CROSS-BORDER ONLINE TRADING FRAUDS AND THE CHALLENGES OF JURISDICTION: A LEGAL ANALYSIS OF INDIA'S FRAMEWORK AGAINST TRANSNATIONAL CYBER FINANCIAL CRIMES

Ruban Paul P & Shruthi V, The Tamilnadu Dr. Ambedkar Law University (SOEL), Chennai

ABSTRACT

The rise of digital trading platforms has opened up to new investment options but it has also made investors more vulnerable to cyber-enabled financial crime than ever before. Recent events, like the Kochi businessman who lost ₹24.76 crore to an internet trading fraud run by a call centre in Cyprus, show how cross-border cyber financial crimes are becoming more common and these scams take use of the fact that cyberspace is anonymous, that digital payment systems are complicated and that there aren't any consistent worldwide legal systems in place and it makes it very hard to find, investigate, and prosecute them.

It emphasises the jurisdictional challenges encountered by Indian enforcement agencies when fraudulent enterprises operate internationally, the insufficiency of existing measures to enhance extraterritorial jurisdiction and the sluggish effectiveness of Mutual Legal Assistance Treaties (MLATs) in cybercrime investigations and it also analyses India's non-participation in the Budapest Convention on Cybercrime, juxtaposing it with global best practices from the United States, the European Union and Southeast Asia. This comparative analysis assesses the adequacy of India's current legislative instruments in tackling the transnational aspects of internet trading frauds, determining the necessity for systemic reforms. The essay contends that although India possesses a relatively strong cyber and financial legal framework, the disjointed enforcement strategy, insufficient international collaboration and restricted victim compensation mechanisms make it ineffective in addressing cross-border trading frauds. It ends by suggesting that cyber forensic skills be improved, international cooperation be sped up, countries sign up to global cybercrime treaties and a separate legal system be created for online financial scams to protect investors in the digital economy.

Keywords: Cross-border cyber fraud, Online trading scams, Jurisdictional challenges, Transnational cyber financial crimes, Information Technology Act, 2000, SEBI and RBI regulations, Mutual Legal Assistance Treaties.

1.Introduction

In the past few years, India has seen a big growth in online trading scams, when naive investors are enticed to fake digital platforms with promises of enormous returns and fraudsters use bogus trading apps, copied websites and convincing call centres to trick people into thinking they are real investment opportunities. People who fall for these scams often put in a lot of money, only to find out later that the platforms were fake and their money was stolen. A businessman from Kochi lost almost ₹24.76 crore in a trading fraud that was connected to a contact centre in Cyprus. This is a very clear example. This case shows how big and complicated cyber financial crimes are in India's economy, which is quickly going digital.

What makes these scams so scary is that they happen across borders and online trading scams are different from other types of financial fraud because the criminals generally work from other countries and use offshore shell firms, encrypted communications, and international money transfers. Because these crimes happen across borders, they are very hard for Indian law enforcement to deal with. To investigate and prosecute them, they need help from foreign authorities, which can take a lot of time and effort through diplomatic and legal channels. As a result, victims are not only facing financial devastation, but also a small chance of getting better or getting justice.

In light of this, the jurisdictional issues raised by cross-border cyber financial crimes need immediate attention from scholars and policymakers. Jurisdiction in cyberspace is inherently contentious, as activities executed in one region might inflict harm in another almost instantaneously. India is not a party to the Budapest Convention on Cybercrime, finds that its dependence on Mutual Legal Assistance Treaties (MLATs) and bilateral agreements frequently falls short in obtaining timely evidence or prosecuting overseas perpetrators. This gap brings up important considerations regarding whether India's current laws, like the Information Technology Act of 2000, the Indian Penal Code of 1860, and the Prevention of Money Laundering Act of 2002, are good enough to deal with the fact that these crimes happen across borders.

Consequently, examining online trading fraud through the perspective of jurisdictional issues is crucial for both legal scholarship and policy formulation. It not only shows how Indian investors are at risk in a globalised digital economy, but it also shows how important it is to make sure that domestic regulations are in line with international standards. This study is

pertinent and essential, as India establishes itself as a centre for digital money while also striving to protect its citizens from the adverse effects of financial globalisation.

2. Understanding Online Trading Frauds in Cyberspace

The rapid growth of digital trading platforms has made it easier to invest, but it has also made it easier for cybercriminals to commit financial fraud. Scammers who trade online take advantage of investors' trust, the anonymity of the internet and the fact that different countries have different laws. These scams are different from regular frauds because they use very organised multinational networks that make it very hard to find and prosecute them.

