</sup>. Senior National Conference leader and former J&K finance Minister Abdul Rahim Rather's son Hilal Ahmed Rather and his partnership firm Paradise Avenue was accused of defrauding J&K bank of Rs 177 crore, and in March the case was transferred to CBI and a chargesheet was filed<sup>2</sup>. Bank frauds worth more than Rs 1.85 lakh crore were reported in the year ended June 2020 compared with over Rs 71,500 crore in the previous fiscal, according to the RBI's Annual Report for 2019-20<sup>3</sup>. Bank frauds, in value terms involving an amount of Rs 1 lakh and above, have more than doubled in 2019-20 period to Rs 1.85 trillion from Rs 71,543 crore in 2018-19 period, up 159 per cent<sup>4</sup>. The CBI registered about 190 cases of bank fraud in year 2020, involving alleged misappropriation of close to ₹60,000 crore, and about a dozen cases, the companies and their top functionaries were accused of cheating the banks of more than ₹1,000 crore<sup>5</sup>. The Enforcement Directorate (ED) has filed a criminal case of money laundering against HDIL as part of its probe into the alleged loan fraud in Punjab and Maharashtra Co-operative (PMC) Bank<sup>6</sup>. Thakur and CA Gopal Chaturvedi were arrested under the Prevention of Money Laundering Act (PMLA), after the ED searched five residential and business premises linked to the Viva Group<sup>7</sup>. The Joint Task Force (JTF) approach needs to be adopted for dealing with serious cases of corruption, tax frauds, terror financing, money-laundering, Ponzi / MLM schemes, banking / financial frauds, illegal betting / lottery, etc. and the JTF in such cases could consist of all the concerned agencies led by the agency connected with the main infraction of the law<sup>8</sup>.

Sixty-two percent of the cybercrime complaints lodged in 2020 were related to financial frauds, police said in a statement in New Delhi and witnessed in incidents of cybercrime during the coronavirus lockdown<sup>9</sup>. *“Among the complaints of various cybercrime received, the predominant ones are of online financial frauds, accounting for around 62 percent of the total”*<sup>10</sup>. A major online financial fraud theft of personal data of applicants by a few micro finance companies said to be front-end firms of investors in some neighbouring countries has been busted in Karnataka<sup>11</sup>. The fraud was done through mobile apps as larger group of people relied on mobiles app during covid pandemic wherein life came to halt and people relied on the technology which came as guise of providing them relief but leading them to victimization. Looking at the figures and news reported we can see that economic conditions are affected by frauds committed and news observations tell about loopholes in implementation of rules and regulations under various Statues. I would like to highlights the recent financial systemic frauds in India, analyzing the statutes and its overall development, implementations, convictions and failures. There are different enactment to regulate and bodies to investigate the matters of such crimes but still lack of

<sup>1</sup> <https://www.timesnownews.com/india/article/14429-crores-of-bank-fraud-cases-registered-by-cbi-in-first-half-of/605963> reported on 13<sup>th</sup> June, 2020, accessed in February, 2021

<sup>2</sup> Ibid

<sup>3</sup> <https://www.bloomberquint.com/business/rbi-annual-report-2019-20-bank-frauds-more-than-double>, reported on 25<sup>th</sup> August, 2020. accessed in February, 2021

<sup>4</sup> [https://www.business-standard.com/article/economy-policy/amount-in-bank-fraud-up-159-to-rs-1-85-trn-in-2019-20-rbi-annual-report-120082500972\\_1.html](https://www.business-standard.com/article/economy-policy/amount-in-bank-fraud-up-159-to-rs-1-85-trn-in-2019-20-rbi-annual-report-120082500972_1.html) reported in 25<sup>th</sup> August, 2020 accessed in February, 2021

<sup>5</sup> <https://www.thehindu.com/news/national/cbi-registers-about-190-cases-of-bank-fraud-in-2020/article33464560.ece>, reported on 31<sup>st</sup> December, 2020, accessed in February, 2021

<sup>6</sup> <https://economictimes.indiatimes.com/news/politics-and-nation/pmc-bank-fraud-case-viva-group-md-ca-remanded-in-ed-custody/articleshow/80425354.cms> reported on 23<sup>rd</sup> January, 2021, accessed in February, 2021

<sup>7</sup> Ibid

<sup>8</sup> Black Money, White Paper, “ Ministry of Finance and Department of Revenue” May 2012

<sup>9</sup> <https://gadgets.ndtv.com/internet/news/new-delhi-cybercrime-complaints-financial-frauds-2020-delhi-police-fake-call-centres-facebook-twitter-instagram-2343490> reported on 25<sup>th</sup> December, 2020 accessed in February, 2021

<sup>10</sup> Ibid

<sup>11</sup> <https://www.ndtv.com/india-news/karnataka-police-busts-fraud-using-mobile-based-loan-apps-2343309> reported on 25<sup>th</sup> December, 2020 accessed in February, 2021

investigation and regulation leads to huge financial frauds leading to economic loss to the country and victimizing of the vulnerable not so techie savvy pushing them to more agony. If we look into the regulations in India there are many legislation to govern and regulate them from Banking Law, Reserve Bank of India (RBI), PMLA, Information Technology Act (ITA), Securities Exchange Board of India (SEBI), Income Tax Act, Financial Act, so on.

***Governing Statutes for financial systemic frauds in India a critical analysis with contemporary tendencies in crimes pre and post pandemic.***

***Banking sectors***

Banking frauds have increased in India using online and offline modes which included online banking fraud, plastic card fraud, telecommunications fraud, telephone banking fraud etc. which were done victimizing the general public in the pandemic not only this but bank loan frauds had shocked the entire country wherein crores of rupees frauds were done by industrialist, politician and businessman's. RBI gets its power under Banking Regulation Act, 1949 under the provision of sec. 35 thereby empowering RBI to make necessary and immediate directions in public interest from time to time after being satisfied. According to its Master Direction (MD) dated 1<sup>st</sup> July, 2016 which was again updated in 3<sup>rd</sup> July, 2017 had made it mandatory for banks, wherein banks need to furnish Fraud Monitoring Return (FMR) in individual fraud cases, irrespective of the amount involved, to RBI electronically using FMR Application in XBRL System supplied to them within three weeks from the date of detection<sup>12</sup>. MD directed the banks that they should have and ensure reporting system which should be streamline as per the norms set forth by RBI. Banks should therefore, strictly adhere to the timeframe fixed in this circular for reporting of fraud cases to RBI failing which they would be liable for penal action prescribed under Section 47(A) of the Banking Regulation Act, 1949<sup>13</sup>. The banks had the directive that they should ensure that all frauds of ₹0.1 million and above are reported to their Boards promptly on their detection and such reports should take note of the failure on part of concerned branch officials and controlling authorities and details of action initiated against the officials responsible for the fraud should be reported<sup>14</sup>. MD had in place rules to deal with banking frauds, where banks needed to annually reviews in that particular year how many total number of frauds were detected and the amount involved in the previous two years data, what was the modus operandi, analysis of fraud with the bank officials/ staff involved in such cases, region wise data of such frauds and number of cases estimated, time required to detect such cases etc. Further, MD also provides for the provisions of status of such to frauds reported to CBI or Police, action finally taken, number of cases disposed of, and what initiative was taken for prevention or punitive major by bank, during the specified year of reported cases of fraud, how much frauds were reduce or minimise such incidence of frauds.

According to MD, the banks shall report to Central Fraud Monitoring Cell (CFMC), RBI and the SSM (Senior Supervisory Manager) of RBI, the details of fraud cases of ₹0.1 million and along with reasons for closure after completing process should be submitted. Under its directive banks are bound to follow the norms set in as follow-

- a. While dealing with cases of fraud, the authorities should close only those cases wherein the actions are completed, with approval from SSM;
- b. the cases are pending with authorities are finally disposed of, further examination of officials and staff involved and their examination has been done and they are made accountability by completing process;
- c. when such frauds taken place how much amount recovered or return off in such matter;
- d. if any insurance claim that is settled as per its application; and
- e. Lastly in such situations banks need to follow the review system and procedure so that they identify causative issues involved and the lacunae which is certified with appropriate authorities dealing with it.

