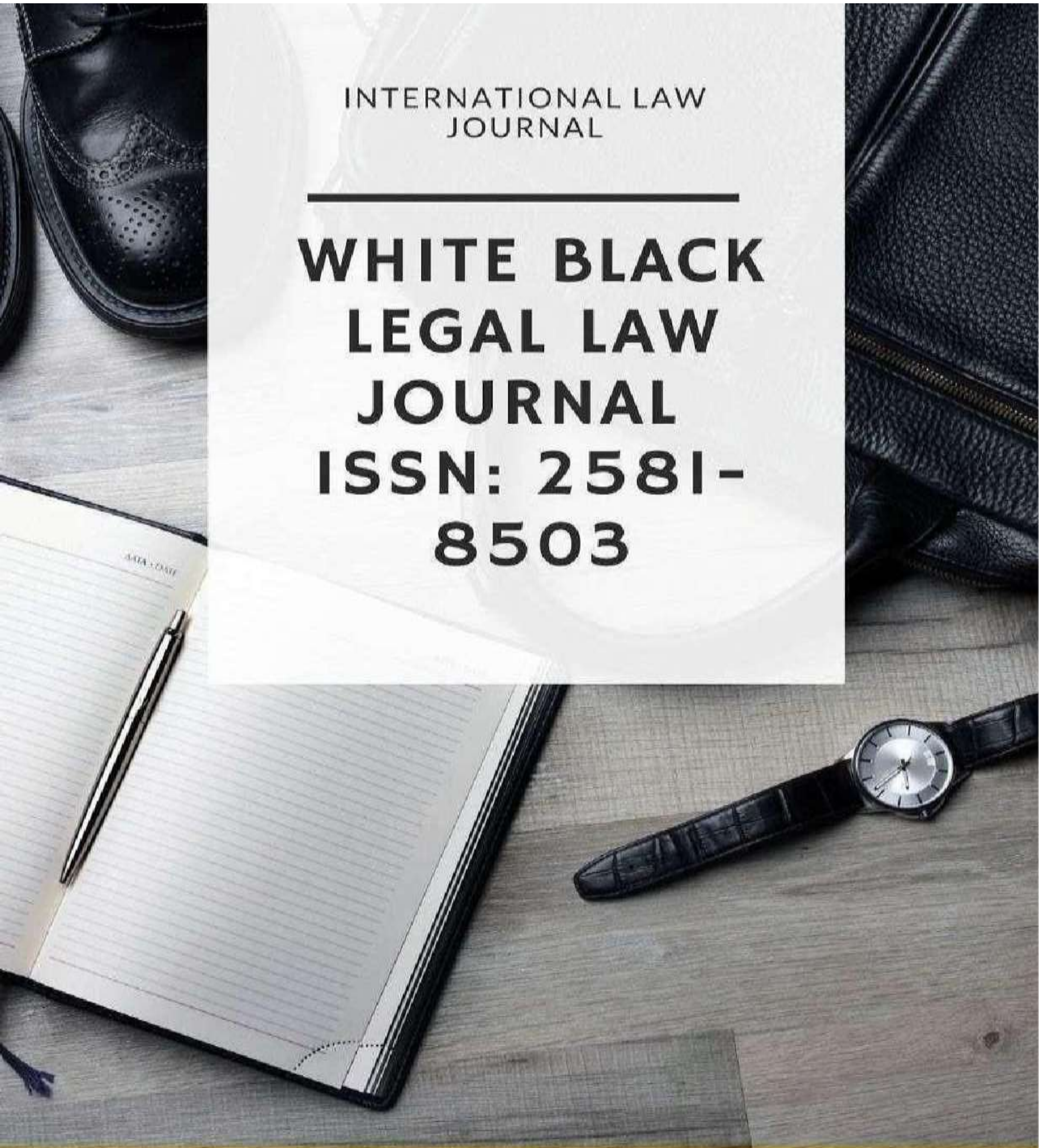

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

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

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

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

Dr. R. K. Upadhyay

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

Senior Editor

Dr. Neha Mishra

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

Ms. Sumiti Ahuja

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

Dr. Navtika Singh Nautiyal

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

Dr. Rinu Saraswat

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

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

Dr. Nitesh Saraswat

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

Subhrajit Chanda

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

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

ABOUT US

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

With this thought, we hereby present to you

CRITICAL ANALYSIS OF FRAUD, RISK AND PROTECTION OF E-COMMERCE IN INDIA

AUTHORED BY: NANDHU ANIL*
LLM Student (Corporate and Commercial law)
Christ Deemed to be University, Bangalore
Ph no: 7034941516
Email: nandhu.anil@law.christuniversity.in