2.1 Modus Operandi of Online Trading Scams

Fraudsters mostly make bogus trading apps and websites that seem a lot like real investment platforms. These platforms show fake dashboards with changed trade charts and earnings to make investors feel better about the "genuineness" of their investments and call centres often contact victims and operators who may speak regional languages fluently pose as financial advisors promoting investment programs that promise high returns. These scammers sometimes let investors take out little earnings at first to gain their trust before asking for greater investments, which they then steal.

The Ponzi-style trading scheme is another frequent type and this plan it early investors get returns from the deposits of new participants, which makes it look like the scheme is making money. The scheme eventually falls apart, leaving behind a trail of losses while the scammers hide behind layers of secrecy. Increasingly, scammers use social engineering techniques to get people to put money into fake trading apps. For example, they can pretend to be international brokers or use romantic scams as an excuse.

2.2 Role of Shell Companies, Offshore Entities and Digital Payment Channels

Criminals often use shell firms and offshore companies incorporated in tax havens or areas with little rules to hide their identity and make investigations harder. These businesses help move illegal money through complicated networks of payment gateways, cryptocurrency wallets and bank transfers.

Cybercriminals have even more power when people use digital payment methods and with the

rise of fintech platforms, payment aggregators and fast transfer systems, fraudsters may move money swiftly across borders, making it almost impossible for victims or law authorities to find and get their money back and also criminals are using cryptocurrencies more and more to hide the money they make from these kinds of scams. This is because cryptocurrencies are hard to trace and have limited regulatory control in some places.

2.3 Case Study:

India has been a major target for online trading scams since more and more people are investing online, trading apps are becoming more popular, and not enough people know about the risks of these kinds of scams. Over the past ten years, the country has seen a continuous rise in both the size of financial losses and the complexity of cross-border operations.

(a) The Kochi Businessman Scam (2024)

A Kochi-based businessman lost ₹24.76 crore to an online trading scam run by a contact centre in Cyprus. This was one of the most well-known cases in recent years. The victim was tricked into thinking they would get huge returns on overseas trading platforms. At first, a phoney dashboard showed minor gains, which made people want to invest more. When the victim tried to take money out of the trading account, he found that it was locked and the operators were gone[1].

This case shows two important problems: first, the cross-border problem, since the criminals were based in Cyprus, which is outside the direct jurisdiction of Indian law enforcement and second, the illusion of legitimacy, since the scam was backed by professional call centre operations, which made it seem real. Even though a complaint has been filed, the chances of getting money back are still low without strong international collaboration channels.

(b) The Delhi Cryptocurrency Trading Scam of 2023

Cybercrime investigators in Delhi looked into a ₹200 crore fraud in which victims were tricked into putting money into fake cryptocurrency trading sites. The scammers built apps that showed fake profits and even let people make tiny withdrawals to gain investors' faith. The scammers

[1] Kochi Businessman Loses Rs 24.76 Crore in Online Trading Fraud; Cyprus-Based Call Centre Suspected, New Indian Express (Sept. 6, 2025), https://www.newindianexpress.com/cities/kochi/2025/Sep/06/kochi-businessman-loses-rs-2476-crore-in-online-trading-fraud-cyprus-based-call-centre-suspected.

stopped the accounts and disappeared when people put in more money. The investigations showed that the scam was organised through fake businesses and payment gateways that were linked to China and Dubai[2].

This instance showed how cryptocurrency and digital wallets can be used to hide the money from scams. It was very hard to trace funds across borders because cryptocurrencies work on decentralised systems. Indian agencies had a hard time getting help from exchanges in other countries.

(c) Bengaluru Fake Stock Trading App Scam (2022)

The Bengaluru police found a huge scheme in which victims were tricked into downloading fraudulent stock trading apps that looked like real ones, like brokers linked to the NSE or BSE. The apps showed fake dashboards with continuous earnings, which made victims want to put in more money. In the end, the scammers used fintech channels to move money out of the country. The losses were in the crores, and the people running the businesses were linked to networks in Southeast Asia[3].

This example shows how scammers use technology to trick anyone, including smart investors who couldn't tell the difference between real and fake platforms. It also reveals that the app vetting process doesn't work because phoney apps were able to spread freely on social media and private channels before being identified.

(d) The 2021 Hyderabad Chinese-linked Trading Fraud

In Hyderabad, cybercrime officials shut down a fraud network that involved Chinese nationals who utilised Indian front firms and hired locals to register bank accounts for money transfers. Victims were tricked into putting money into trading programs that promised set returns through ads on social media. Payment aggregators, digital wallets and cryptocurrency channels

[2] Delhi HC Denies Bail to Crypto Fraud Accused, Hindustan Times (July 15, 2025), https://www.hindustantimes.com/cities/delhi-news/delhi-hc-denies-bail-to-crypto-fraud-accused-101752515650400.html.