<sup>12</sup> Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs (Updated as on July 03, 2017) available at [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=10477](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10477)

<sup>13</sup> Ibid

<sup>14</sup> Ibid

In dealing with cases of fraud/embezzlement, banks should not merely be actuated by the necessity of recovering expeditiously the amount involved, but should also be motivated by public interest and the need for ensuring that the guilty persons do not go unpunished<sup>15</sup>. General rule which is followed in cases of fraud is that the cases should invariably be referred to respective State Police that is based on the jurisdiction or to CBI as the case may be depending on the kind of bank fraud, as specified by RBI in this behalf. The rising trend in loan related frauds in financial sector is a matter of serious concern and the delay in detection and reporting of such frauds by banks<sup>16</sup> has increased the burden on financial sector and banking sector. This frauds raises various issues relating to prevention by using Know Your Customer (KYC) norm, and Customer Identification Procedure (CIPs) mode set by RBI, so that there could be early detection of banking frauds of different types and they are timely reported. This entire process was taken care by an Internal Working Group (IWG) of RBI in consultations with various banks and other stakeholders in banking and financial sector. With this objective in mind, the focus was set by RBI, that there can be prevention, following the laid down procedure like monitoring and dissemination which could lead to early detection with prompt reporting and can be taken care by the investigation agencies. In this entire regulation norms that were initiated laying down the process of staff accountability wherein their negligence is taken into account to avoid risk that directly impact economy. RBI set forth the framework which laid clear stipulated timelines for the banks that required to be followed strictly.

RBI came up with the Red Flagged Account (RFA) is one where a suspicion of fraudulent activity is thrown up by the presence of one or more Early Warning Signals (EWS), wherein such signals in a loan account should immediately put the bank on alert regarding a weakness or wrong doing which may ultimately turn out to be fraudulent<sup>17</sup>. They also made the provision for continuous monitoring of those EWS account wherein banks were set to be on a vigilance and alert mode from the fraud perspective during annual review of accounts. During audit, auditors do come across occasions wherein certain transactions in the bank account or documents of banks leading to the possibility of fraudulent transactions which can be highlighted and alerted to the banks. Whenever such situation comes, the auditor are bound to immediately bring it to the notice of management and also the Audit Committee of the Board (ACB) for appropriate action to be taken in such incidences. The best incidence of financial fraud committed and neglected by auditors can be seen in Punjab National Bank (PNB) case raising the issues of role of auditors in detecting fraud in while auditing. In PNB, MK Sharma was knowing about the fraud but didn't file any complaint with audit office and according to ICAI is mandatory for every auditor to verify and scrutinized every transaction which takes place through SWIFT but in this case the auditor deliberately didn't verify the transactions done through SWIFT and the Internal Auditor, Concurrent Auditor And Statutory Auditor Of The Bank should have been checking the transactions which has been done through SWIFT but they deliberately ignored all the transactions<sup>18</sup>. On march 2013, non-fund based loan of PNB was Rs 407 crore, on March, 2014 it zoomed to Rs. 3458 crore and on March 2017, it raised to Rs. 4302 crore<sup>19</sup>. The value of PNBs fraudulent transactions are nearly 50 times the bank's Q3FY18 net profit of Rs 230.11 crores and there were five banks that have been directly affected by the fraudulent transactions as they have offered credit based on the Letter of Undertakings (LoUs) issued by PNB which includes banks which were affected are UCO bank, Allahabad Bank, Axis Bank, Union Bank of India, and SBI<sup>20</sup>. After detailed investigation it came out to be 12,700 cr. or 1.27 billion approximately, but by the time this investigation was done, it was already very late and PNB was under crisis situation because of Mr .Nirav Modi's who

<sup>15</sup> Ibid

<sup>16</sup> Loan frauds circular by circular DBS.CO.CFMC.BC.No.007/23.04.001/2014-15 dated May 7, 2015. Available at <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=9713&Mode=0> accessed in February, 2021

<sup>17</sup> Supra note No. 16

<sup>18</sup> Lovejit kaur, "PNB SCAM: Shining Diamond Trader Took Away PNB's Shine" ISSN: 2321-9939, Volume 8, Issue 1 ©IJEDR 2020 also available at <https://ijedr.org/papers/IJEDR2001010.pdf>

<sup>19</sup> Ibid

<sup>20</sup> S. Gayathri and 2T. Mangaiyarkarasi, "A Critical Analysis of the Punjab National Bank Scam and Its Implications", Volume 119 No. 12 2018, 14853-14866 ISSN: 1314-3395 (on-line version) url: <http://www.ijpam.eu> also available at <https://acadpubl.eu/hub/2018-119-12/articles/6/1387.pdf>

had never intended to pay back the money ever otherwise there would have no need to roll back the LOU year after year<sup>21</sup>. Monetary loss in this case could have been prevented by the early proactive detection and follow-up with the concerned paying/intermediary banks in the transaction that took place through LOU, this financial fraud gave various stakeholders and country an economic set back. This case was dealt by CBI and ED and case was filed for fraud and money laundering against him. He absconded to London after committing offence in India. Modi is the subject of two sets of criminal proceedings, with the CBI case relating to a large-scale fraud upon PNB through the fraudulent obtaining of LoUs or loan agreements, and the ED case relating to the laundering of the proceeds of that fraud. He also faces two additional charges of "causing the disappearance of evidence" and intimidating witnesses or "criminal intimidation to cause death" added to the CBI case<sup>22</sup>. Indian investigating agencies are fight a case of extradition under sec. 91 which is the threshold of the Extradition Act, 2003, in the London court, so that he can be brought back to India and punished. Fugitive diamond merchant Nirav Modi appeared via video link for a routine 28-day remand hearing, before Westminster Magistrates' Court in London, where he was further remanded in custody until January, 2021, to conclude hearings in his extradition case<sup>23</sup>. Nirav Modi's sister and brother-in-law have "turned approvers" in USD 2 billion PNB fraud case against him and they will help the ED confiscate assets worth Rs 579 crore<sup>24</sup>. This case has brought the loopholes of the governing bodies into picture dealing with banking fraud at such a huge scale without being identifying for years with the help of the staff of banks officials.

After the above case another case of bank fraud came to limelight and this time it was YES bank fraud. In this case CBI had registered the case for alleged cheating, fraud, criminal conspiracy in sanctioning of loans by YES Bank and in exchange receiving kickbacks by Kapoor from DHFL promoters<sup>25</sup>. CBI in its first information report mentioned that, the scam started taking shape between April and June 2018 when Yes Bank invested Rs 3,700 crore in short-term debentures of the debt-laden DHFL and whereas ED in its chargesheet filed in May under anti-money laundering laws highlighted the Kapoor's illegal gratification amounting Rs 5,050 crore. Along with several irregularities in distributing bank loans to corporate entities, by misusing his official position, creating shell companies for laundering money, defaults, and creating tainted assets<sup>26</sup>. The ED has arrested Yes Bank co-promoter Rana Kapoor in a fresh money laundering case linked to an alleged Rs 4,300 crore fraud at the PMC Bank in Maharashtra<sup>27</sup>. Investigation agency during the investigation found that many family companies were engaged in this fraud and there is case of quid pro quo. This financial systemic frauds are impacting the economy of the country and raising alarming loopholes in the regulatory mechanism of frauds in banking sectors. Central Vigilance Commission (CVC) report, wherein they said that-

*“as per RBI annual report 2018-19 released, an amount of 71542 crore worth of frauds have been detected by banks as a whole involving 6801 incidents while 5916 cases of frauds were reported during 2017-18 amounting to 41167 crores. This indicates a serious 15% Y-o-Y growth in frauds during 2018-19 in number of cases and 73.8% in terms of amount of frauds and in the last 11 financial years,*

<sup>21</sup> G. Singh, S. Srivastav, A. Gupta and V. Garg, "An Analysis of Financial Fraud through PNB Bank Scam and its technical Implications," 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2020, pp. 436-442, doi: 10.1109/ICCAKM46823.2020.9051500. also available at <https://ieeexplore.ieee.org/abstract/document/9051500>

<sup>22</sup> <https://economictimes.indiatimes.com/news/politics-and-nation/pnb-scam-nirav-modis-extradition-from-britain-to-india-set-to-be-decided-on-february-25/articleshow/80175717.cms> reported on 8<sup>th</sup> January, 2021

<sup>23</sup> <https://economictimes.indiatimes.com/news/politics-and-nation/nirav-modis-remand-in-uk-extended-till-january-7/articleshow/80013170.cms> reported on 29th December, 2020

<sup>24</sup> <https://economictimes.indiatimes.com/news/politics-and-nation/nirav-modis-sister-brother-in-law-turn-approver-in-pnb-money-laundering-case/articleshow/80155317.cms> reported on 7th January, 2021

