INTERNATIONAL JOURNAL OF
RECENT TRENDS IN MULTIDISCIPLINARY RESEARCH
May-June 2024, Vol 4(03), 13-17.
No: 2583-0368
ISSN

Rising Problems of Money Laundering in Cyber Plat Form

Sudesna Sarkar[1], Rijuka Roy Barman[2]
[1]BCOM. LLB. (H) [4th year], Amity Law School/ Amity University, Kolkata, West Bengal, India.
[2]BBA. LLB. (H) [4th year], Amity Law School/ Amity University Kolkata, West Bengal, India.

OPEN ACCESS
Article Citation:
Sudesna Sarkar[1], Rijuka Roy Barman[2], 'Rising Problems of Money Laundering in Cyber Plat Form", International Journal of Recent Trends in Multidisciplinary Research, May-June 2024, Vol 4(03), 13-17.

Publishedby5thDimension Research Publication

Abstract: Now a days, business is getting globalized. E-commerce is a very essential things in online trading platform. Without money business is not possible. Everything has a positive and negative site. Excessive money exchange attracts criminals. Crimes can be committed in cyber platform very efficiently without any evidence and traces. After Covid-19, committing financial fraud has increased. Criminals' detection becomes very difficult. It becomes very difficult in international aspect. This cyber fraud spreads in many countries though online. Several conferences are taken places. Various treaties are implemented in these regards. Still the problem remains unresolved. Sufficient domestic laws are in enforced to prevent this crime. How laws are applied and dealt to prevent and detect the cyber criminals and crimes are discussed to bring certainty.

Key Words: E-commerce, Information Technology Act, 2000, Customs, Treaties, UNCITRAL Model Law on Electronic Commerce, Computer Emergence Response Team, The Indian Evidence Act, 1872

1. Introduction

Money laundering has continued since ancient times. Now, everything is going online. After 2020, marketing and booking of services have increased in the online medium. Due to these, online payment is increased. Recently, various platforms have been generated for dealing with online platforms. Recently, various digital currencies have been generated for easy and quick online payment and money transactions. This online transaction greatly impacts the financial system and economic condition. Everything has a positive and negative impact. When the money transaction gets digital, the money laundering starts in the online platform. This type of crime is known as *'cyber-laundering.'* In ancient times, there was no proper infrastructure for detecting cybercriminals. Now, there are proper infrastructure and legal frameworks to prevent and give punishment to criminals. Still, the detection of criminals for cyber laundering is challenging. Various problems need to be faced during the process of investigation. Territorial and evidentiary are two crucial problems that create huge obstructions in carrying out the investigation. This problem is happening all over the world. Technology advancements have also led to a rise in criminal activity. Wealth transfer from one country to another and converting black money into white have become convenient by the electronic medium. Money transfers for illegal become very easy through online mediums. The flawless internet access attracts criminals to commit these kinds of crimes.

2. Cyber Crime

Cybercrime is a modern form of criminal activity. This definition encompasses any unlawful activity carried out through computers, the Internet, or other technologies authorized by the Information Technology Act. Cybercrime is the most prevalent and destructive type of crime in contemporary India.

Technically proficient criminals use the internet to commit several illegal activities. Using a more expansive definition, cybercrime can be defined as any illicit behaviour in which one can utilize a computer, the internet, or both as a target, a tool, or both. Examples include cyberterrorism, cyberstalking, email spoofing, email bombing, cyber pornography, cyber defamation, and other newly created cybercrimes. Some conventional crimes may also be classified as cybercrimes if they are committed using a computer or the Internet.[3]

3. E-Commerce

Buying and selling goods and services over an electronic network—most commonly the Internet—is known as e-commerce. It has gained popularity due to increased customer demand and convenience in online transactions. The main forms of e-commerce include business-to-business (B2B), business-to-consumer (B2C), business-to-government (B2G), consumer to-consumer (C2C), and mobile commerce (m-trade). The Information Technology (IT) Act 2000 became the first e-trade law in India. In 1997, the United Nations General Assembly approved a model law on digital trade for uniformity in regulation and substitutes for data storage and transmission technologies based on paper. The IT Act aims to provide legal recognition for transactions through digital information exchange and other electronic communication, also known as digital trade (e-trade).[5]