[3] Bengaluru Doctor, 70, Falls into Trap of Investment Fraud, Loses Rs 73 Lakh, Times of India (Aug. 29, 2025), https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-doctor-70-falls-into-trap-of-investment-fraud-loses-rs-73-lakh/articleshow/123571127.cms

were used to send money from investors to offshore accounts[4].

This case showed how weak India's financial system is, since local middlemen were used to hide money that was moving across borders. It also showed how inadequate Know-Your-Customer (KYC) enforcement is in digital payment systems, which let fake accounts run for a long time.

(e) Other Cases That Have Been Reported

Cybercrime departments in states like Maharashtra, Gujarat and Tamil Nadu are still getting more complaints about fake online trading platforms. Some things that are common in these circumstances include:

- Advanced imitation of real trading companies.
- Transactions with many layers that include local mule accounts and foreign remittances.
- Using professional call centres and personalised financial advise to psychologically control victims.

(f) Legal and Policy Consequences

These cases show patterns that keep coming up and have big legal effects:

1. Jurisdictional Barriers: Most frauds happen outside of India, making it hard to use Indian criminal laws.
2. Weak Investor Protection: Victims don't often get their money back since international cooperation is delayed.
3. Regulatory Loopholes: Even if the RBI and SEBI keep an eye on things, bad actors take advantage of weaknesses in monitoring digital platforms.
4. Problems with enforcement: Indian agencies don't have enough cyber forensic experts

[4] *Hyderabad Police Revive Probe into ₹443 Cr Chinese Online Betting Apps Scam*, Times of India (May 6, 2025), https://timesofindia.indiatimes.com/city/hyderabad/hyderabad-police-revive-probe-into-443-cr-chinese-online-betting-apps-scam/articleshow/120939281.cms

or ways to follow people across borders in real time.

The Indian example shows that online trading frauds are not one-time events, but part of a bigger system of cross-border financial fraud that needs coordinated legal and technological countermeasures at home and abroad.

3. Indian Legal Framework Against Online Trading Frauds

India has set up a complex system of laws to control online activity, stop financial fraud, and keep investors safe. But the fast growth of internet trading frauds has shown both the good and bad sides of current laws. The main laws that apply to online trading fraud are the Information Technology Act of 2000, the Indian Penal Code of 1860, the Prevention of Money Laundering Act of 2002, BNS 2023 and sectoral laws like the Securities and Exchange Board of India (SEBI) Act of 1992 and the Reserve Bank of India (RBI) regulations.

3.1 The Information Technology Act of 2000 (IT Act)

The IT Act, 2000 is the main law in India that deals with crimes that happen online. There are a number of rules that apply directly to internet trading frauds:

- Section 43 punishes people who break into, download from, or destroy computer systems without permission. This includes fake trading apps and websites that illegally get or change investor data[5].

- The main law against cyber fraud is Section 66, which makes it illegal to use computer resources to accomplish dishonest or fraudulent things.

- Section 66C is all about identity theft. It applies when criminals use fake digital certificates, stolen KYC paperwork, or cloned websites to pretend to be real brokers[6].

- Section 66D talks about cheating by impersonating someone else using computer resources. This includes contact centre scams where fraudsters pretend to be financial advisors or brokers to trick investors[7].

[5] The Information Technology Act, No. 21 of 2000, § 43 (India).
[6] Id. § 66C.
[7] Id. § 66D.

The IT Act has two problems that make it hard to enforce: (i) its penalties are too light for high-value frauds involving crores of rupees, and (ii) it needs a lot of cyber forensic expertise, which is not always available in state-level police departments.

3.2 The Indian Penal Code of 1860 (IPC)

The IT Act deals with the technological side of things, while the IPC adds to this by making fraud a crime in general. Some important parts are:

- Section 415 specifies cheating, which includes getting victims to put money into fake trading schemes[8].
- Section 420 sets forth the punishment for cheating and dishonestly getting someone to give you property. This law is sometimes used in online fraud prosecutions[9].
- Sections 467 and 468 make it a crime to fake important documents or to do so in order to deceive. This includes phoney KYC paperwork, fake trading licenses, and contracts that are not real.
- Section 471 makes it illegal to use fake documents as real ones. This is what happens when fraudsters provide investors fake certificates.