<sup>25</sup> [https://www.business-standard.com/article/current-affairs/yes-bank-loan-fraud-cbi-charges-rana-kapoor-with-criminal-conspiracy-120062501509\\_1.html](https://www.business-standard.com/article/current-affairs/yes-bank-loan-fraud-cbi-charges-rana-kapoor-with-criminal-conspiracy-120062501509_1.html) reported on 25th June, 2020

<sup>26</sup> Ibid

<sup>27</sup> <https://timesofindia.indiatimes.com/business/india-business/ed-arrests-yes-bank-co-founder-rana-kapoor-in-fresh-money-laundering-case/articleshow/80483241.cms> reported on 27th January, 2021

53334 fraud cases worth 2.05 lacs crores have been reported”<sup>28</sup>. The statistical data reported by CVC shows unruly concerns of banking sector but also echoes upon lack of awareness and its ineffectiveness in the system. During last 11 years, `2.05 lac crores of frauds have been reported which is almost equal to 2.50 lac crores capital infused by the government during the last 5 years<sup>29</sup>. Further the report of CVC it states that, “as per RBI annual report for 2018-19, 73% of the total frauds are large ticket corporate frauds worth 100 crores and above, involving a total amount of 5.22 lac crores; the average lag between the date of occurrence and its detection by banks was 22 months while for large ticket frauds of 100 crores and above, the time lag was whopping 55 months”<sup>30</sup>.

The reported stressed that due to such a long excessive delay in detecting the fraud which fails the law to perform a deterrent impact on the fraudsters leading this entire lag works in their favour providing them an incentive.

In banking sector when a customer opens an account he/she has to go through the KYC norm same ways there should be Know Your Employee (KYE) for the banks. In recent cases it was identified that banking frauds took place because of the insider help of the employee of the bank who were accomplice in neglecting the regulations of banks under law and governing bodies which was against the bank set norms, because of such abetment fraud happened. Governance describes the elements of organizational control and accountability that are necessary for the good management of any organization, private or public and in addition to this effective implementation of a good governance system decreases the risk of fraud by encouraging a work environment that is not conducive for such behavior especially because there is better monitoring and control of management and accountability of the board through the nomination and remuneration committees, which sets the tone at the top<sup>31</sup>. The employee should go through the background checks on periodic rotations, their internal assessment should be conducted periodically, placing strict compliances of vigilance assessments, and internal audits of employee so that effectively employees are employed which are conducive for banking sector as per CVC. In cases of banking frauds it was found that KYC norms not followed and authenticity of the document are not scrutinized by the banks. Further it’s observed that due diligence not followed by employees of new borrowers as per the guidelines provided. Verification not done as per the various list provided under RBI and SEBI guidelines wherein the name of the borrower company/ Promoters/ Directors/ guarantors has to be scrutinized well whether they fall under any defaulter list, caution list or banned list of any governing bodies set under the law like Income Tax list, RBI defaulter List, etc. Frauds are increasing in banking sector and we can read news of frauds in various banks wherein strict norms are to be followed by the regulatory. The Organisation for Economic Co-operation and Development (OECD) principles for enhancing integrity in public procurement address transparency, good management, prevention of misconduct, compliance and monitoring, and accountability and control<sup>32</sup>. RBI has taking stringent steps to curb this menace of frauds in banks one such move can be seen in the recent action taken by RBI against Standard Chartered Bank which is positive move. RBI has, by an order dated January 21, 2021, imposed a monetary penalty of ₹2 Crore on Standard Chartered Bank–India for non-compliance with certain directions issued by RBI contained in the “Reserve Bank of India (Frauds - Classification and Reporting by commercial banks and select FIs) Directions 2016”<sup>33</sup>. RBI under the provisions of Section 47A (1) (c) read with sec. 46 (4) (i) of the Banking Regulation Act, 1949, for delays in reporting of frauds to RBI, revealed during the statutory inspection of the bank with reference to its financial position as on March 31, 2018 and March 31, 2019<sup>34</sup>.

<sup>28</sup> Central Vigilance Commission, Vigeye Vani, quarterly Newsletter, Special Issue on Banking Sector, Oct-Dec 2019 also available on <https://cvc.gov.in/sites/default/files/Final%20Book%20CVC.pdf> Pg. 17

<sup>29</sup> Ibid

<sup>30</sup> Ibid Pg. 20

<sup>31</sup> Maria Krambia-Kapardis, “Corporate Fraud and Corruption A Holistic Approach to Preventing Financial Crises” 1<sup>st</sup> published 2016 by Palgrave MacMillan, Pg. 113

<sup>32</sup> Ibid, Pg. 146

<sup>33</sup> Press release available at [https://www.rbi.org.in/scripts/BS\\_PressReleaseDisplay.aspx?prid=51006](https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=51006) in January, 2021 available on

<sup>34</sup> Ibid

During the last year due to outbreak of pandemic of Covid-19 in the beginning of 2020 brought the economy halt due to the long lockdown declare by the government. During lockdown the people moved from offline banking to online banking. Wherein RBI also insisted the customer to use the online platform for various transactions using the banking apps. This phase of pandemic added to larger economic fraud in banking sector and data theft of the customer where they were cheated. This mobile app's were directly available on play store and directly installed using the phone where they were asked for access of the mobile phone which they accepted which provided access to the providers with all information which the culprits used against victims and this apps were monitored from their cloud system in their home countries and in certain cases they hacked all the information and data of victims for victimizing them with financial theft. Criminals use the Internet, phone, postal mail, and anything else they think may help them get someone else's money and they are persistent because it has worked before, and chances are that it will work again<sup>35</sup>. Frauds and different scams are not new but during pandemic it emerged out because growth in digital transactions which revolutionized with expansion of the digital transaction and other technologies have led to increased number of e-banking fraud. While, Covid-19 has accelerated digital transactions and payments, it has also necessitated remote working conditions, thereby making banks and financial institutes more vulnerable to threats wherein cyber criminals have been quick to exploit the opportunities presented by these changes as cyber frauds have surged dramatically; with employees working through 'home network', vulnerabilities are at its peak and cyber criminals are taking advantage of this opportunity, as phishing emails, trojans embedded in apps and websites and other scams are taking place at breakneck speeds, and attackers are well resourced, constantly evolving their modus operandi and using untraceable money laundering techniques; this has exposed a weak point in security of financial institutions, due to a lack of controls and the use of legacy systems as well as staff training within financial institutions,"<sup>36</sup>.

RBI has issued a cautionary notice regarding a new fraud using mobile numbers and SBI has uploaded the notice issued by RBI's Department of Supervision, Central Office Cyber Security & IT Risk Group (CSITE) on its website for its customers and according to the notice, a social engineering fraud using mobile numbers similar to banks' toll free number is underway; reliable inputs were received by the department, on a new modus operandi of social engineering frauds using mobile numbers resembling a Supervised Entity's (SE) Toll Free number and registering these mobile numbers in the name of that SE on caller identification mobile apps such as TrueCaller<sup>37</sup>. Suppose that a SE's toll free number is 1800 123 1234 (not an actual number). The fraudster obtains a number, say 800 123 1234, resembling the SE's toll-free number and registers successfully on the True caller app (or any caller identification application) as the toll free number of that SE<sup>38</sup>. Using this tactic the fraudster in this way get to the customer who receive and attend their calls during call baits the victims in such a ways that they end-up providing their sensitive information of their debit /credit card credentials like their complete name, username, date of birth, One time password (OTP) etc. using this credentials fraudsters get access to the victim's accounts entire details which he/she uses against the victim while carrying out fraudulent transactions. Cyber fraud and scams are certainly not the only type of crime to suffer the consequences of under-reporting and other challenges associated with reporting, but nevertheless, there is still a critical need to improve understandings and practices associated with this particular type of crime<sup>39</sup>.