ABSTRACT

The emergence of new trends in the economy is due to the rapid growth of e-commerce platforms. The accessibility and comfortability of these online platforms bridged traditional business methods from the scenario. The main drawback which retards the growth of e-commerce is the expansion of fraud in these platforms. Both consumers and retailers are victims of these fraudulent transactions. E-commerce fraud is criminal cheating on purchases from an online store with the help of some electronic gadgets such as desktops and mobiles with the intention of monetary benefits. Deception is the basic idea behind e-commerce fraud. The easy availability of private data resources is the backbone of e-commerce fraud. This is the main reason for the increasing number of these frauds. Fraudsters will get any personal details of both credit and debit cards from resources obtained by hacking. Maintaining anonymity in these crimes is very easy for these fraudsters. The absence of physical verification and easy manipulation of email IDs are boosting the anonymous nature of these crimes. The lack of strict laws and systematic procedures for taking action against these crimes are also reasons for the increase in number. Usually, these fraudsters loot small amounts of money from many victims; this will affect the authorities' seriousness in taking action due to the quantity of pecuniary. Recent reports cited that 57%of total frauds in India are through online platforms.

The primary objective of this research is to identify common types of e-commerce fraud, including credit card, affiliate, chargeback, phishing, interception, and triangulation fraud, and how to protect from these frauds. Credit card fraud includes stolen credit card information used for purchases from online stores. Generating fake gateways or typosquatting to get affiliate commission is typical in e-commerce. Collecting personal usernames and passwords through phishing is also common in online platforms. Manipulation of products by sellers, such as duplicating and selling defective products, is also standard in e-commerce sites.

This study aims to identify these frauds in e-commerce and how to get protection from these illegal actions. Sellers should be aware of inconsistent order data, more orders, unusual location details, multiple shipping addresses in the same billing address, and many short-duration transactions. These are signs of fraud in our online stores.

After studying the reasons behind these scams, Solutions are also prescribed to avoid this rapid increase in fraud in e-commerce platforms. Site security should be regularly scrutinised. Security factors such as HTTPS, AVS, and PCI should be used for the safety of the sites. Card transactions should be made authenticated by CVV number. Use of anti-fraud tools can also be used. Double verification of physical addresses can also avoid the risk of fraudulent purchases. To avoid these scams, consumers avoid sharing high-security personal details with unknown online stores.

The lack of relevant provisions regarding jurisdiction and strict laws to address these online frauds is the main reason for the large number of online scams in INDIA. The legal system should be updated quickly in this rapidly growing tech era.

KEYWORDS - E-COMMERCE, FRAUD, RISK MANAGEMENT, PROTECTIVE MEASURES, LEGISLATIONS

INTRODUCTION

The rise of e-commerce has undeniably transformed the way we shop, bringing convenience and endless choices to our fingertips. E-commerce technologies have changed the structure and environment of business worldwide[1]. However, amidst the digital revolution lies a lurking threat of fraud. E-commerce fraud has become pervasive, overshadowing the online marketplace's immense

[1] Sumanjeet, The state of e-commerce laws in India : a review of Information Technology Act, 52 Int. J. Law Manag. 265–282 (2010).

opportunities. As transactions move from traditional brick-and-mortar stores to virtual shopping carts, fraudsters have adapted, finding innovative and sophisticated methods to exploit the vulnerabilities of online systems. Understanding the multifaceted nature of e-commerce fraud is essential for businesses and consumers to navigate the digital landscape securely. In the rapidly evolving landscape of electronic commerce, the digital marketplace has become a bustling hub of activity, connecting buyers and sellers from across the globe. While this unprecedented connectivity brings immense opportunities for businesses and consumers, it exposes them to significant risks, particularly in fraud. As e-commerce continues to flourish, so do the sophisticated tactics employed by cybercriminals aiming to exploit vulnerabilities in online transactions[2].