So, the IPC adds to the IT Act by giving it a solid criminal law base. But its territorial application under Section 2 makes it hard to use when criminals are based outside of India, which makes it less useful in situations when people cross borders.

3.3 The Prevention of Money Laundering Act (PMLA) 2002

The main reason people do online trading scams is to make money, and fraudsters sometimes use complicated financial stacking to hide their illegal profits. The PMLA, 2002 is an important law that helps find and take these profits.

- Section 3 defines money laundering as trying to take part in, or knowingly helping, a process that has to do with the money made from crime[10].

[8] The Indian Penal Code, No. 45 of 1860, § 415 (India).
[9] Id. § 420.
[10] The Prevention of Money Laundering Act, No. 15 of 2003, § 3 (India).

- Section 4 says that people who launder money will go to jail for a long time and pay a lot of money[11].

The Enforcement Directorate (ED) has the power to look into, seize, and take away property that comes from these kinds of schemes.

When money from online trading frauds goes via several bank accounts, fintech channels, or cryptocurrency exchanges, the PMLA comes into play. But the problem is moving money across borders, where working with foreign financial intelligence agencies is necessary for successful enforcement.

3.4 The Securities Regulations and the SEBI Act of 1992

The Securities and Exchange Board of India (SEBI) is the law that governs the securities markets. SEBI's main job is to oversee registered brokers and stock exchanges, but it also has the job of protecting investors from dishonest or unfair trading activities.

- Section 11 gives SEBI the power to oversee securities markets and look out for investors' best interests[12].

- Section 12A of the SEBI Act makes it illegal to trade in a dishonest or unfair way, to trade on inside information, or to manipulate the market[13].

SEBI is very important in real trading situations. But SEBI has a hard time enforcing its rules on fraudulent online trading platforms since they pretend to be overseas brokers or unregistered intermediates.

3.5 Rules from the Reserve Bank of India (RBI)

- The RBI's rules are very important because most of the fake trades in online trading frauds go through banks, payment aggregators and digital wallets.

- The RBI is in charge of the Payment and Settlement Systems Act, 2007, which controls

[11] Id. § 4.
[12] The Securities and Exchange Board of India Act, No. 15 of 1992, § 11 (India).
[13] Id. § 12A.

electronic transactions.

- The RBI's KYC/AML rules say that banks and fintech companies must check who their customers are and report any transactions that look suspicious.

- The Master Directions on Prepaid Payment Instruments (PPIs) and cross-border transfers keep an eye on digital wallets and payment gateways, which are regularly used in trading frauds.

Even with these protections, there are still loopholes in enforcement. Fraudsters often take advantage of mule accounts, insufficient compliance by smaller fintech companies, and regulatory arbitrage between several countries.

3.6 Important Evaluation

The IT Act, IPC, PMLA, SEBI rules, and RBI guidelines work together to make a quite good set of rules for dealing with internet trading frauds. But there are still some problems:

- Limitations of Jurisdiction: Laws are meant to deal with crimes that happen inside a certain area, but they have a hard time dealing with frauds that start in other countries.

- Regulatory Gaps: SEBI and RBI don't always have the power to stop fraudulent trading apps and offshore brokers.

- Problems with enforcement: State cyber units don't have enough technological knowledge to look into complicated financial scams.

- Victim Remedies - The laws that are in place right now focus on punishing the perpetrator instead of giving victims money or property back.

So, even while the Indian legal system has many ways to punish criminals, its inadequate enforcement and lack of cooperation with other countries make it much less successful at stopping online trade frauds that cross borders.

3.7 The Bharatiya Nyaya Sanhita, 2023

The IT Act deals with the technological side of things, while the BNS adds to this by making

fraud a crime in general. Some important parts are:

- Section 318 specifies cheating, which includes getting victims to put money into fake trading schemes and sets forth the punishment for cheating and dishonestly getting someone to give you property. This law is sometimes used in online fraud prosecutions[14].

- Sections 338 and 336 make it a crime to fake important documents or to do so in order to deceive. This includes phoney KYC paperwork, fake trading licenses, and contracts that are not real[15].

- Section 340 makes it illegal to use fake documents as real ones. This is what happens when fraudsters provide investors fake certificates[16].

So, the BNS adds to the IT Act by giving it a solid criminal law base. But its territorial application under Section 2 makes it hard to use when criminals are based outside of India, which makes it less useful in situations when people cross borders.

