Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/19868
DOI URL: http://dx.doi.org/10.21474/IJAR01/19868

RESEARCH ARTICLE

IMPACT OF ELECTRONIC PAYMENTSON MONEY LAUNDERING CASES IN INDIA

Sonika Bodake and Vineela Thera
Research Scholar, Department of Law, Sri Padmavati Mahila Visvavidyalayam, Tirupati, AP.

Manuscript Info

Manuscript History
Received: 08 September 2024
Final Accepted: 17 October 2024
Published: November 2024

Key words:-
Money Laundering, Electronic Device Smart Card Monetary Aggregate, Electronic Money Open Market Sales

Abstract

In recent years, there has been a lot of interest in the development of electronic money systems. Electronic money has the potential to simplify and lower the cost of small-value payments for both consumers and companies, potentially replacing cash as the primary means of payment in the future. A consumer keeps track of the money or "value" that they have accessible to them on their electronic device, which could be a prepaid card or a personal computer that they use to access a computer network such as the Internet. We refer to this record as electronic money. Such a change would have an impact on the effectiveness of monetary policy implementation. A better coordination of monetary and fiscal policy would be necessary, as well as adjustments to the central bank's operating aim, should the usage of e-money significantly reduce demand for reserves. Technology advancements have made it feasible to launder money obtained illegally through online bookies, casinos, and, most notably, the buying and selling of cryptocurrency.

Introduction:-

The electronic payment system is an operational network, regulated by regulations, rules and business standards, which connects clients' accounts in banks and enables the exchange of funds from those accounts electronically .This system enables the transfer of large sums of money in a short period of time without obstacles in the form of borders or continents, which makes it difficult to monitor the origin of electronic transfer .Electronic money (e-money) is the term for the retail payment sector that is seeing rapid innovation and information technology development. Due to the growing use of prepaid cards, e-purses, e-wire transfers of money orders, e-banking, and e-loans, this trend is having an impact on the banking sector.

The last ten year, there have been a "silent revolution" payment methods. Payment systems are transitioning from paper-based processes to electronic, real-time settlement and execution. By "real-time," it imply that payments are processed continuously, around-the-clock, rather than only periodically over the course of a few days or even an overnight period. Because they have faith in the financial system overall and in electronic operations specifically, consumers have generally been willing to adopt these new electronic technologies. However, because these significant changes have happened gradually and often in less evident or dramatic ways, this is a quiet revolution.

Money laundering is the process of concealing the origins of illicitly obtained funds to make them appear legitimate. It involves a series of transactions and activities that obscure the true source of the money, allowing criminals to enjoy the proceeds of their illegal activities without raising suspicion or attracting law enforcement attention.

Corresponding Author:- Sonika Bodake
Address:- Research Scholar, Department of Law, Sri Padmavati Mahila Visvavidyalayam, Tirupati, AP.

Traditionally, money laundering involved physical cash and complex networks of intermediaries. However, with the rise of digital currencies and cryptocurrencies, criminals have found new avenues to launder money. Virtual assets have become an attractive choice due to their decentralized nature, allowing individuals to conduct transactions without revealing their identities.

Definition of Money Laundering

Money laundering in the definition of the European Parliament and the Council of the European Union means intentional committed actionswhose purposes consist in concealing or disguising "the true nature,source, location, disposition, movement, rights with respect to, or ownership of property" (Directive 2001/97/EC of the European Parliament and of the Council, Art. 1 (C)). The properties themselves are derived from criminal activity or from an act of participation in such activity. The committed actions must have been done in knowledge of the fact such of the illicit origin. The conversion, exchange, transfer, transport, acquisition, possession or use of assets for the purposes of concealing their illicit origin belong to these illegal committed actions in terms of § 1 (C) of the Directive 2001/97/EC (also in § 1956 Money Laundering of USA Patriot Act). paper money).

Genesis and Concept of Money Laundering

To launder money is to disguise the origin or ownership of illegally gained funds to make them appear legitimate. Hiding legitimately acquired money to avoid taxation also qualifies as money laundering. Money laundering has attracted growing attention in the last decade, in part because of its importance to drug trafficking. It has proven nearly impossible to interdict the flow of drugs into the United States or to halt their distribution within the country. The term "electronic payment" describes a payment method that excludes the use of actual cash or checks. Debit cards, credit cards, smart cards, e-wallets, and so on are included. Risks associated with online payments include identity theft, false customer rejection, and theft of payment information.Money laundering is a process in which illegally acquired money, through various financial transactions, is translated into legal flows and it is an illegal activity. It harms the economic growth of countries and is most often used to finance terrorist activities and is considered a serious threat at the global level.