Covid -19 lead to the setback to people where people lost their jobs and specially the middle class and lower income people suffered during this period and became vulnerable adding to their agony. During this pandemic people were lured for small loan amounts through the mobile apps which provided them microloan hassle free. This acted as a hope to such people which ended them into victimization of fraudulent transactions. The modus operandi, the CID said they found each company possessed several

<sup>35</sup> Bryan Seely, "Cyber Fraud: The Web of Lies", ISBN: 978-1-533-15677-8, 2016, Pg. 8

<sup>36</sup> <https://www.livemint.com/industry/banking/how-covid-19-has-increased-the-pressure-on-banks-to-combat-cyber-frauds-11602642338591.html> reported on 14th October, 2020, accessed in February, 2021

<sup>37</sup> <https://www.financialexpress.com/money/alert-rbi-cautions-against-fraud-using-mobile-numbers-similar-to-banks-toll-free-number/2166212/> reported on 9<sup>th</sup> January, 2021, accessed in February, 2021

<sup>38</sup> Ibid

<sup>39</sup> Mark Button & Cassandra Cross, "Cyber Frauds, Scams and their Victims", 1<sup>st</sup> published 2017 by Routledge. Pg. 2

microloan apps of their own and on installation, users were made to part with details of PAN, Aadhaar, bank account number among others and grant permission for accessing SMSes, call logs, camera and storage on the phone<sup>40</sup>. The data provided by the National Payments Corporation of India (NPCI) shows that in September, transactions based on Unified Payments Interface (UPI) hit a volume of over 180 crores — nearly double the 99.9 crores volume recorded in April and total transactions have additionally reached Rs. 3, 29,027 crores; in all this transaction platforms including Google Pay, Paytm, and PhonePe also been a significantly increased and adapted and as a result, scams have also increased alongside<sup>41</sup>. Over 2.9 lakh cyber security incidents related to digital banking were reported in 2020, as per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 1, 59,761; 2, 46,514 and 2, 90,445 cyber security incidents pertaining to digital banking were reported during 2018, 2019 and 2020, respectively; the percentage rise in digital transactions is 46 per cent in 2020 in comparison to 2018-19; and the numbers of digital transactions have increased from 3,134 crore in the financial year (FY) 2018-19 to 4,572 crore in FY 2019-20<sup>42</sup>. During February 2020 till date people have shifted more from offline banking to net banking using bank sites or the apps which are available for this purpose like UPI, Google Pay, Amazon Pay, phonepe etc. which are used by major chunk of the people. People during this pandemic shifted to this easy mode of transactions which gave them flexibility for digital transactions hassle free at home, but it also being read in news and reported under various sources that such platform left the people at vulnerable end. As this platforms are not regulated under any of the regulations specifically.

During this entire period the spam calls and pesky calls were reported at high rate where the sensitive information were asked to the customers leading to them at hands of fraudsters. As digital transactions are adopted easily but people are not that vigilant and not aware about such tactics used which leads them to indulgence in victimization. Lots of cases were reported for such banking digital frauds in this pandemic period and how long this will go is still not known. To address the nuisance of pesky calls and messages as well as to make digital transactions secure and check financial frauds, the government has been proposed to impose a financial penalty against telemarketers including disconnection of resources in case of repetitive violations<sup>43</sup>. The governance of this sector is well dealt soon by the government laying down stricter provisions for the service provider of such apps and regulations of not only app's but also the banks itself incorporating into its legislation the digital transactions amendments. Legislation is not always the solution to the problem unless it is enforced, and in some cases, there may be a requirement to use certain mechanisms to ensure that the legislation serves its stated purpose(s) and having the legislative and regulatory framework is not sufficient to ensure that a corrupt officer or a fraudster would be brought to justice because existing legislation may not be enforced for various reasons<sup>44</sup> due to scattered rules and regulations having loopholes it becomes complex to implement.

### ***Money laundering***

Money laundering has its various facet that is connected with other crimes which are in different forms like fraud, again fraud is varied areas like tax evasions, black money, and also involve in financing terrorism. In money laundering the money is from illegal activities which is also called as 'hawala'. The tainted money is projected as clean money through intricate processes of placement,

<sup>40</sup> <https://www.ndtv.com/india-news/karnataka-police-busts-fraud-using-mobile-based-loan-apps-2343309> reported on 25th December, 2020 accessed in February, 2021

<sup>41</sup> <https://gadgets.ndtv.com/internet/features/digital-payments-paytm-kyc-google-pay-frauds-india-coronavirus-outbreak-2307236> reported on 8<sup>th</sup> October, 2020, accessed on February, 2021

<sup>42</sup> [https://www.business-standard.com/article/finance/over-290-000-cyber-security-incidents-related-to-banking-reported-in-2020-121020401220\\_1.html](https://www.business-standard.com/article/finance/over-290-000-cyber-security-incidents-related-to-banking-reported-in-2020-121020401220_1.html) reported on 4th February, 2021

<sup>43</sup> <https://www.financialexpress.com/industry/technology/govt-to-set-up-digital-intelligence-unit-to-tackle-pesky-calls-financial-frauds/2195446/> reported on 16<sup>th</sup> February, 2021

<sup>44</sup> Maria Krambia-Kapardis, "Corporate Fraud and Corruption A Holistic Approach to Preventing Financial Crises" 1<sup>st</sup> published 2016 by Palgrave MacMillan, Pg. 137



layering and laundering<sup>45</sup>. The operational principles of money laundering are a three-stage process which require, first, moving the funds away from any direct association with crime; second, disguising the trail to foil pursuit; and, third, making the money available to criminals once again while keeping its source secret<sup>46</sup>. Money laundering is a challenge from many years which in past used to take place through persons in offline modes but because of technology development online transaction are done through electronic modes which becomes more complex and beneficial for culprits. India being the member country of Financial Action Task Force (FAFT) which is global watchdog of money laundering and countering the financing of terrorism. India had observed the recommendation and implemented the standardize framework set by FAFT. In FATF report, there is a “*Professional money laundering network (PMLN), which is a collection of associates or contacts working together to facilitate PML schemes and/or subcontract their services for specific tasks. These networks usually operate globally, and can include two or more PMLOs that work together. They may also operate as informal networks of individuals that provide the criminal client with a range of ML services. These interpersonal relationships are not always organized, and are often flexible in nature*”<sup>47</sup>. In this schemes they use money mules who transfer value through laundering, stolen money or transportation of goods or either using other merchandise of ML. These mules are recruited by criminals for the purpose of money laundering using platforms like online social media or through advertisement and such people are called as mule ‘herders’ and provided with lucrative offers in form of job.

Money laundering does not require international transactions; there are instances of purely domestic laundering<sup>48</sup>. To control the illegal activity of money laundering, the government of India came with the legislation of Prevention of Money Laundering Act, 2002 (PMLA) to curb the illegal transactions with PMLA, RBI and SEBI. The PML Act, was introduced to curb money laundering and also to attached property which was involve in such transactions with an objective to deal with serious issues of money laundering affecting Indian financial system. Under this regulation the transaction are being kept on a check and the transactions could come to light with the assessment norms. Due to which the culprits started with using method of structuring or smurfing which means breakdown the cash deposits amount below the restricted limit as specified under the law. Smurfing is the breakdown of large sums of money into (well) below threshold chunks and distributing it across multiple depositors who use multiple accounts to avoid unwanted attention; to detect smurfing, one needs to zoom out from the micro event of the single transaction and take into consideration a range (or history) of transactions, preferably across a number of accounts potentially associated with a number of account holders.<sup>49</sup>. This modus operandi response is one, in which the financial institutions created to detect smurfing, or structuring. Herein a point is to be noted that, there should be some more dynamic rules, supplementary formal laws which can fix smurfing threshold of such cash deposits. In this entire smurfing transfer, the amount below threshold limit specified is transferred breaking them into small amount or transferred in small amount in different banks which becomes very safe for them to avoid the clutches of the law.

Customer due diligence (CDD) is one of the initiative of RBI which is important in various banking transactions which take place. This CDD helps to know their customers well based on their transactions, so that they can be identified and can be categorized into low risk, medium risk and high risk customer categories. This categorization of customers at bank level will help to tackle risk associated with account holder/customer and also to see the compliance under laws, regulations applicable to them are followed and help to detect fraud at early stage for any violation or non-compliances of any rules and regulations by customer at internal level of bank and taking care of

<sup>45</sup> Praveen Kumar, “Money Laundering in India: Concepts, Effects and Legislation”, J International Journal of Research, Vol. 3, Issue: 7, July:2015 also available at [http://www.raijmr.com/ijrhrs/wp-content/uploads/2017/11/IJRHS\\_2015\\_vol03\\_issue\\_07\\_11.pdf](http://www.raijmr.com/ijrhrs/wp-content/uploads/2017/11/IJRHS_2015_vol03_issue_07_11.pdf).

<sup>46</sup> Ibid.