4. Challenges in the Detection of Cyber-Laundering

Jurisdictional Challenges: In the legal field, jurisdiction is very important to resolve a dispute. A court should have jurisdiction while deciding a case. The court cannot handle the case if it lacks jurisdiction. There is no limitation of jurisdiction about e-commerce. It is not necessary for the offender and the victim to live in the same nation to commit a cybercrime. There are no geographical boundaries in cyberspace. It becomes very flexible for hackers, virus attackers, software pirates and crooks to commit crime in cyber platform. In the international aspect, jurisdiction plays a crucial role for continuing investigations and finding out the criminal. There are no uniform laws in international aspects. The first treaty related to cyber offenses was 'The Convention on Cybercrime' on 23rd November 2001 in Budapest. It was signed by twenty-one member states. This treaty discussed the procedural power, the jurisdiction of the court, adjudication and protection of cybercrime, and common criminal policy, The International Cybercrime Treaty came into force after the U.S. World Trade Center attack on 11th September 2001. This treaty was signed by the USA, UK, Canada, South Africa etc. This treaty removed the uncertainty in the realm of cyberspace. Section 75 of The Information Technology Act, 2000 states that anyone, regardless of nationality can commit an infraction outside of India. This act also applies to such computers, computer systems, or computer networks that are involved in such crimes. The cooperation between the countries is required for investigation to solve these problems in the international aspect. Then only this territorial and jurisdictional can be removed.

Technology always has positive and negative sites. Due to the development of technology, there is easy of access to many things within a moment. It brings flexibility in business, jobs, and education as well as gives crime opportunities to criminals in an updated way. Due to the problem of jurisdiction, the criminals of cyber platforms become untraceable. In international law, treaties, and conventions are works as a law. But all treaties are not signed by all countries. So, the perpetrator and victim are situated in two countries. The perpetrator is situated in a country which does not sign a treaty in respect of which judgment is given. Then that judgment is not binding on that country. The perpetrator will remain untouched. Treaty should be signed by both countries for enforcing it. This is a crucial area in the international field. Customs and general principle are very less effective in such scenario. Twenty-Second G-7 Summit on Cybercrime (1996) highlighted the issue regarding the for prevention and investigation of cyber-terrorism to protect the privacy and communication. Paris Cyber Crime Conference (2000) raised the issue for establishment of International Criminal Tribunal to lay down jurisdiction in global aspect for handling the criminals. Updated technology is required for exchanging evidence between the countries for detecting criminals. All countries are not that much of developed for providing it [10]

Evidentiary challenges: This segment discusses the law of evidence for applying it to the Internet, based on the Indian Evidence Act of 1872 and the Information Technology Act of 2000. Most evidence used in internet-related litigation is computer-generated, making it important to define what a "computer" is. Any electronic, magnetic, optical, or other high-speed data processing system or device that can execute arithmetic, logic, and memory operations is called a computer.

The Indian Evidence Act of 1872 permits "copies" to be produced by "mechanical processes" or by "printing" uniformly, but it does not define a computer. Before analyzing the admissibility, proof, production, and effect of such evidence, it would be worthwhile to investigate the kinds of evidence produced by computers.

4.1 Types of Computer-generated evidence.

Computer-generated evidence can be classified into three types: *real evidence*, which is calculated or analyzed by the computer itself and information from other devices, such as built-in clocks or remote sensors; hearsay evidence, which is copies of human-provided information, such as drawn cheques and paying-in slips credited to a bank account; and derived evidence, which combines real evidence with human-provided information to create a composite record, typically treated as hearsay evidence.

Real evidence is tangible information that the tribunal of fact can obtain through its senses, such as a bank computer automatically calculating a customer's bank charges based on tariff, account transactions, and daily cleared credit balance. Hearsay evidence, on the other hand, is a combination of real evidence and human-provided information, such as individual cheques and paying-in entries. Lastly, derived evidence is a combination of real and human-provided information, often treated as hearsay evidence, to create a composite record. An example is the daily balance column in a bank statement, which uses both real and hearsay evidence.

To investigate the admissibility of these types of evidence, it is important to understand the nature of the threshold requirements required to admit these types of evidence.

4.2 Admissibility

This section looks at the admissibility of electronic evidence in court. Because computer-generated evidence is a relatively recent development, Indian law has yet to address it. Thus, while the emphasis is on the Indian Evidence Act,

positions in the United Kingdom and the United States of America are also examined, and references to the UNCITRAL Model Law on Electronic Commerce are included.