This comprehensive exploration delves deep into the intricate web of fraud that permeates the e-commerce sphere. From identity theft and payment fraud to account takeovers and phishing schemes, the tactics used by fraudsters have grown increasingly sophisticated, posing a substantial threat to both businesses and consumers. Through insightful analysis and real-world examples, this article sheds light on the various forms of e-commerce fraud, allowing readers to grasp the complexity of the challenges faced in the digital marketplace.

Assessing Risks and Vulnerabilities

To combat the ever-expanding array of cyber threats, businesses must proactively identify vulnerabilities within their e-commerce systems. The common risk factors that make businesses susceptible to fraud include weak cybersecurity measures, inadequate payment protocols, and loopholes in identity verification processes. By understanding these vulnerabilities, organisations can implement robust preventive strategies, fortifying their defences against potential attacks.

E-Commerce Protection

In the battle against e-commerce fraud, knowledge is power. This article equips businesses and consumers with practical, actionable strategies to safeguard online transactions. Many measures can be employed to create a resilient digital marketplace, from advanced fraud detection tools and machine learning algorithms to consumer education initiatives and secure payment gateways[4]. By

[2] Dave Chaffey, E-Business and E-Commerce Management: Strategy, Implementation and Practice (5 ed. 2013)

[4] Sheen Kaul, 'History and Development of Consumer Protection Laws in India' (Legal Bites - Law And Beyond, 19 June 2020) accessed 21 June 2021

exploring these protective strategies, readers will gain valuable insights into building a safe online environment where trust and reliability prevail.

What is e-commerce fraud?

E-commerce fraud is the fraud done online, explicitly targeting e-commerce platforms.

E-commerce fraud is any fraudulent or illegal activity conducted during an online transaction. It involves deceptive practices aimed at exploiting vulnerabilities in online shopping, leading to financial loss, identity theft, or other forms of harm to businesses and consumers. Malicious actors deceive companies and consumers into fraudulent transactions, obtain unauthorised access to personal and financial data, and take advantage of the online retail environment in other ways. This kind of fraud can harm the reputations of the companies and sectors involved, resulting in significant financial losses for them and their clients.

TYPES OF E-COMMERCE FRAUDS

IDENTITY THEFT

Identity theft is a serious crime when someone collects and uses another person's data, such as Social Security numbers, credit card details, or bank account information, without permission. This stolen identity can be used for various fraudulent activities, causing significant financial and emotional distress to the victim.

METHODS OF IDENTITY THEFT

- Phishing and Social Engineering

Cybercriminals use fake emails, websites, or phone calls to confuse individuals into revealing sensitive information.

- Data Breaches

Hackers gain unauthorised access to databases containing personal information, which is then sold or used for identity theft.

- Dumpster Diving

Thieves search through trash for discarded documents containing personal details.

- Skimming

Criminals use secret devices to get credit card information during legitimate transactions.

- Impersonation

Thieves pose as someone else to access benefits, medical services, or financial accounts.

CREDIT CARD FRAUD

In a staggering revelation, one of the gangs in India's cybercrime hotspot, Jamtara, was reportedly pocketing between Rs 1 lakh and Rs 1.5 lakh daily through credit card frauds. As per a TOI report, the disclosure of their daily earnings emerged during the initial interrogation of three individuals apprehended by police[5].

Credit card fraud is a pervasive and evolving threat in the digital age, posing substantial risks to consumers, businesses, and financial institutions alike. This fraud involves the unauthorised use of credit card information to purchase or withdraw funds, causing significant economic losses and distress to victims.

Tactics Employed by Fraudsters

- Card Skimming

Criminals use hidden devices to capture credit card information during legitimate transactions, often at ATMs or gas stations.

- Phishing and Spoofing

Fraudsters send fake emails or create websites to trick people into divulging their credit card details.

- Data Breaches

Hackers gain unauthorised access to credit card information databases, which are then sold on the dark web or used for fraudulent activities.

- Account Takeover

Cybercriminals access a victim’s online account and change account details to make unauthorised purchases.