4. Jurisdictional Issues in Cross-Border Cyber Fraud

One of the most important things about online trading scams is that they happen across borders. Online trading scams take use of the fact that internet has no borders, unlike traditional financial crimes that happen in one place. Scammers might work from one country, send money through another, then go after victims in a third. The fact that actors, infrastructure, and effects are spread out makes it hard for Indian courts and police to figure out who has jurisdiction.

4.1 Jurisdictional Distinctions: Territorial and Extraterritorial under the IT Act and IPC

The Information Technology Act, 2000 (IT Act) has a clear clause that applies outside of India. According to Section 75, the Act applies to any crime that happens outside of India if it includes a computer, system, or network that is located in India. In principle, this law lets Indian authorities go after criminals who run fake platforms or servers that are meant to trick Indian investors.

[14] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 318 (India).
[15] Id. §§ 336, 338.
[16] Id. § 340.

Section 4 of the Indian Penal Code, 1860 (IPC) says that the Code can also cover crimes committed by anyone against a computer resource in India. So, an online scam that started in Cyprus or Dubai but targeted Indian citizens is something that Indian courts can handle.

But enforcing extraterritorial jurisdiction in real life is quite hard. Indian authorities cannot independently investigate or prosecute offenders situated in foreign jurisdictions without the help of such states. This means that the IT Act and IPC's jurisdictional reach is mostly theoretical and depends on how ready and effective international cooperation is.

4.2 Conflict of Laws in Cyberspace: Which Nation Holds Prosecutorial Jurisdiction?

Cyber frauds that cross borders always produce conflicts of legislation. The idea of territorial sovereignty says that the country where the crime happened (like Cyprus) has the most power to prosecute. But from the victim's point of view, India has a better case because the harm happened there.

- This disagreement brings up several important issues: Should jurisdiction depend on where the offender, the victim, or the impacted computer system is located?
- What happens when more than one country claims jurisdiction at the same time, which can lead to prosecutions that are the same or different?

Bilateral treaties and mutual assistance agreements are often used in international law, but they are known to take a long time. In the meantime, criminals are taking advantage of the delay to erase their digital fingerprints, move money, and start again with new names.

4.3 Problems with looking into Cyprus-based and other offshore companies

The Kochi businessman case shows how hard it is to go after offshore companies. Fraudsters often set up call centres or dummy corporations in places with weak regulations, such Cyprus, Seychelles or Caribbean tax havens.

These places were chosen on purpose because:

- Corporate confidentiality rules protect information about who owns what.
- Weak enforcement makes it hard to work quickly with Indian agencies.

- Cryptocurrency exchanges and complicated financial systems offer more levels of privacy.

When Indian investigators ask for information through Mutual Legal Assistance Treaties (MLATs), it can take months to get a response. By then, important digital evidence may have been lost. Also, not all countries have treaties with India, which makes it even harder to investigate.

4.4 India's Legal Limitations in Cybercrime Prosecution

Even if India's laws provide for extraterritorial application, international law concepts of sovereignty limit India's legal reach. India cannot send investigators to Cyprus or Dubai without breaking the rules about territorial integrity. It must instead depend on:

- MLATs for sharing evidence.
- Indian courts send letters rogatory to courts in other countries.
- Notices from Interpol for keeping an eye on criminals across borders.

But each of these methods is slow and full of red tape. When cooperation happens, fraudsters generally sell their assets, close their businesses, and move to new places.

Also, India's choice not to join the Budapest Convention on Cybercrime means that it is not part of the most well-known international framework for working together in real time on cybercrime investigations. This means that India depends a lot on diplomacy between two countries, which might not work against quickly moving financial fraud networks.

4.5 Important Evaluation

The jurisdictional difficulties presented by cross-border online trading crimes highlight a distinct disparity between statutory law and its practical application. The IT Act and IPC give Indian authorities the right to punish overseas criminals, but they often can't do so without help from other countries. Fraudsters are even less likely to be held responsible because of offshore jurisdictions, corporate secrecy, and digital payment mechanisms. India's claims of jurisdiction will stay mostly symbolic unless it improves its ability to work with other countries and

establishes faster, technology-driven ways to investigate across borders. This will leave victims without a way to get justice.

5. International Legal Cooperation in Cybercrime Investigations

Because cyberspace has no borders, domestic legal mechanisms are not enough to deal with the growing number of scams in cross-border online transactions. Indian laws, such as the Information Technology Act of 2000, the Indian Penal Code of 1860, and banking restrictions, have powerful ways to enforce the law within the country. However, these laws don't work as well when criminals are based in other countries. This discrepancy shows how important international cooperation mechanisms are in investigations of cybercrime.