Science and technology have advanced to the point where video conferencing equipment can now be set up in the courtroom. In that case, the magistrate would record or dictate evidence in open court. If that is done, the requirements of sections 274 and 275 of the CrPC, which require the magistrate to take evidence in writing or by dictation in open court, will be fully met. However, there is one disadvantage to using this method. Because the witness is not in court, there may be difficulties if he commits contempt of court or perjuries himself and it is immediately discovered that he has perjured himself. As a result, as a matter of procedure, evidence by video conferencing in open court should only be taken if the witness is in a country with an extradition treaty with India, and the loss is considered contempt of court, and perjury is also punished.

4.3 Proof

Now that the admissibility case has been established, the inquiry shifts to the issue of document proof. It is well established that only documents produced and proved by a witness in court can be considered evidence.

The question now revolves around the authenticity of the electronic evidence, specifically whether the electronic record is authentic or how one can ensure the integrity of the system that generated the evidence. In addition, is the aforementioned record to be considered primary or secondary evidence? Is the electronic record original or a copy? These questions are important when considering how evidence should be treated in a proceeding.

4.4 Authenticity

A document's admissibility is one thing, but its probative value is quite another. The traditional rationale for authenticating a document is to ensure that the document is what it claims to be to establish a link between it and an individual. An example of authentication is the establishment of a link between a monthly computer-generated summary of account activity and the corresponding customer. Before the summary of the account can be considered relevant to a legal issue, it must be demonstrated that it is an authentic statement of transactions between the customer and the plaintiff. For the document to carry any evidential weight and conviction, it must be proven to be genuine. This can be accomplished by identifying the person to whom the document is addressed. Everyone who reads the writing can now trace it back to its issuer and signer and determine the text's origins beyond a reasonable doubt. Thus, a signature can be used to identify a person and link them to the content of a document.

Nowadays, it is common in legal literature to state that handwritten signatures and paper documents have been surpassed by technological advances. Every signature can be perfectly reproduced and copied innumerable times using modern instruments such as a scanner and plotter. The future of subscription will be a digital signature system, albeit with some technical cautions and a higher level of security.

4.5 Electronic Signature

Electronic signatures, a form of digital signature, gained popularity due to advancements in technology. These signatures are not based on written or embossed statements but are the result of encryption applied to specific data. Countries like the USA, Singapore, Malaysia, and Germany were among the first to pass laws addressing *Electronic Signatures*[20]. The Indian IT Act passed in 2000, established a public-key infrastructure for digital signatures using asymmetric key encryption and granted legal validity.

4.6 Best Evidence Rule

The Indian Evidence Act, amended by the IT Act, allows electronic documents to be considered primary evidence if they were produced during regular use, routinely fed into the computer during normal activities, and the computer was operational for most of the period. This provision resolves the issue of primary versus secondary evidence in electronic records, requiring the contents of the output to be authentic and have reasonable grounds to believe they are authentic. The destruction of originals could lead to court sympathy for electronic images, raising questions about the Best Evidence Rule in common law of evidence. The IT Act also ensures that the computer output containing the information was produced during regular use, routinely fed into the computer during normal activities, and the computer was operational for most of the period.

5. Case Study

Reserve Bank of India issued a circulation on 6th April institution India on Development and Regulatory policies on 6th April 2018 issued a statement policy to exercise the authority granted by Sections 45 JA and 45L of the RBI Act, 1934, Section 35A read in conjunction with Section 36 (1)(a), and Section 56 of the Banking Regulations Act, 1946. Paragraph 13 of this circular prohibits banks and other entities under RBI from providing the service of virtual currency. This virtual currency generates hacking and brings significant loss. This situation leads to money laundering and terrorist financing. This prohibition put an end to the business of virtual currency. There is no restriction on the dealing of virtual currency in India. All banks and entities under RBI also stopped accepting any virtual currency in exchange for the purchase of virtual currency.

The Supreme Court turned the prohibition and stated that there is a good impact of the trading of cryptocurrency in the market. The Inter-Ministerial Committee recommended the Crypto-token Regulation Bill 2018. But this is rejected as an extraordinary apparatus. The court specified that virtual currency is not considered normal cash. Under certain circumstances, it worked as cash. So, RBI needs to control these virtual currencies under the monetary system. This kind of circulation which is issued by RBI is illegal and unenforceable.