<sup>47</sup> FATF Report Professional Money Laundering, July 2018, available at <http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf> accessed in February, 2021

<sup>48</sup> Money Laundering: Methods and Markets available at [https://piie.com/publications/chapters\\_preview/381/3iie3705.pdf](https://piie.com/publications/chapters_preview/381/3iie3705.pdf) accessed in February, 2021

<sup>49</sup> Derek Chau, Maarten van and Dijck Nemcsik, “Anti-Money Laundering Transaction Monitoring Systems Implementation”, John Wiley & Sons, 2021. Pg. 23

operational level of banking system also. The employers of the banks need to alert and should cross check the identification of customers transactions sensing the risk involved based on KYC norms. The employee needs to be check on the internal policies and code of conduct laying down standard working compliances and employer need to alert and equipped with assessment and evaluation of its staff that they don't involve in unfair modes adopted like bribery, corruption and embezzlement etc. This compliance will help to identify the fraudster who are involve in banking frauds and money laundering. Standing Committee, 2012 had Finance examining for PML (Amendment) Bill 2011, wherein it's reported that, black money is also generated by illegal mining and other activities through use of cash transactions in form of bribes and corruption. PML (Amendment) Act, 2012, had enlarged the definition of offences of money-laundering which had covered various activities like concealment, acquisition, possession and use of proceeds of crime as criminal activities, further it had removed then limit of Rs. 5 lakh fine under the Act<sup>50</sup>. In the case of M/S Mahanivesh Oils & Foods Pvt., the Delhi High court had observed:

*"The 2013 Amendment to Section 3 of the Act by virtue of which the words "process or activity connected with proceeds of crime and projecting it as untainted property" were substituted by the words "any process or activity connected with proceeds of crime including concealment, possession, acquisition or use and projecting or claiming it as untainted property". The words "concealment, possession, acquisition or use" must be read in the context of the process or activity of money-laundering and this is over once the money is laundered and integrated into the economy. Thus, a person concealing or coming into possession or bringing proceeds of crime to use would have committed the offence of money-laundering when he came into possession or concealed or used the proceeds of crime. For any offence of money-laundering to be alleged, such acts must have been done after the Act was brought in force. The proceeds of crime which had come into possession and projected and claimed as untainted prior to the Act coming into force, would be outside the sweep of the Act".<sup>51</sup>*

The 2013 amendment also introduce the concept of 'reporting entity' to include therein a banking company, financial institution, intermediary or a person carrying on a designated business or profession<sup>52</sup>. Even though the act was amendment still there were cases of non-compliance by various companies and business. In July 2015, the HKMA took disciplinary action against SBI, Hong Kong Branch (SBI HK) for breaches of the AMLO. The HKMA found that SBI HK failed to: (i) carry out CDD measures before establishing business relationships with customers; (ii) continuously monitor its business relationships; (iii) establish and maintain effective procedures for determining whether its customers or their beneficial owners (BOs) were politically exposed persons (PEPs); and (iv) establish effective procedures regarding CDD and continuous monitoring of business relationships<sup>53</sup>. Current practice is to have such dynamic rules supplementary to the fixed rules, and the fixed cash deposit threshold rule acts as a safety blanket, whilst the dynamic rule deals with those schemes that seek to circumvent the (known) fixed threshold rule<sup>54</sup>. Indian is very fertile for corruption, corrupt practices and illegal activities through which money is earned and this money is kept in different banks or international banks using money laundering scheme. Money laundering is a financial threat to nation when such money is used in against security of the country or in terrorist activities which raises question on regulations of such transactions. The acceptance level with regard to the reporting function of banks was low (2.71±1.19); about 68.3 per cent expressed that banks should not disclose the details of their transactions to any third party, including financial intelligence units; some showed reluctance (40.9 per cent) to perform certain transactions through banks if the transactions were reportable and few even expressed that they may prefer to close the account in case their transactions got reported (34.6 per

<sup>50</sup>The Prevention of Money-Laundering (Amendment) Bill, 2011 available at [https://www.prsindia.org/sites/default/files/bill\\_files/Prevention\\_of\\_Money\\_Laundering\\_Amendment\\_Bill\\_2011.pdf](https://www.prsindia.org/sites/default/files/bill_files/Prevention_of_Money_Laundering_Amendment_Bill_2011.pdf) accessed February, 2021

<sup>51</sup> M/S Mahanivesh Oils & Foods Pvt. vs Directorate Of Enforcement on 25 January, 2016

<sup>52</sup>Supra Note No. 51

<sup>53</sup> Arun Srivastava, Mark Simpson, Richard Powell, "International Guide to Money Laundering Law and Practice", 5<sup>th</sup> Edn. Published by Bloomsbury Professional, 2019. Pg. 1002

<sup>54</sup> Supra Note No. 50

cent)<sup>55</sup>. Above 50 per cent of the participants felt that banks should not disclose the details of their transactions to any third party, including income tax officials and financial intelligence units<sup>56</sup>. Despite the lack of academic or technical guidance, the CDD procedures are at the center of the AML/CFT discussions. Unlike screening of customers, monitoring of transactions or internal risk assessment, any changes in the CDD measures directly affect the consumers' experience and as confirmed by the FATF, onboarding processes have direct implications for the financial inclusion:

[...] rigid CDD requirements that insist on government-issued identification documents, adopted by some countries or financial institutions, have acted as barriers to these disadvantaged populations obtaining access to the formal financial system (FATF, 2017)<sup>57</sup>.

FATF (FATF Recommendation 10) uses the term "customer due diligence" in international standards while also mentioning "e-KYC" or "KYC/CDD requirements" in its financial inclusion and AML/CFT Guidance (FATF, 2017)<sup>58</sup>. The benefits of implementing the Recommendations of FATF were highlighted, which was stated thus, in the following manner by the reports of the Indian government: (i) securing a more transparent and stable financial system that is more attractive to foreign investors, (ii) ensuring that financial institutions are not vulnerable to infiltration or abuse by organized crime groups, (iii) building the capacity to fight terrorism and trace terrorist money, (iv) meeting binding international obligations, and avoiding the risk of sanctions or other action by the international community, and (v) avoiding becoming a haven for criminals<sup>59</sup>. In 2019, Finance Act, 2019, brought about important amendments of PML Act by insertion of explanations to the sections under the act removing the ambiguity which was there previously in those sections. This explanation tried to provide certainty to the sections increasing the scope of offences that are covered under the Act dealing under section 3 offence of money laundering<sup>60</sup>.

The year 2021 is when the next mutual evaluation by the FATF is scheduled (Financial Action Task Force, 2019) and with the next evaluation on the horizon, there have been suggestions to make ML a "stand-alone" offence (Pandey, 2019)<sup>61</sup>. Due to the ongoing Covid-19 pandemic from 2020 till now, economies worldwide are being affected and, criminals endure to abuse these crisis situation for financial gain. FATF mutual evaluation of India's anti-money laundering regime and legal measures

<sup>55</sup> Viritha B. Mariappan V. , (2016),"Anti-money laundering practices in banks: customer's awareness and acceptance in India", Journal of Money Laundering Control, Vol. 19 Iss 3 pp. 278 - 290

<sup>56</sup> Ibid

<sup>57</sup> Shust, P.M. and Dostov, V. (2020), "Implementing innovative customer due diligence: proposal for universal model", Journal of Money Laundering Control, Vol. 23 No. 4, pp. 871-884.

<sup>58</sup> Pavel M. Shust and Victor Dostov, "Implementing innovative customer due diligence: proposal for universal model" available at <https://www.emerald.com/insight/content/doi/10.1108/JMLC-01-2020-0007/full/pdf?title=implementing-innovative-customer-due-diligence-proposal-for-universal-model>

<sup>59</sup> Shannu Narayan, "Anti-Money Laundering Law in India: A 'Glocalization' Model", Statute Law Review, 2018, Vol. 00, No. 00, 0–12 <https://doi.org/10.1093/slr/hmy005>

<sup>60</sup> Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the [proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming] it as untainted property shall be guilty of offence of money-laundering.

[Explanation.--For the removal of doubts, it is hereby clarified that,--

(i) a person shall be guilty of offence of money-laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime, namely:--

(a) concealment; or

(b) possession; or

(c) acquisition; or

(d) use; or

(e) projecting as untainted property; or

(f) claiming as untainted property,

in any manner whatsoever;

(ii) the process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or claiming it as untainted property in any manner whatsoever.]