Phases Of Money Laundering In E- And M-Commerce

The concealment or disguise of the origin, location, nature etc. of property takes place as a result of a complicated and multistage process that can consist of a lot of single transactions. The transactions can be furthermore carried out by credit and financial institutions supported by transaction systems for international payments (e. g., Target, SWIFT). The illicit assets are legalized within the scope of money laundering by a process that consists of three main phases.

Placement:

Assets from illicit dealings are converted in this phase into other forms of properties to allow their investment or movement in legal properties. Examples are deposits, checks, prepaid cards with electronic chips, gold, virtual currencies and securities instead of cash.

Layering:

It will be tried by a set of transfers of assets between accounts of different financial institutions and other economic subjects to cover up the identity of the true owner or the money launderer. The determination of the origin of the property becomes more and more difficult and expensive on accounts of numerous transfers. Besides, different legal restrictions, like the transaction reporting obligation for transaction amounts higher than a legally defined amount (e.g. money changes, owner of foreign bank accounts), are avoided by the money launderers.

Integration:

Integration is the final money laundering process where seemingly legal money flows from fictitious accounts to one primary account, with the aim of investing money in legal business ventures Money is invested in securities, movable and immovable property, the purchase of companies and the like, in countries that have an underdeveloped degree of control over the origin of money states that money laundering consists of three steps. The first step of "money laundering" is to deposit money in banks or buy expensive goods and transfer them abroad. The second step is the realization of complex financial transactions between banks in various countries aimed at hiding the origin of money. The last step is to create the illusion of the legality of money through fake invoices.

Fake invoicing:
This method involves selling goods or works of art at far higher prices than estimated. Goods or works of art are sold to a intermediary in the value of the money to be laundered. When the trade is completed, the work of art is returned by the intermediary to the original owner, who refunds the money to the buyer, in the amount reduced by the commission.

Reverse money laundering.
An organization that wants to launder money steals goods (luxury goods) in the amount it wants to launder. The goods are sold and the money from the goods is invested in a bank in another country. After that, through the banks controlled by the organization that performs money laundering, it is requested to issue new banknotes of a certain currency in the amount of the invested amount from the sold goods. The country whose currency is requested prints banknotes in the requested value and delivers them to banks that are under the control of organizations that want to launder money.

These methods are not the only ones used and very often a combination of several of these methods is used to ensure stratification and conceal the illegal origin of money.

Cryptocurrencise :
Cryptocurrencies and digital currencies are important instruments in cyber laundering. Mixing services, sometimes known as tumblers, are used by criminals to combine their illicit and legitimate money. Because of this, it is difficult for the authorities to determine the original source of the funds.Compared to conventional non-cash payment options, cryptocurrency transactions offer a higher level of privacy. Virtual money can be exchanged online by users, and transactions are typically characterised by the absence of in-person customer interactions. This allows for anonymous funding, which can be either cash funding or third-party funding through virtual exchangers that fail to sufficiently identify the funding source. For global corporations, having a global presence increases the dangers associated with AML/CTF since it complicates surveillance and enforcement.Law enforcement may target certain exchangers in order to obtain client information that the exchanger may gather, but they are not permitted to launch an inquiry or take assets against a single central location or business (administrator). Consequently, using virtual currency for transactions offers a degree of anonymity not achievable with conventional credit and debit cards, or outdated Internet payment methods.

Online Gaming and Gambling:
Platforms for online gaming have grown in popularity as a means of money laundering. The regular international transfer of virtual assets, in-game money, and objects creates a complex network of transactions that is challenging for investigators to comprehend. Money can be laundered through online auctions and sales, gambling websites, and even virtual gaming sites. Ill-gotten money is converted into the currency that is used on these sites, then transferred back into real, usable, and untraceable clean money.

Proxy Servers and AnonymisingSoftwar:
A technique known as ‘proxy piercing’ allows hosts to ascertain whether or not a user is making a proxy purchase. A transaction in which a customer uses a proxy server to mask their IP address is referred to as a proxy purchase. By using proxy piercing, one may determine whether a customer attempting a transaction is using a proxy. Next, it will ‘pierce’ the proxy server and identify the original IP of the transaction, according on the degree of the piercing programme. Proxy piercing goes one step further and can also pinpoint that user's exact location.Proxy servers are frequently used by scammers to conceal their real identities when they make chargebacks or fraudulent transactions.They do this action to evade discovery that the address on their payment method does not correspond to the geo location of their IP address. By breaking through that barrier, proxy piercing determines whether a buyer is making use of a proxy.