- Carding

Criminals use stolen credit card information to test the card's validity through small transactions

[5] :https://economictimes.indiatimes.com/news/india/how-jamtara-scamsters-pocketed-rs-1-5-lakh-everyday-through-credit-card-frauds/articleshow/103692692.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

before making larger, unauthorised purchases.

CHARGEBACK FRAUDS

Chargeback fraud, or friendly fraud, occurs when a customer falsely claims a transaction as unauthorised, leading to a chargeback. While chargebacks protect consumers, dishonest individuals exploit this system to commit fraud, causing financial losses to businesses employed in Chargeback Fraud.

Tactics Employed by Fraudsters

- False Claims

Fraudsters falsely dispute a legitimate transaction, claiming they did not authorise or receive the purchased goods or services.

- Product Not as Described

Customers might exaggerate product discrepancies or claim items received significantly differed from what was advertised.

- Friendly Fraud

Customers knowingly deny purchasing, seeking a chargeback while retaining the purchased goods or services.

- Identity Theft

Criminals use stolen credit card details to make purchases, and when the cardholder notices, they dispute the transactions, leading to chargebacks.

PHISHING

Phishing fraud is a prevalent cybercrime where attackers impersonate trusted entities to trick individuals into divulging sensitive information, such as login credentials, credit card details, or social security numbers. Phishing attacks can occur through emails, text messages, or malicious websites, posing significant risks to individuals and organisations. The Delhi High Court has clarified the concept of phishing in "National Association Of Software Communication (NASSCOM)[6] case that 'Phishing' scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

[6] National Association Of Software Communication (NASSCOM) v. Ajay Sood and Others, 119 (2005) DLT 596

Methods Employed by Phishers

- Email Phishing

Fraudsters send deceptive emails, often mimicking legitimate organisations, to trick recipients into clicking on malicious links or providing sensitive information.

- Spear Phishing

Phishers target specific individuals or organisations, tailoring their messages based on personal information to increase the likelihood of success.

- Vishing

Attackers use voice calls, posing as trusted entities or government agencies, to extract sensitive information from victims.

- Smishing

Phishers send deceptive text messages, urging recipients to click on malicious links or call a fraudulent number to divulge personal information.

- Clone Phishing

Phishers create identical copies of legitimate websites to deceive users into entering their login credentials, capturing the information for malicious purposes.

SPAMMING

Spamming fraud, often called spam, is the unsolicited sending of bulk messages, primarily via email, to defraud individuals, promote dubious products or services, or distribute malware. Spam emails flood inboxes worldwide, posing severe risks to individuals and organisations.

Tactics Employed by Spammers

- Phishing Scams

Spammers impersonate trusted entities, tricking recipients into revealing sensitive information or visiting malicious websites.

- Malware Distribution

Spam emails contain malicious attachments or links that, when clicked, download malware onto the recipient's device, compromising security.

- Fraudulent Offers

Spammers send emails offering fake products, services, or investment opportunities to deceive recipients into making financial transactions.

- Stock and Investment Scams

Spam emails promote fraudulent stocks or investment schemes, aiming to manipulate stock prices for financial gain.

- Affiliate Marketing Scams

Spammers promote products or services, earning commissions through affiliate marketing, often for counterfeit or substandard goods.

Spamming fraud remains a significant challenge in the digital landscape, requiring constant vigilance, education, and collaboration to mitigate its impact. By implementing robust email filtering, educating users, enforcing legal measures, and fostering collaboration among stakeholders, individuals and organisations can actively combat spamming fraud and contribute to a safer online environment. The Central Information Commission also has contributed to techno transactions in Mrs Sucheta Charudatta Dhekane[7]'s case that precautionary measures have to be taken by the bank to protect customers. Stay informed, remain cautious, and employ strong security practices to defend against the pervasive and evolving threat of spamming fraud.

GIFT CARD FRAUD

Gift card fraud has emerged as a significant threat in the digital age, where fraudsters exploit vulnerabilities in gift card systems to commit various scams and illicit activities. This form of fraud affects individual consumers and poses risks to businesses and financial institutions.

Tactics Employed in Gift Card Fraud

- Card Skimming

Criminals use skimming devices to capture gift card data during legitimate transactions, enabling them to clone or use the cards fraudulently.