<sup>61</sup> Sameer Sharma, "Independence and temporality: examining the PMLA in " Journal of Money Laundering Control Vol. 23 No. 1, 2020 pp. 208-223 available at <https://www.emerald.com/insight/publication/issn/1368-5201>

framed to check financial crimes, in India was scheduled last year in 2020, but was postponed to 2021. The outcomes from a mutual evaluation have a direct impact on its citizens' and businesses' abilities to carry out cross-border financial transactions and poor outcome can have a negative impact on its position in the global economy<sup>62</sup>. The FATF meet held in February 2021 wherein they discussed ongoing key issues which includes digitalisation, which has the potential to make anti-money laundering and counter-terrorist financing (AML/CFT) action more effective and efficient and in particular, agreed to start new work on digital transformation of AML/CFT for operational agencies<sup>63</sup>. The FATF's mutual evaluations, as well as high-profile examples of abuse, demonstrate that criminals are still able to hide their illicit assets behind anonymous or complex legal structures and also discussed the preliminary findings in its ongoing work to overcoming the challenges linked to the effective recovery of criminals' assets, tackle money laundering from environmental crimes and the financing of ethnically and racially motivated terrorism.<sup>64</sup> According to the last report of FATF report of 2019-2020, it was stated that during the FATF's 12-month review of the implementations of the FATF, standards for virtual assets and virtual asset service providers, 25 jurisdictions reported that they were now undertaking a risk-based approach to supervision of VASPs<sup>65</sup>. Jurisdictions under augmented monitoring are aggressively working with the FATF to address strategic deficiencies in their systems to counter money laundering, terrorist financing, and proliferation financing and they came with increased monitoring, that means those countries who has stanch to resolve rapidly their strategic deficiencies and worked on FATF recommendation within timeframes set by it which were subject to check and evaluation by FATF. With the increase of technology and internet India has become a largest markets which is using biometrics-based CDD mechanisms. Here, biometric data (digital photo and a voice print) and ID information are stored in a central database coupled with an e-government website (ESIA). FATF has advised countries and their financial institutions to design AML/CFT measures that meet the goal of Financial Inclusion without compromising the measures that exist for the purpose of combating crime<sup>66</sup>. When an individual wants to go through remote CDD, he/she logs in ESIA using biometrics and login/password and authorizes the transfer of personal information to the financial institution, wherein the verification is done at the ESIA level, while confirmation is still based on knowledge (login/ password) and inherence (biometrics) and similar approach is taken in India where biometric/OTP verification is required in addition to presenting Aadhaar card (The Economic Times, 2018)<sup>67</sup>.

Banks and NBFCs required to carry out money laundering risk assessments periodically; and recent amendments to KYC directions mandate Regulated Entities (REs) to carry out the Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise periodically to identify, assess and take effective measures for mitigating its money laundering and terrorist financing risks for clients, countries or geographic areas, products, services, transactions or delivery channels; wherein the REs should take cognisance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time and REs will also apply a risk based approach (RBA) in mitigating and managing the identified risks and should have board approved policies, controls and procedures in this regard<sup>68</sup>. REs are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions and REs shall take steps to implement the provisions of the aforementioned Act and

<sup>62</sup> FATF Annual Report 2019-2020, available at <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF-annual-report-2019-2020.pdf> accessed March, 2021

<sup>63</sup> Outcomes FATF Plenary, 22, 24 and 25 February 2021, available at <https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-february-2021.html> accessed in March, 2021

<sup>64</sup> Ibid

<sup>65</sup> Supra Note No. 63

<sup>66</sup> Ehi Eric Esoimeme, "A comparative analysis of the prepaid card laws/regulations in Nigeria, the United Kingdom, the United States and India", *Journal of Money Laundering Control*, <https://doi.org/10.1108/JMLC-03-2017-0010>

<sup>67</sup> Supra Note No. 59

<sup>68</sup> Financial Stability Report July 2020 on "RBI Annex 3: Important Regulatory Measures, Regulatory package – COVID-19, 2020, available at

<https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/10ANNEX3A05D35B78D2743B18004824EDBC349E5.pdf>

Accessed March, 2021

Rules, including operational instructions issued in pursuance of such amendment(s)<sup>69</sup>. Obligations of Banking Companies, Financial Institutions, and Intermediaries Banking companies, financial institutions, and intermediaries are required under the PMLA to:

- (i) maintain records of all transactions for a period of 10 years as the offence of money laundering may surface years after it has been committed and keep track of the nature and value of transactions conducted be it single or 'a series of transactions';
- (ii) report suspicious transactions (STRs) to the concerned authority within a specified time period<sup>70</sup>.

PMLA law was enacted to deal with money laundering but had failed to address them and deal them, when they are done through sophisticated mode by high profile people in form of white collar crimes which impact the financial sectors and markets in India. Many cases are being reported to address relating tax evasions, banking frauds, benami transactions which uses method of money laundering to cleansing their money in their business. The provisions on duties of banking companies, financial institutions, and intermediaries are in compliance with the preventive obligations set by international legal instruments, which insist on record keeping and reporting requirement but in the Act we can see that there are flaws when it comes to enforcement<sup>71</sup>.

The first case in of money laundering and the money which were in foreign banks was file in 2009. In case of Ram Jethmalani<sup>72</sup>, Writ Petition (Civil) No.176 of 2009 was filed by Shri Ram Jethmalani and five others against the Union of India, RBI, SEBI, the Director of Directorate of Enforcement and the Chairman, Central Board of Direct Taxes, Department of Revenue, Ministry of Finance, Government of India, against the purported inaction of the Government to arrange for recovery of large sums of money deposited by Indian citizens in foreign banks and, in particular, in Swiss Banks. The SC ordered to constitute the Special Investigation Team (SIT), that were given responsibilities of investigation and initiation of proceeding against the culprits based on the kind of proceeding civil or criminal in nature and the SIT shall also be charged with the responsibility of preparing a comprehensive action plan, including the creation of necessary institutional structures that can enable and strengthen the country's battle against generation of unaccounted monies, and their stashing away in foreign banks or in various forms domestically<sup>73</sup>. The SIT was constituted in 2014 to investigate and curb generation of black money stashed abroad and report to the SC. Importantly, the SIT considered its mandate to include investigating the revelations in the Panama Papers concerning India. The SIT has inquired into the names of 415 Indians, reportedly including actors, businessmen and politicians, whose names have been linked to offshore companies floated by the Panama law firm Mossack Fonseca in tax havens around the world. However, to date, no major political figure in India has been prosecuted as a result of the disclosures in the Panama Papers<sup>74</sup>. The latest list, after similar ones came in the past like 'Swiss leaks' and the HSBC-list related to Indians, claims it has sourced data in connection to millions of documents which show heads of state, criminals and celebrities using "secret hideaways" in tax haven country of Panama<sup>75</sup>. In the 74 cases found actionable, the CBDT said invasive actions were taken in 62 cases with searches conducted in 50 cases, and surveys in 12 cases leading to detection of undisclosed foreign investments of about Rs.1140 crore (approx) and in 16 cases, criminal prosecution complaints have been filed in jurisdictional courts, which are at various stages of hearing<sup>76</sup>. No progress on the Panama Papers in which over 1800 Indian names had been disclosed<sup>77</sup> India, a country ranked by Transparency

<sup>69</sup> Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on December 18, 2020) available at [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=11566](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566) accessed March, 2021

<sup>70</sup> Supra Note No. 60

<sup>71</sup> Ibid

<sup>72</sup> Ram Jethmalani & Ors vs Union of India & Ors. on 23 September, 2011

<sup>73</sup> Ibid

<sup>74</sup> Supra Note Not. 54 Pg. 1017

<sup>75</sup> <https://www.thenewsminute.com/article/panama-papers-black-money-sit-investigate-500-indians-offshore-holdings-41167> reported on 4th April, 2016, accessed March, 2021

<sup>76</sup> <https://www.newindianexpress.com/nation/2018/jun/21/centre-probing-fresh-cases-of-panama-paper-leaks-1831566.html> reported in 21st June, 2018, accessed March, 2021

<sup>77</sup> <https://www.nationalheraldindia.com/india/no-progress-on-the-panama-papers-in-which-over-1800-indian-names-had-been-disclosed> reported on 5th April, 2020, accessed March, 2021

International in 2016 as 40/100 (with zero being most corrupt and 100 least corrupt) and 79th amongst 176 countries in the Corruption Perception Index, raises challenging legal issues relating to anti-money laundering (AML) regulations<sup>78</sup>.