In the case of Hitesh Bhatia V. Kumar Vivekanand, the plaintiff has a business dealing in bitcoins. He takes the identity proof of every business purpose. He brought an allegation against the accused (Mr. Kumar Vivekanand), that he

purchased bitcoins. The transaction happened through an online portal such as 'Binance.' That Bitcoin transaction was considered illegal. Due to this, the plaintiff's account had been frozen. The plaintiff asked about the legality of money that was paid for purchasing the Bitcoin. The defendant admitted that all payments were 'scams' and he refused to return all the Bitcoins which was considered as cheating. The plaintiff submitted the allegations before the Station House Officer and the Data Protection Officer but they did not take any action. Considering this, the plaintiff used the Code of Criminal Procedure (Cr.P.C.) u/s.156(3). The investigation officer submitted that he received money from three different accounts in this transaction. A resident of Nagpur who filed a fraud complaint under sections 66C and 67 of the Information and Technology Act, 2000, contributed Rs. 6,00,000 of the total amounts. The plaintiff credited an additional Rs. 3,00,000 from the defendant. He received that amount from a person who resides in Telangana. He also registered an FIR for alleging cyber fraud. The remaining amount was transferred from the accused's account.

The court emphasized that the plaintiff submitted the screenshot of the WhatsApp conversation between them. The accused sent money intentionally through a prima facie account and had hidden the illegality of money from the plaintiff and transferred it against the sale of Bitcoin. He tried to encash it from the 'safe heaven' countries, where regulation is not proper. Due to this plaintiff suffered a wrongful loss. The Court held that a cognizable offense was committed under sections 403, 411, and 420 of the Indian penal code.24

6. Legal Framework for Cybercrimes

To combat cyber laundering and related cybercrimes, Indian authorities, have implemented cybersecurity measures, established financial regulations, and developed specialized units for cybercrime investigation. It's critical to keep up with the most recent cybersecurity risks and recommended practices to safeguard people and businesses against financial crimes such as cyber laundering. Some of the cybersecurity measures and initiatives that were taken in place are as follows: -

a) **National Cyber Security Policy (NCSP):** It aims to create a secure and resilient cyberspace environment. It outlines strategies for enhancing cybersecurity, protecting critical infrastructure, and promoting cybersecurity awareness and education.
b) **Indian Computer Emergency Response Team (CERT-In):** The national nodal organization in charge of handling cybersecurity events and providing early warning, incident detection, and response services. It also issues guidelines and advisories to various sectors to enhance cybersecurity.
c) **Cyber Coordination Centre (CyCord):** The Indian government established CyCord to coordinate responses to cyber threats and incidents across various government agencies and departments.
d) **Data Protection Laws:** This is an effort to improve data security and privacy and control the processing of personal data, India introduced the Personal Data Protection Bill.
e) **National Critical Information Infrastructure Protection Centre (NCIIPC):** Its main goal is to defend against cyber threats and attacks on the critical information infrastructure (CII) sectors, which include finance, energy, and transportation.
f) **Sectoral Computer Emergency Response Teams (CERTs):** Various sectors, including banking, power, and telecommunications, have their sectoral CERTs to monitor and respond to sector-specific cyber threats.

In addition to that, the Indian Government took initiatives to spread awareness of Cyber Laundering such as the

Information Security Education and Awareness (ISEA)_Program which focuses on raising cybersecurity awareness and providing training to individuals, organizations, and government personnel.

Cybersecurity Best Practices and Guidelines: The government and CERT-In regularly issue cybersecurity best practices and guidelines for various sectors, including banking, healthcare, and government. Further, they raise awareness through campaigns.

Cybersecurity Awareness Campaigns in which the government conducts cybersecurity awareness campaigns to educate the public and organizations about safe online practices and cyber threats. Efforts have been made to encourage research and development in the field of cybersecurity, with a focus on developing indigenous cybersecurity solutions.