- Tampered Cards

Fraudsters replace physical gift cards in stores with tampered ones, allowing them to monitor and use the card's information after purchase.

- Phishing

Scammers use deceptive emails or websites to trick individuals into providing gift card numbers and PINs, claiming false emergencies or rewards.

- Social Engineering

Fraudsters impersonate authority figures, requesting victims to purchase gift cards for various reasons, such as settling fake debts or avoiding legal consequences.

- Account Takeover

Criminals gain unauthorised access to online gift card accounts, manipulating balances or transferring funds to other accounts.

CYBERSQUATTING

Cybersquatting, an unethical practice, involves registering, trafficking, or using a domain name with the bad-faith intent to profit from the goodwill of a trademark belonging to someone else. This act harms brands and confuses consumers, leading to potential financial and reputational damage.

Tactics Employed in Cybersquatting

- Trademark Infringement

Cybersquatters register domain names identical or confusingly similar to established trademarks, attempting to capitalise on the brand's recognition.

- Typosquatting

Cybersquatters register domain names with common typographical errors related to popular websites or brands, intending to exploit users who make typing mistakes.

- Brandjacking

Cybersquatters create domain names imitating a brand's online presence, including social media handles, to deceive consumers and tarnish the brand's reputation.

- Ransom Domains

Cybersquatters register domains corresponding to a company's name or product and demand a ransom from the rightful owner to release the domain.

LAWS REGULATING E-COMMERCE FRAUDS IN INDIA

In India, e-commerce frauds are regulated by various laws and regulations to protect consumers and maintain the integrity of online transactions. The primary legal framework governing e-commerce and related scams in India includes:

Information Technology Act, 2000 (IT Act)

The IT Act is the central legislation that deals with electronic commerce and cybercrimes in India. It includes provisions related to unauthorised access, data theft, and hacking. Section 43, Section 65, and Section 66 of the IT Act are particularly relevant in the context of e-commerce fraud.

Section 43[8] - Penalty and Compensation for Damage to Computer, Computer System, etc.:
This section penalises unauthorised access to computer systems, including e-commerce platforms. If someone gains unauthorised access or causes damage to computer systems, they can be held liable for penalties.

Section 65[9] - Tampering with Computer Source Documents:
This section punishes individuals who knowingly or intentionally conceal, destroy or alter any computer source code, which can be crucial evidence in e-commerce frauds or cybercrimes.

Section 66[10] - Computer-Related Offenses:
Sub-sections (A), (B), and (C) of Section 66 cover offences such as unauthorised access to computer systems, computer-related offences, and damaging computer systems, all of which apply to e-commerce frauds.

Section 66C[11] - Identity Theft:
This section deals explicitly with identity theft, a common element in many e-commerce frauds. It penalises the theft of sensitive personal information.

Section 66D[12] - Cheating by Personation by Using Computer Resources:
This section deals with fraudulent activities involving impersonation, which can occur in e-commerce frauds where individuals pretend to be someone else to deceive customers or businesses.

[8] sec43 IT ACT 2000. Penalty for damage to computer, computer system, etc

[9] sec65 IT ACT 2000. Tampering with computer source documents.

[10] sec66 IT ACT 2000. Hacking with computer system.

[11] sec 66 C IT ACT 2000 cheating by impersonation

[12] section 66D IT ACT 2000, violation of bodily privacy

CONSUMER PROTECTION ACT, 2019

The Consumer Protection Act 2019 empowers consumers in India. It provides a mechanism for redressing complaints related to e-commerce transactions, ensuring consumers have rights and legal protection against fraudulent activities by sellers or service providers.

The Consumer Protection Act 2019 (CPA 2019) in India was enacted to strengthen consumer rights and provide an adequate legal framework for addressing consumer grievances. Under this act, e-commerce transactions are explicitly handled, ensuring consumers engaging in online purchases are protected. Here are the key provisions related to e-commerce under the Consumer Protection Act, 2019

Definition of E-commerce

The CPA 2019 defines electronic service providers and retailers, distinguishing between service providers and product sellers in the digital space.

Product Liability

E-commerce platforms are considered product sellers under the CPA 2019. If a consumer faces any harm or damage due to a defective product bought online, they can seek compensation from both the platform and the actual seller.