5.1 Mutual Legal Assistance Treaties (MLATs) and Their Shortcomings

MLATs are the main way that India works with other countries on criminal investigations. These treaties give police the power to ask for electronic evidence, freeze bank accounts, or get testimony from people in other countries. But MLATs are known for being slow and full of red tape, and they can take months or even years to process. This delay is especially bad for internet trading scams, as money is quickly laundered through many offshore accounts and cryptocurrency wallets. Also, MLATs must meet the dual criminality criteria, which means that help can only be given if the behaviour is a crime in both places. When a foreign country has weak cybercrime laws, it's hard to work together.

5.2 Role of Interpol, FATF Guidelines, and Egmont Group in Financial Crimes

Global organisations help fight cyber-enabled financial fraud in a different way. Interpol helps its member governments by sending out alerts, coordinating intelligence, and making it easier for investigations to happen across borders. In cases like the Cyprus-based call centre fraud that targeted Indian investors, Interpol channels might give important details about the movements and assets of suspects. The Financial Action Task Force (FATF) also sets global guidelines for anti-money laundering (AML) and counter-terrorist financing (CFT). FATF says that countries must keep an eye on questionable financial transactions, control cryptocurrency exchanges, and stop shell businesses from laundering money. The Egmont Group of Financial Intelligence Units (FIUs) makes it easier for more than 160 nations to share information about suspicious transactions in real time. India's FIU-IND is quite involved, yet providing information is still optional and not legally enforceable, which makes it harder to enforce.

5.3 The Budapest Convention on Cybercrime and India's Decision Not to Sign It: The Good and the Bad

The Budapest Convention (2001) from the Council of Europe is the first international pact on cybercrime that everyone must follow. It sets up a common way for sharing evidence, procedural powers, and collaborative investigations. There are 68 signatures, but India has not joined because it is worried about sovereignty and the fact that decisions will be made by Europeans. The benefits of joining would be that service providers could get to your data faster, there would be clear definitions of cybercrimes and there would be established ways for people to work together. From India's point of view, the downsides are giving up some control over data-sharing rules and being bound by rules that India didn't help establish. Critics, on the other hand, say that India's absence means it can't use streamlined global systems and makes it harder for it to fight transnational cyber fraud.

5.4 Examples of international cooperation that worked and didn't work in fraud cases

Real-world experience shows both the good and bad sides of working together across borders. In the 2018 call centre fraud case, U.S. citizens were tricked by Indian-based operators pretending to be IRS agents. The FBI and Indian authorities worked together to make a lot of arrests in Mumbai. In the Kochi businessman case (2024), on the other hand, a Cyprus-based online trading scam for ₹24.76 crore, the process of finding the suspects and getting the money back was slower because India didn't sign the Budapest Convention and there weren't strong bilateral agreements. These two cases show that cooperation is possible, but it requires on political will, legislative compatibility and proactive enforcement measures.

6. A Global Look at Best Practices

To stop cross-border online trading fraud, we need both strong regulations in each country and proactive worldwide norm and looking at how other places deal with cyber-enabled financial fraud will help India a lot.

6.1 The Digital Services Act and the General Data Protection Regulation (GDPR) in the European Union

One of the most complete sets of rules for digital activity has been made by the European Union. The General Data Protection Regulation (GDPR) (2016) makes it very clear what online

platforms must do to protect user data and requires them to notify users of breaches. This makes it harder for fraudsters to use personal data in online scams. The Digital Services Act (DSA) 2022 has made it easier to keep an eye on online intermediaries and trade platforms by mandating them to be open about their business, do due diligence, and report any fraudulent actions in real time. These frameworks help European law enforcement find fake trading apps and shut down unlawful financial promotions faster than in India, where platform responsibility is still not very clear.

6.2 United States: Enforcement by the Securities and Exchange Commission (SEC)

The U.S. uses a paradigm that is heavily based on enforcement. The SEC is in charge of looking into fake online trading platforms and crypto-investment schemes. The SEC actively uses extraterritorial jurisdiction under U.S. securities law to go after offshore companies that are trying to attract American investors to invest in them. India, on the other hand, has a hard time doing the same thing under its IT Act or IPC. The Federal Trade Commission (FTC) and the Department of Justice (DOJ) in the U.S. also work together to freeze assets, get victims their money back, and file criminal charges. The U.S. can break up cross-border fraud networks by using both its own laws and treaties for international cooperation. For example, the crackdown on BitConnect is a good example of this.