7.Suggestion and Conclusion

It is clear from the discussion above that, among all other crimes, money laundering is a form of financial crime. Today, this crime has become a serious threat to society. Money laundering is a very traditional and old crime. Through money laundering black money can be turned into white money. Day by day, people become more dependent on online platforms. During COVID-19, the use of online platforms has increased so much. After COVID-19 it has a huge effect. Money laundering comes in online platforms when money transactions are increased in online mediums. In online platforms, it becomes very difficult to trace and deal with the criminals of cyber laundering due to various issues. In an online platform, the collection of evidence is very easy as well as difficult. Every transaction that happens in the online portal is recorded. At the same time, recorded evidence of online portals can be tampered with. Then it becomes difficult to collect evidence; nothing can be done without it. In an online portal, criminals and victims can be from the same country or two different countries. If the criminals and victims are of the same country, investigation and other proceedings become flexible. If they are from different countries, then it becomes very difficult to trace them. Because in this case international laws are involved. Every state has its sovereignty. There is a conflict of sovereignty in the application of international law for cybersecurity There are no uniform laws for dealing with these kinds of cybercriminals in cyberspace. So, the execution of treaties, and the evolution of customary international are required for the development and protection of people in cyberspace. From this, it is very clear that territorial and evidentiary issues are the major problems among others. There are proper structures and laws for dealing with criminals in cyberspace in India. The "Information Technology Act, 2000" was passed by India to address concerns about cyber platforms. This act supports India's privacy and data protection laws. But time is required for the changing and laying down of new rules in the international aspect. Governments of all states should take initiative and should be stricter in

these matters. Until or unless any uniform law comes into force cooperation between all the states should be increased for tracing cyber criminals.

Reference

[1] Tom Kellermann "Money Laundering in Cyberspace" WBFSWP 2 (2004)
[2] Rakesh Kumar Handa and Rizwan Ansari "Cyber-Laundering: An Emerging Challenge for Law Enforcement" 5 JVVI 81 (2022)
[3] Prof. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law", Kamal Law House, 2012
[4] Rajendra Madhukar Sarode, "Future of E-Commerce in India Challenges & Opportunities" 1(12) IJAR 646 (2015).
[5] Sumanjeet, "E-Commerce Laws In The Indian Perspective" available at: http://www.smsvaranasi.com/insight/e commerce_laws_in_the_indian_perspective.pdf (Visited on January 27, 2024).
[6] Dr. Viswanath Paranjape, Cyber Crimes & Law 135 (Central Law Agency, Allahabad 2nd edn. 2019)
[7] Dr. Viswanath Paranjape, Cyber Crimes & Law 139 (Central Law Agency, Allahabad 2nd edn. 2019)
[8] Information Technologies Act, 2000 (21 of 2000)
[9] Dr. Viswanath Paranjape, Cyber Crimes & Law 187 (Central Law Agency, Allahabad 2nd edn. 2019)
[10] Dr. Viswanath Paranjape, Cyber Crimes & Law 188 (Central Law Agency, Allahabad 2nd edn. 2019)
[11] Section 62, Expln. 2: " ..... [N]umber of documents made ... in case of printing...." (emphasis supplied)
[12] Peter Murphy A Practical Approach to Evidence, 1988, Blackstone Press, London, p. 186
[13] <http://www.uncitral.org/english/texts/electcom/ml-ec.htm>
[14] State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.
[15] Anupam Chakraborty v. State of Assam, 1984 Cr LJ 733.
[16] State of Bihar v. Radha Krishna Singh, AIR 1983 SC 684.
[17] C. McCormick Handbook of Law of Evidence 684-86 (3d Edn., E. Cleary 1984
[18] Ford Motor Credit Co. v. Swarens, 447 S.W.2d 53 (Ky. 1969)
[19] America Federal Rule of Evidence 803(6).
[20] <http://www.mit.gov.in/cyber.htm>
[21] Section 62, Indian Evidence Act, 1872.
[22] Section 63, Indian Evidence Act, 1872.
[23] Internet And Mobile Association of India V. Reserve Bank of India (2020) SCC 275
[24] Hitesh Bhatia V. Kumar Vivekanand (2021) 3207 of 2021
[25] All India Council for Technology, India, available at: Cyber Security | Government of India, All India Council for Technical Education (aicte-india.org) (Visited on February 22, 2024)
[26] Dr. Viswanath Paranjape, Cyber Crimes & Law, 68 (Central law Agency, Allahabad, 2nd edn., 2019)
[27] Reserve Bank of India, Chapter 9 Report of the Working Group on Electronic Ranking (January, 2011)
[28] Hollis Duncan "A Brief Primer on International Law and Cyberspace" CEIP 1 (2021)