Misleading Advertisements

The act prohibits misleading advertisements, including those in the digital sphere. E-commerce platforms are liable for any misleading or false claims made on their platforms.

Unfair Trade Practices

Unfair trade practices, including deceptive practices in e-commerce transactions, are covered under the CPA 2019. If a consumer faces harassment or financial loss due to such practices, they can seek legal recourse.

E-commerce Dispute Resolution

The CPA 2019 establishes Consumer Disputes Redressal Commissions at the district, state, and national levels. Consumers can file complaints related to e-commerce disputes at these commissions.

Product Recall

E-commerce platforms are obligated to recall products that are hazardous, unsafe, or violate consumer rights. The act specifies procedures for product recall in the e-commerce context.

E-commerce Liability

E-commerce platforms can be held liable for any harm or damage caused to consumers due to defective products, inadequate services, or false claims made on their platforms.

Consumer Data Protection

While the CPA 2019 doesn't specifically address data protection, e-commerce platforms must handle consumer data responsibly to avoid legal issues related to privacy and data breaches.

INDIAN PENAL CODE 1860

Certain sections of the IPC, such as Section 420 (dealing with cheating and dishonestly inducing delivery of property), are applicable in cases of fraud and deceptive practices in e-commerce transactions. In the Indian Penal Code (IPC), several provisions deal with various types of fraud and related offences. These provisions aim to penalise individuals involved in fraudulent activities, ensuring legal consequences for dishonest and deceptive practices. Here are some of the vital fraud-related provisions in the IPC:

Section 415[13] - Cheating:

This section defines cheating as an act which dishonestly induces a person to deliver any property, to alter their position, or to do or omit to do something which they would not do if they were not deceived. The offence of cheating is punishable under Section 417 of the IPC.

Section 416[14] - Cheating by Personation:

This section deals with cheating by personation, where someone cheats on another person by

[13] Sec 415 IPC1860 cheating

[14] Sec 416 IPC1860 Cheating by Personation

pretending to be someone else. The offence is punishable under Section 419 of the IPC.

Section 417[15] - Punishment for Cheating

Section 417 prescribes the punishment for cheating. Whoever cheats shall be punished with imprisonment of either description for a term that may extend to one year, with a fine, or with both.

Section 418[16] - Cheating with Knowledge that Wrongful Loss May Ensue to Person Whose Interest Offender is Bound to Protect:

This section deals with cheating when the offender knows that a wrongful loss may ensue to a person whose interest the offender is bound to protect. The punishment is the same as provided under Section 417

Section 420[17] - Cheating and Dishonestly Inducing Delivery of Property:

Section 420 deals with cases where a person cheats and thereby dishonestly induces the person deceived to deliver any property to any person or to make, alter, or destroy the whole or any part of a valuable security or anything which is signed or sealed and which is capable of being converted into a valuable security. Section 420 prescribes more severe punishment, which may extend to imprisonment for a term of up to seven years and a fine.

SUGGESTIONS TO AVOID E-COMMERCE FRAUDS IN INDIA

Preventing e-commerce fraud in India or anywhere else requires a combination of vigilance, awareness, and innovative online practices. Here are some suggestions to help consumers and businesses avoid falling victim to e-commerce fraud:

FOR CONSUMERS

Buy from Reputable Websites: Stick to well-known and reputable e-commerce websites. Be cautious

[15] Sec 417 IPC1860 Punishment for Cheating

[16] Sec 418 IPC1860 Punishment for Cheating

[17] Sec 420 IPC1860 Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect

when dealing with lesser-known or newly established online stores.
Check Website Security: Look for "https://" in the website URL, indicating a secure connection. Avoid websites with misspelt domain names or unusual URLs.

Read Reviews: Check customer reviews and ratings of sellers and products. Genuine customer feedback can provide valuable insights into the credibility of the seller.

Beware of Unrealistic Deals: If a deal seems too good to be true, it probably is. Scammers often lure victims with unbelievably low prices to entice them into making impulsive purchases.

Use Secure Payment Methods: Opt for secure payment methods like credit cards or trusted payment gateways. Avoid direct bank transfers or sharing financial information over emails or chat platforms.