In past few years we have seen lots of cases of money laundering in high profile people involving in it. This has raised the issues of governance in India on money laundering and governance systems taking place in companies and banks. NDTV started facing the music of law when in 2013, its minority shareholders of Securities Private Limited, approached SEBI with a sequences of complaints wherein this complaint exposed may Promoters and key managerial personnel's of NDTV involved in fudging accounts, money laundering by floating shell companies across the world which became real turning point, forcing Income Tax and Enforcement Directorate to act when the NDA Government came to power<sup>79</sup>. Laundering of US \$20 million by the "letter box shell company" "NDTV Networks Plc., U.K." owned by another letter box shell company "NDTV Network BV, Netherlands" owned by NDTV Ltd., India; Laundering of US \$100 million by NDTV Network Plc., U.K. received from shady transaction of alleged sale "Step Up Coupons" and "Bonds sales" but NDTV did not disclose the details of its hidden investors; Laundering of US \$150 million by NDTV Network BV, Netherlands in the garb of alleged sale of "26 indirect stake" of NDTV Network Plc., U.K. allegedly to NBCU Inc., USA, a subsidiary of GE Inc., USA; Laundering of US \$117 million for sale of "NDTV Imagine" allegedly to GE Corp. Inc., USA subsidiary; Laundering of US \$40 million by NDTV Network Plc., U.K. in the garb of alleged sale of "49% indirect stake" of letter box shell company NDTV Lifestyle Holdings Pvt. Ltd., India to Maxis Ltd., Malaysia and T. Ananda Krishnan, 2 of the accused in the 2G Scam case but received on behalf of P Chidambaram; and Laundering of Rs.40 crores by letter box shell company PR and RR Ltd., Cyprus owned wholly by Prannoy Roy and Radhika Roy for clandestinely purchasing beach house "Resort Aman Kini" in Goa, India<sup>80</sup>. SEBI shut their eyes on NDTV's money laundering and siphoning by promoters; the petition filed by QSL (minority shareholder) before the Delhi HC wherein the ED and DG (Investigation) Income Tax are parties, it is clearly spelt out that PMLA should be invoked against RRPR Holding P Ltd. also as it has committed various violations covered under IPC, SEBI Act and Money Laundering<sup>81</sup>. The CEO of the company admitted the fraud happened in the company through shell companies' worth of 150 Million dollars in June, 2016 after that confession ED registered cases under PMLA Act for money laundering. In this entire fraud the culprits were charge under Income Tax Act, PMLA, RBI and SEBI Act. According to RBI estimates, the top 30 loan defaulters currently account for one-third of the total gross NPAs of PSU banks; country's top five PSU banks had outstanding's of Rs 4.87 lakh crore to just 44 borrowers, if borrowers were to be categorized in terms of those having outstanding's of over Rs 5,000 crore and these businesses include Essar, Reliance ADAG, Jaiprakash Associates, Adani's, GVK, GMR and Lanco which are stress problem with fairly endemic<sup>82</sup>.

In 2019 amendment was done PML (Maintenance of Records) which is the 3<sup>rd</sup> amendment in this behalf for the maintenance of records. This amendment has inserted digital KYC<sup>83</sup>, about Aadhaar number etc. With the advancement of technology and e-banking and online transactions this was needed. RBI in January 2020 issued a circular notified that their need to be changes made to the Master Direction on Know Your Customer ("MD-KYC") of 2016, so that the PMLA Rules which were amended could be incorporated dealing with digital KYC, equivalent e-documents, Video based

<sup>78</sup> Supra Note No. 54. Pg. 1016

<sup>79</sup> Sree Iyer, "NDTV Frauds V 2.0 - The Real Culprit: A completely revamped version that shows the extent to which NDTV and a Cabal will stoop to hide a saga of Money Laundering, Tax Evasion and Stock Manipulation.", 2<sup>nd</sup> edn. Kindle version, self-published book in India, 2018.

<sup>80</sup> Ibid

<sup>81</sup> Ibid

<sup>82</sup> <https://www.nationalheraldindia.com/india/no-progress-on-the-panama-papers-in-which-over-1800-indian-names-had-been-disclosed> reported on 5th April, 2020, accessed March, 2021

<sup>83</sup> "digital KYC" means the capturing live photo of the client and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the reporting entity as per the provisions contained in the Act; available at <http://egazette.nic.in/WriteReadData/2019/210818.pdf> accessed in March, 2021

Customer Identification Process (V-CIP), for undertaking CDD, enhanced due diligence through - Accounts of non-face-to-face customers (other than Aadhaar OTP based on-boarding) and digital KYC Process<sup>84</sup>. RBI further update the Master direction in March, 2020 dealing with small account that shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government<sup>85</sup> as due to impact of Covid-19 which forced the country in compulsory lockdown which force people for online transaction. Again in April, 2020, Money Laundering and Terrorist Financing Risk Assessment by REs, so that risk assessment' exercise periodically is carried out to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. during the pandemic<sup>86</sup>. FATF (2020b) points to an increase in ML and TF risks stemming from Covid-19-related crime, which could include (i) increased misuse of online financial services and virtual assets to move and conceal illicit funds; and (ii) possible corruption connected with governmental stimulus funds or international financial assistance<sup>87</sup>. Financial Services Information Sharing and Analysis Center (2020) identified over 1,500 high-risk domains (i.e. those likely to have been set up by threat actors) created on or after 1 January 2020 containing both a Covid-19 and financial theme and; Google (2020), meanwhile, reported 18 million daily malware or phishing emails related to Covid-19 in early April 2020, which was in addition to more than 240 million Covid-19-related daily spam messages<sup>88</sup>.

The process of attaching assets worth hundreds of crores in the money laundering probe into several bank fraud cases has slowed down due to the Covid-19 lockdown and ED agency is also pursuing many other bank fraud cases involving over ₹10,000 crore, wherein the CBI had registered more than 40 cases that were to be taken by the ED<sup>89</sup>. As the pandemic Covid-19 is going to last for the longer period, RBI in December, 2020 further amended to keep the check on CDD procedure under Master Direction wherein 'CDD Procedure and sharing KYC information with Central KYC Records Registry' has to be kept by the banks<sup>90</sup>. ED had raided a Delhi-based company and is probing two other entities in connection with a money laundering case linked to alleged bank loan frauds of over ₹ 800 crore wherein SBBEL had diverted the loan funds through its sister units and also by employing the modus operandi of showing bogus and fictitious sale/purchase transactions"<sup>91</sup>. ED had arrested two directors of a Tamil Nadu-based company in an alleged money laundering case worth ₹ 325 crore linked to a bank fraud case and in probe it was found that, the accused "in collusion with the valuers availed loans from erstwhile Corporation Bank (now Union Bank of India) on the basis of inflated value of the properties offered as collateral and indulged in willful diversion of funds through various group account"<sup>92</sup>. ED had attached seven sugar mills worth over ₹ 1,097 crore in a money laundering case against former Uttar Pradesh BSP MLC Mohammed Iqbal and his family wherein they incorporated 7 companies in 2011, the agency further said that, "These mills were acquired by the accused "through laundering of illegitimate money through various shell companies having dummy directors and sham transactions,"<sup>93</sup>. ED had attached assets worth over ₹ 35 crore belonging to daughter and son-in-law of former Union Home Minister Sushil Kumar Shinde in a money laundering case linked to an alleged

<sup>84</sup> Master Direction - Know Your Customer (KYC) Direction, 2016, available at <https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607> accessed in March, 2021

<sup>85</sup> Ibid

<sup>86</sup> Ibid

<sup>87</sup> Juan Carlos Crisanto and Jermy Prenio, "Financial crime in times of Covid-19 – AML and cyber resilience measures", Financial Stability Institution, ISSN 2708-1117 (online) ISBN 978-92-9259-384-1 (online), May, 2020. Available at <https://www.bis.org/fsi/fsibriefs7.pdf> accessed in March, 2021

<sup>88</sup> Ibid

<sup>89</sup> <https://www.thehindu.com/news/national/lockdown-slows-down-assets-attachment-in-money-laundering-cases/article31275315.ece> reported in April 2020, accessed in March, 2021

<sup>90</sup> Supra Note No. 85

<sup>91</sup> <https://www.ndtv.com/india-news/money-laundering-case-probe-agency-raids-delhi-firm-in-alleged-rs-800-crore-bank-fraud-case-2377636> reported in 24th February, 2021, accessed in March, 2021

<sup>92</sup> <https://www.ndtv.com/india-news/probe-agency-arrests-2-tamil-nadu-firms-directors-in-money-laundering-case-2385160> reported on 6th March, 2021, accessed in March, 2021

<sup>93</sup> <https://www.ndtv.com/india-news/enforcement-directorate-seizes-7-sugar-mills-in-money-laundering-case-against-former-up-mlc-2387031> reported on 9th March, 2021, accessed in March, 2021

bank fraud<sup>94</sup>. In the TRP case wherein households were bribed and induced to watch specific channels, which fraudulently enhanced the Television rating points (TRP) for the Television channel and on the basis of rigged TRP, the investigation revealed that Television channels namely Fakt Marathi, Box Cinema and Maha Movie, had entered into a criminal conspiracy to cheat and committed the offence of criminal breach of trust, forgery in order to gain wrongfully by manipulating Television Rating Points (TRPs) of these Television Channels and; ED the movable and immovable properties of the channels owners/entities have been attached to the tune of Rs. 32 Crore against the total Proceeds of Crime to the tune of Rs. 46.77 crore generated during the manipulation period of TRP of the channels under the PMLA, 2002<sup>95</sup>.