Dark Web and Encryption :
The dark web is an encrypted part of the internet that hosts online content not indexed by conventional search engines. Also known as the ‘darknet’, its first structure was conceived by the US Naval Research Laboratory in the mid-90’s as an anonymised and ciphered network for the ease of communication between US spies.

Issues and Challenges Regarding Electronic Payment System

Lack of Security:

Online payment systems for the internet are an easy target for stealing money and personal information. Customers have to provide credit card and payment account details and other personal information online. This data is sometimes transmitted in an un-secured way, Providing these details by mail or over the telephone also entails security risks.

Lack of Usability:

Electronic payment system requires large amount of information from end users or make transactions more difficult by using complex elaborated websites interfaces. For example credit card payments through a website are not easiest way to pay as this system requires large amount of personal data and contact details in web form.

Lack of Trust:

Electronic payments have a long history of fraud, misuse and low reliability as well as it is new system without established positive reputation. Potential customers often mention this risk as the key reason why they do not trust a payment services and therefore do not make internet purchases .

Issues with e-Cash:

The main problem of e-cash is that it is not universally accepted because it is necessary that the commercial establishment accept it as payment method. Another problem is that when we makes payment by using e-cash, the client and the salesman have accounts in the same bank which issue e-cash. The payment is not valid in other banks.

Users Perception:

Regarding Acceptance of Electronic Payment Systems User's acceptance is a pivotal factor determining the success or failure of any information system project. Many studies on information technology report that users attitudes and human factors are important aspects affecting the success of any information 4.6 Lack of Awareness Making online payment is not an easy task. Even educated people also face problems in making online payments. Therefore, they always prefer traditional way of shopping instead of online shopping. Sometimes there is a technical problem in server customers tried to do online payments but they fails to do. As a result they avoid it.

Overcoming the Problems of Electronic Payment Systems

• Encryption Online shopping are very sensitive to notion that e-commerce is insecure, particularly when it comes to online payments. Most online payment systems use an encryption system to add security to the transmission of personal and payment details. There are various encryption schemes in use to prevent from frauds of online payments.

• **Digital Signatures:** The parties involved in online payments, transactions should use digital signatures in order to ensure authentication of transactions.

• **Firewalls:** A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system to protect private network and individuals machines from the dangers of the greater internet.

Comparison of the Credit Card Issuing:

Bank's Country with the Billing Address Country Another key point to bear in mind is to check the issuing country and the billing address. Make sure the issuing country and billing address country are the same. This is especially important, because minor banks may not have rigorous identification procedures. The issuing bank phone number is based on the first 6 digits of credit card number known as the Bank Identification Number (BIN).

Request more identification in case of doubts :

While consumers value their privacy and require quick web site ordering facilities, it is important to gather sufficient customer identity details during the ordering process. The customers' name, credit card number and expiry date is not enough.

The Global Fight against Money Laundering via Virtual Assets

As the use of virtual assets in money laundering schemes continues to rise, international efforts and frameworks are being established to combat this illicit activity. Governments, financial institutions, and regulatory authorities

understand the need for enhanced regulatory measures and collaboration to address the challenges posed by money laundering via virtual assets.

• International Efforts and Frameworks: Recognizing the global nature of money laundering via virtual assets, international organizations such as the Financial Action Task Force (FATF) have taken steps to provide guidance and recommendations to member countries. The FATF has emphasized the importance of implementing effective measures to prevent the misuse of virtual assets for money laundering purposes. According to the International Monetary Fund (IMF), as of October 2020, 58 out of 129 jurisdictions have criminalized money laundering via virtual assets (IMF). However, there is still a need for greater global alignment and consistency in addressing this issue.

• **Concerns for Financial Systems** : The use of virtual assets in money laundering schemes poses significant concerns for financial systems worldwide. The decentralized and borderless nature of virtual currencies makes it challenging to track, identify, and investigate illicit activities. Criminals exploit the anonymity and pseudonymity offered by virtual assets, making it difficult for law enforcement agencies to trace the origin and destination of funds.

• **Need for Enhanced Regulatory Measures:** To effectively combat money laundering via virtual assets, there is a pressing need for enhanced regulatory measures. Countries around the world are updating their legal frameworks to address the rise of virtual assets in money laundering schemes. These regulatory measures focus on improving the transparency and accountability of virtual asset transactions, enhancing customer due diligence requirements, and ensuring that virtual asset service providers (VASPs) comply with anti-money laundering and counter financing of terrorism (AML/CFT) regulations. The goal is to establish a robust framework that effectively addresses the risks associated with money laundering via virtual assets.