Enable Two-Factor Authentication: Enable two-factor authentication for your e-commerce accounts whenever possible. This adds an extra layer of security.

Keep Software Updated: Regularly update your web browser, operating system, and antivirus software to protect against malware and phishing attacks.

Be Cautious with Personal Information: Avoid sharing unnecessary personal information. Legitimate e-commerce platforms don't need extensive personal details.
Monitor Your Accounts: Regularly check your bank and credit card statements for unauthorised transactions. Report any suspicious activity immediately.

FOR BUSINESSES

Secure Your Website: Implement SSL certificates, use strong encryption methods, and update your e-commerce platform's software to protect customer data.

Educate Your Customers: Provide guidelines to customers on identifying genuine communication from your business. Warn them about phishing attempts.

Implement Multi-Factor Authentication: For employees accessing sensitive business systems, use multi-factor authentication to add an extra layer of security.
Regular Security Audits: Conduct regular security audits and vulnerability assessments of your e-commerce platform to identify and fix potential weaknesses.

Train Your Employees: Educate your employees about cyber threats, phishing scams, and safe online practices. Human vigilance is crucial in preventing fraud.
Use Verified Payment Gateways: Integrate trusted and verified payment gateways to process transactions securely.

Implement Fraud Detection Tools: Utilize fraud detection tools and machine learning algorithms to identify suspicious patterns and prevent fraudulent transactions.

Quick Customer Support: Provide prompt customer support to address customer concerns or issues, ensuring they feel valued and heard.

Adopting these precautions and promoting awareness among consumers and employees can significantly reduce the risk of falling victim to e-commerce fraud. Stay informed, be vigilant, and prioritise security in all online transactions.
Regenerate

CONCLUSION

In the ever-expanding digital landscape of India, the flourishing e-commerce sector offers unparalleled convenience and accessibility. However, this convenience comes hand-in-hand with the lurking threats of fraud and cybercrime. As consumers and businesses traverse this online realm, the need for vigilance, awareness, and proactive measures cannot be overstated.

For consumers, discernment is paramount. By patronising reputable platforms, verifying sellers, and adopting secure payment methods, individuals can fortify their defences against fraud. Embracing digital literacy and staying updated on the latest scams empower consumers to make informed decisions, ensuring their online experiences are safe and gratifying.

On the other hand, businesses bear a dual responsibility – to protect their customers and their integrity. Employing stringent security measures, from SSL certificates to advanced fraud detection algorithms, is the first line of defence. Regular employee training and robust customer support further bolster these defences, instilling confidence in consumers and deterring potential fraudsters.

In the digital age, the battle against e-commerce fraud in India necessitates a unified front. Law enforcement agencies, businesses, consumers, and regulatory bodies must collaborate, share insights, and adapt swiftly to evolving threats. Legal frameworks, such as the Consumer Protection Act and the IT Act, provide essential tools to penalise wrongdoers, yet education and awareness remain the bedrock of prevention.

As India accelerates toward a digital future, safeguarding e-commerce is not just a matter of individual concern but a collective responsibility. By fostering a culture of caution, resilience, and collaboration, India can nurture a digital marketplace where trust thrives, ensuring that the promises of e-commerce are realised without compromising the security and confidence of its participants. Together, as vigilant consumers and businesses, India can pave the way for a secure and thriving e-commerce ecosystem for generations.

REFERENCES

Sumanjeet, The state of e-commerce laws in India : a review of Information Technology Act, 52 Int. J. Law Manag. 265–282 (2010).

Dave Chaffey, E-Business and E-Commerce Management: Strategy, Implementation and Practice (5 ed. 2013)

D. Kannan, E-Frauds and Its Causes in Digital Transactions - A Myth or Reality, 2 INDIAN J.L. & LEGAL Rsch. 1 (2021).

Pratham Malhotra, From Physical Markets to E-Commerce: Development of Consumer Rights in India, 1 Jus Corpus L.J. 321 (2021).

K. Kashyap & M. Chaudhary, Cyber Security Laws and Safety in e-Commerce in India, 2023 LAW & Safety 207 (2023).

Sonika Sekhar, 'The History of Consumer Protection' (Law Times Journal, 19 November (2018)