The global Anti-Money Laundering Market is expected to grow at a compound annual growth rate (CAGR) of 13.6% from 2019 to 2027 and the Asia Pacific region is expected to register the highest CAGR in the next few years owing to the rise in fraud and money laundering incidents in developing economies like in India and China<sup>96</sup>. The measure issues in curbing the offences of money laundering is due to jurisdictions issues and loopholes in governance nationally and internationally. Institutional limitations in many countries, including judicial and police systems, extradition arrangements, immigration, asset seizure, anti-money laundering, and anti-corruption laws are some of the issues that may have to be addressed; jurisdictional overlaps and less than adequate international co-ordination hamper actions against money launderers and as of now more than ninety jurisdictions offer the protection of bank secrecy laws which impose criminal sanctions on those who release information regarding clients' transactions<sup>97</sup>. Due to online banking transactions and adaptability of technology of e-banking makes it difficult for banks to monitor and assess the account activities of the clients creating complications for lay employee of banks.

The difficulties in exercising uniform regulation and oversight over a multitude of non-bank financial institutions such as exchange houses, check cashing services, insurers, mortgagors, brokers, importers, exporters and other trading companies, gold and precious metal dealers, casinos and express delivery services, makes it extremely difficult to detect money laundering<sup>98</sup>. If we look into the Indian governance provisions which is spread over various governing bodies who controls following procedures given under varied laws which are combating money laundering in various Acts, Regulation, Government policies and guidelines issues by different governing bodies within India and cross border financial transactions using online and offline mode. Money laundering is not only covered under PMLA, 2002 apart from it, other Acts Regulations and Guidelines are their like Income Tax Act, Customs Act, Foreign Exchange Management Act (FEMA), Companies Act, Benami Transactions (Prohibition) Act, SEBI, RBI etc. India is a developing country which is more prone to money laundering activities which gives inherent threats to the economy and also this money used in terrorist activities affecting the security of the country and requisite measures needed for prevention of crimes under money laundering umbrella. Money laundering is a huge concern which affects the economy of the country and also affects financial market and its activities are carried out across globe which is a concern nationally and internationally. Money laundering activities has no border and are internationalized leading complexity of jurisdictions. Crime doesn't stop at borders, good cooperation between national supervisors therefore plays a key role in mitigating cross-border ML/TF risks<sup>99</sup>. Money laundering is a sophisticated complex process which are committed in large scale and the cases are already highlighted above. Money laundering affects the Indian economy which also a big loss to the Indian financial market. Though we have many statues to govern this crimes but still the number of

<sup>94</sup> <https://www.ndtv.com/india-news/ed-attaches-assets-of-sushil-kumar-shindes-daughter-her-husband-under-pmla-2391464> reported on 15th March, 2021, accessed in March, 2021

<sup>95</sup> <https://economictimes.indiatimes.com/news/politics-and-nation/ed-attaches-rs-32-cr-assets-of-tv-channels-in-trp-case/articleshow/81553810.cms> reported on 18 March, 2021, accessed in March, 2021

<sup>96</sup> <https://www.globenewswire.com/news-release/2021/01/21/2161853/0/en/Anti-Money-Laundering-Market-Size-Will-Reach-USD-2385-8-Million-by-2026-Facts-Factors.html>, reported on 21<sup>st</sup> January, 2021, accessed in March 2021

<sup>97</sup> Report of The Technical Group on Market Integrity, available at <https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=280#c2>, accessed in March, 2021

<sup>98</sup> Ibid

<sup>99</sup> Supra Note No. 63



cases are increasing every year. Government need to have a mechanism which can curb, investigate and punish the culprits so that this crimes comes to halt.

### Conclusion

Financial systemic frauds had impacted pre and post pandemic in financial market. Banking regulation are working but still we don't have a systemic method to detect banking frauds using urbane modes with helps of insider of the banks. Money laundering also somewhere in many cases take place using the banks to transfer the illegal money by not getting highlights in transactions. With advancement of technology government need to have a mechanism wherein track can be kept of all financial transactions and timely they could be detected using the database. Time to time RBI and SEBI came with their notification and directives in this regard but implementation is lagging which leads to commission of such systemic frauds. We need to have a investigating authorities who should have powers to resolve the matters high handedly so that country does not have to bear the economic loss to the Indian economic financial market which can be used for the development of the country.

### References Books and Articles.

1. Black Money, White Paper, "Ministry of Finance and Department of Revenue" May 2012.
2. Lovejit kaur, "PNB SCAM: Shining Diamond Trader Took Away PNB's Shine" ISSN: 2321-9939, Volume 8, Issue 1.
3. S. Gayathri and T. Mangaiyarkarasi, "A Critical Analysis of the Punjab National Bank Scam and Its Implications", Volume 119 No. 12 2018, 14853-14866 ISSN: 1314-3395.
4. G. Singh, S. Srivastav, A. Gupta and V. Garg, "An Analysis of Financial Fraud through PNB Bank Scam and its technical Implications," 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2020.
5. Maria Krambia-Kapardis, "Corporate Fraud and Corruption A Holistic Approach to Preventing Financial Crises" 1st published 2016 by Palgrave MacMillan.
6. Bryan Seely, "Cyber Fraud: The Web of Lies", ISBN: 978-1-533-15677-8, 2016.
7. Mark Button & Cassandra Cross, "Cyber Frauds, Scams and their Victims", 1st published 2017 by Routledge.
8. Praveen Kumar, "Money Laundering in India: Concepts, Effects and Legislation", International Journal of Research, Vol. 3, Issue: 7, July, 2015.
9. Arun Srivastava, Mark Simpson, Richard Powell, "International Guide to Money Laundering Law and Practice", 5th Edn., Published by Bloomsbury Professional, 2019.
10. Derek Chau, Maarten van and Dijck Nemcsik, "Anti-Money Laundering Transaction Monitoring Systems Implementation", John Wiley & Sons, 2021.
11. Viritha B. Mariappan V. , (2016),"Anti-money laundering practices in banks: customer's awareness and acceptance in India", Journal of Money Laundering Control, Vol. 19 Issue 3.
12. Shust, P.M. and Dostov, V. (2020), "Implementing innovative customer due diligence: proposal for universal model", Journal of Money Laundering Control, Vol. 23 No. 4.
13. Shannu Narayan, "Anti-Money Laundering Law in India: A 'Glocalization' Model", Statute Law Review, 2018, Vol. 00, No. 00, 0-12.
14. Ehi Eric Esoimeme, "A comparative analysis of the prepaid card laws/regulations in Nigeria, the United Kingdom, the United States and India", Journal of Money Laundering Control, <https://doi.org/10.1108/JMLC-03-2017-0010>
15. Sree Iyer, "NDTV Frauds V 2.0 - The Real Culprit: A completely revamped version that shows the extent to which NDTV and a Cabal will stoop to hide a saga of Money Laundering, Tax Evasion and Stock Manipulation.", 2<sup>nd</sup> edn. Kindle version, self-published book in India, 2018.
16. Juan Carlos Crisanto and Jermy Prenio, "Financial crime in times of Covid-19 – AML and cyber resilience measures", Financial Stability Institution, ISSN 2708-1117, May, 2020.

### Reports

1. RBI Annual Report 2019-2020
2. RBI Annex 3: Important Regulatory Measures, Regulatory package – COVID-19, 24 Jul 2020, Financial Stability Report July 2020
3. Master Directions on Frauds – Classification and Reporting by commercial banks & select FIs
4. FATF-annual-report-2019-2020
5. Central Vigilance Commission, Vigeve Vani, quarterly Newsletter, Special Issue on Banking Sector, Oct-Dec 2019.