Measures Against Money Laundering

A lot of international organizations, as for example the Financial Action Task Force on Money Laundering (FATF), the Basel Committee on Banking Supervision (BCBS) and institutions like the European Commission etc. which have worked out different regulations, recommendations and standards. Recommendations as an international standard, for national supervisory authorities and economic subjects, e. g., financial institutions, that deal with combating of the international money laundering.

A large number of national supervisory authorities see no danger of money laundering in newer electronic payment systems if the following measures are undertaken (Committee on Payment and Settlement Systems, (2004)):

Smart cards or wallets may be uploaded only up to a certain value

• Payment systems are accounted and require the involvement of a bank in each transaction (no person-to-person transfers).

• Recording of all transactions.

• Restriction of the application possibilities on a national level
(no cross-border transfers).

The unique certification of users of payment systems by a trust center that guarantees the non-repudiation of transactions worldwide is the one Technical solution . Registration with thetrust ed centers and having certificates can already be kept in a variety of payment devices, including software wallets and prepaid cards. The trust centers can be mutually recognized based on their certificates, and the appropriate national authorities (roots) can carry out their own certification. Currently, certification programs are pretty isolated fixes. They can, however, be quickly incorporated into a comprehensive certification infrastructure. This is the outcome of using symmetrical cryptography with the hierarchical construction approach for certification. In addition to enabling non-repudiation of transactions, the addition of certification and digital signatures as functional components of electronic payment systems will also enable cross-border interoperability and transaction verification, which will be another effective measureagainst the international money laundering on electronic markets..

Conclusion:-

International coordination and collaboration are required in the fight against money laundering using virtual assets. For the purpose of updating legal frameworks, improving regulatory measures, and establishing efficient control and supervision of virtual asset transactions, governments, financial institutions, and regulatory authorities must collaborate. Adopting a comprehensive strategy that is globally coordinated will help the international community tackle money laundering schemes that are made possible by virtual assets.

As a result, we must make use of the current technology to ensure a respectable minimum degree of network security until the usage of electronic signatures becomes widely accepted. Even while each of the payment methods has advantages over the others, it is hard to state that any one of them is ideal. The customer selects payment options like Net Bill Checks or E-cash, which offer a better level of anonymity, if they wish to keep their private intact. Use of smart cards is appropriate if security is the top priority. E-payment systems have the potential to benefit service providers as well as consumers, thereby increasing national competitiveness. The popular management of security and privacy aspects as viewed by both buyers and sellers is critical to the effective implementation of electronic payment systems, which in turn boosts market confidence.

References:-

1. Banking Regulation (Amendment) Act, 2020 (Act 39 of 2020)
2. Consumer Protection Act, 1986
3. Income Tax Act 1961
4. Indian Penal Code, 1860
5. Information Technology Rules, 2021
6. Information Technology Rules,(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) 2011
7. Internet banking and the Payment and Settlement Systems Act, 2007
8. Negotiable Instrument Act, 1881
9. Prevention of Money Laundering Act, 2002
10. G.S.Bajpai,Cyber Crime and Cyber law, Serials publications new Delhi published in 2011 ISBN 078-81-8387-484-7
11. Gupta R.K , Internet Banking and Payment Systems ,Payment and Settlement Systems Act, 2007, Act No. 51 of 2007, (2nd Edition, LexisNexis 2024), p. 89.
12. **Gupta R.K , Banking Law and Technology (2nd Edition), Eastern Law House, 2024, p.153**.
13. Jain M.P. ,**Indian Constitutional Law** (8th Edition), LexisNexis, 2020, p. 98
14. **Jain.p.k, Information Technology Act, 2002, Cyber Law and Information Technology (3rd Edition), LexisNexis, 2023, p. 89.**
15. John Smith, **Banking Fraud Cases** (2nd Edition), Thomson Reuters, 2021, p. 88.
16. **Miller, Matt & Nance, Jessica.Advanced Persistent Threats: How to Defend Against the Most Dangerous Cyber Threats** (2023) (1st ed.). Wiley
17. Mishra, R.C., Cyber Crime: Impact on the New Millennium, (2002), p. 246
18. Rao P.S , Consumer Protection Law , Consumer Protection Act, 1986, Act No. 68 of 1986, (5th Edition, LexisNexis 2023), p. 78.