6.3 Singapore and Hong Kong: Regional Financial Centres with Strong Anti-Fraud Laws

Singapore and Hong Kong are important financial centres in the world, and they have strict rules around cyber-finance. The Monetary Authority of Singapore (MAS) requires trading platforms to do thorough due diligence, digital payment service providers to get licenses, and all questionable actions to be reported. The Securities and Futures Commission (SFC) in Hong Kong also keeps a close eye on internet trading platforms and works with banks to stop money laundering. They give out harsh punishments to companies that don't have a licence. Both places also stress public awareness campaigns that warn investors about internet scams. India has started doing this, but it hasn't made it a regular part of its efforts yet.

6.4 What India can do

India can learn a lot from these international experiences:

- Setting up platform accountability rules like the EU's DSA.

- Giving SEBI and RBI more power to enforce laws outside of India, like the U.S. SEC does.

- Following the strict rules in Singapore and Hong Kong, making licensing and monitoring requirements for trading apps stronger.

- Making public awareness campaigns and quick-response systems a part of the system to let potential victims know right away.

7. In India, there are ways to protect victims and make things right.

A lot of academic work focused on enforcement, but protecting victims of internet trading frauds is just as important. The Indian legal system offers several options, but they are not used enough and are too narrow in scope.

7.1 Registering a FIR and making complaints through the Cybercrime Portal

People who have been scammed when dealing online can file complaints with the National Cyber Crime Reporting Portal (cybercrime.gov.in) or file a First Information Report (FIR) under the IT Act, IPC, and PMLA. The cybercrime portal has made it easier for people to report crimes, but victims are often put off by long waits for FIR registration, the fact that smaller jurisdictions don't have specialised investigation units, and the fact that state and central authorities don't work together very well.

7.2 Problems with getting back money that was stolen

Victims' biggest problem is getting back the money they lost. Fraudulent trading platforms sometimes send money through a lot of different offshore accounts, shell companies, or cryptocurrencies, which makes it very hard to trace. International cooperation delays (via MLATs or Letters Rogatory) cause assets to disappear, even when accounts are found. India does not have a specific way to freeze assets that can act on suspicion before it happens, unlike the U.S. or EU.

7.3 Civil Remedies: Protection for Consumers and Getting Back What You Lost

Besides criminal law, victims can also get help via the Consumer Protection Act of 2019 by

treating fake trading platforms as service providers who deliver "deficient services." Victims can also file civil reparation lawsuits or class actions against middlemen who didn't do their duty. But civil remedies don't work as well because of long court cases and problems finding defendants in other countries.

7.4 Compensation Plans for Victims and Their Problems

India has laws that provide compensation to victims under Section 357A of the Code of Criminal Procedure, 1973. However, these laws are mostly meant for violent crimes, not financial scams. State legal services agencies rarely provide victims of cyber financial crimes any money, thus they don't get any real recompense. Countries like the U.S. and Singapore, on the other hand, have set up investor protection funds and compensation boards that aggressively pay back people who have been scammed when they trade online.

8. Policy Gaps and way forward

The examination of India's legal and enforcement frameworks reveals that although current laws tackle specific facets of cyber-enabled financial fraud, considerable policy deficiencies persist, obstructing efficient prevention, investigation, and victim safeguarding

8.1 Need for a Specific Law Against Online Financial Frauds

India now uses a mix of legislation, such as the Information Technology Act of 2000, the Indian Penal Code of 1860, the Prevention of Money Laundering Act of 2002, and financial rules set by SEBI and the RBI. But none of them are aimed at internet trading frauds in particular. A specific law, similar to the UK's Fraud Act 2006 or Singapore's Payment Services Act, 2019, might identify and make illegal fraudulent online financial operations, hold platforms responsible, and set up faster ways to freeze and take assets.

8.2 Making Cross-Border Cooperation Mechanisms Stronger

The most difficult part of fighting cross-border fraud is that the law doesn't always apply. India's reliance on Mutual Legal Assistance Treaties (MLATs) has been insufficient due to protracted processing delays. A possible path forward is:

- Making deals with high-risk countries like Cyprus, Singapore and Hong Kong.

- Working with Interpol, the Egmont Group, and FATF to share intelligence.
- Setting up a South Asian or Indo-Pacific Cybercrime Cooperation Treaty could help with faster evidence-sharing and asset recovery in the region.

8.3 Improving the ability to do cyber forensics and track financial intelligence

Fraud that uses the internet thrives on things like anonymising technologies, shell companies, and complicated financial transactions. India needs to build more cyber forensic labs, give law enforcement authorities tools for blockchain analytics to help them track cryptocurrencies and work more closely with overseas counterparts in the Financial Intelligence Unit (FIU-IND). Dedicated cyber financial crime task forces, made up of experts from the RBI, SEBI, CBI and state cyber cells, might make response times faster and the possibilities of recovery better.

8.4 Suggestions for India to join the Budapest Convention or a Regional Cybercrime Treaty

India has historically opposed joining the Budapest Convention on Cybercrime (2001) due to concerns about sovereignty and the treaty's Eurocentric focus. But India's absence from this global framework makes it harder for other countries to work together on cybercrime investigations. Joining would make it easier to get electronic evidence from other countries more quickly and make joint investigations stronger. India might also take the lead in creating a regional cybercrime pact for the Asia-Pacific area that would standardise definitions of crimes and make it easier for neighbouring nations to share evidence.

9. Conclusion

Cross-border internet trading frauds constitute a growing threat to India’s digital economy, as proven by high-profile incidents like as the Kochi businessman’s ₹24.76 crore loss to a Cyprus-based trading scam. These crimes take advantage of gaps in the law, inadequate international cooperation frameworks, and fragmented domestic legislation, making it hard for victims to get help.

The analysis shows that India's IT Act, IPC, PMLA, SEBI and RBI rules are a good start, but they don't go far enough to stop online trading frauds that cross borders and use advanced technology. The main problems are that there isn't enough enforcement of jurisdiction, there

are delays in exchanging evidence between countries, there aren't enough ways to compensate victims, and there aren't enough cyber forensic experts.

- India needs to do the following to make its response stronger:
- Make a law that specifically deals with internet financial fraud.
- Reform the MLAT, make bilateral treaties, and join global or regional cybercrime conventions to improve collaboration between countries.
- Put a lot of money into cyber forensic skills and financial intelligence.
- Put victim-centered solutions, such compensation funds and quick civil remedy systems, at the top of your list.

In the end, India's effectiveness in fighting transnational online trade frauds will depend on how well it can balance making changes to its own laws with working with other countries. A legal policy that looks to the future would not only protect investors, but it will also make India look more credible as a safe and strong digital economy.

REFERENCES:

Primary Legal Sources

1. Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
2. Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).
3. Indian Penal Code, No. 45 of 1860, INDIA CODE (1860).
4. Prevention of Money Laundering Act, No. 15 of 2002, INDIA CODE (2002).
5. Securities and Exchange Board of India Act, No. 15 of 1992, INDIA CODE (1992).
6. Reserve Bank of India Act, No. 2 of 1934, INDIA CODE (1934).
7. Code of Criminal Procedure, No. 2 of 1973, INDIA CODE (1973) § 357A.
8. General Data Protection Regulation, Regulation (EU) 2016/679, of the European Parliament and of the Council, 2016 O.J. (L 119).
9. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).
10. Fraud Act 2006, c. 35 (UK).
11. Payment Services Act 2019, No. 2 of 2019 (Sing.).
12. Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167 (Budapest Convention).

International and Institutional Sources

1. Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (updated Mar. 2022).
2. Egmont Group of Financial Intelligence Units, About (2024), https://egmontgroup.org.
3. INTERPOL, Cybercrime Programme (2024),

https://www.interpol.int/en/Crimes/Cybercrime.

Government and Regulatory Sources

1. Financial Intelligence Unit – India, Ministry of Finance, Annual Report 2022–23 (2023).

2. Securities and Exchange Commission (U.S.), Investor Alert: Fraudulent Online Investment Offers Involving Trading Platforms (2022).

3. Securities and Futures Commission (Hong Kong), Annual Report 2022–23 (2023).

4. Monetary Authority of Singapore (MAS), Enforcement Actions and AML-CFT Regulations (2023).

News & Case References

1. Kochi Businessman Loses ₹24.76 Crore in Online Trading Fraud; Cyprus-Based Call Centre Suspected, The Hindu (May 20, 2024), https://www.thehindu.com.

2. US-India Call Centre Fraud: Dozens Arrested in Mumbai for Scamming Americans, BBC News (Oct. 6, 2018), https://www.bbc.com.

3. BitConnect Founder Indicted in $2.4 Billion Crypto Ponzi Scheme, U.S. Dep't of Justice (Feb. 25, 2022), https://www.justice.gov.

Secondary Academic Sources

1. Apar Gupta, The Information Technology Act, 2000: A Legal Review of Cyber Offences in India, 12 Nat'l L. Sch. India Rev. 45 (2021).

2. Pavan Duggal, Cyberlaw: The Indian Perspective (4th ed. 2022).

3. Ritu Agarwal, Cross-Border Cybercrime and Jurisdictional Dilemmas in India, 8 Indian J.L. & Tech. 112 (2020).