# Directorate of Distance Education
## Centre for Distance and Online Education (CDOE)
## NALSAR University of Law, Hyderabad

**Reading Material**

# ONE YEAR ADVANCED DIPLOMA IN CYBER LAWS

# 1.2 E-COMMERCE & TAXATION


**By:**

## Mr. Na. Vijayashankar

Privacy and Data Protection Consultant

Visiting Professor – NALSAR

Print 2019
Re-Print 2023
(For private circulation only)

# Table of Contents

# Chapter 1: E Commerce & Taxation

**Syllabus:** E-Commerce - Salient Features, On-line contracts, Mail Box rule, Privity of Contracts, Jurisdiction issues in E-Commerce, Electronic Data Interchange, E Advertising, E Procurement, E Governance, Intermediaries,Fintech Business, Raising Capital for E Business, Venture Funding, FDI etc.

**Learning Objectives**

After studying this chapter, the student should be able to understand the scope of E Commerce and the intricacies of E Business. Students would understand what are the different components of E Commerce and would also be exposed to the important legal aspects involved in E Commerce such as E-Contracting.

## Definition and Scope of E Commerce

E Commerce is not all Amazon or Flipkart or Snapdeal or e-bay who is the prominent online platforms for buying and selling goods. Apart from E Banking, E-Trading which are specific segments of services marketing, there are companies like Uber and Ola or travel sites like Trivago and Goibibo which represent "Aggregators" of other service providers, OLX, Quikr kind of companies which provide platform for individuals to trade in second hand/used products, real estate companies such as 99acres.com etc. The Mobile Apps such as PayTm, PhonePe, etc. also provide e-commerce platforms along with E Banking. There are also E Education and E- Governance which has components of E Commerce supporting the Education or Governance activities. Companies providing services such as "Driverless Cars", "Smart Power Network", Smart City Services" also have E Commerce/E Governance/E Services.

Study of E Commerce therefore involves the different aspects of Technology, Law and Consumer Behaviour in all the above types of activities.

E-Commerce essentially means conducting "Commerce" over the network. "Commerce" essentially means "Exchange of Goods" and could involve "Money" as the common medium of settlement of value of exchange.

While it is popular to define "E-Commerce" as "Commercial Transactions conducted across Internet or an electronic network" we can better define the term as

> "E Commerce means exchange of goods and services for a consideration using electronic documents".

This definition is more useful in the application of law since Indian Cyber Law defines the law in

relation to "Electronic Documents" and not in relation to "Internet" or "Network Devices". "Electronic Documents" by legal definition in India are any "Binary Expressions".

This definition would make the study of E Commerce neutral whether it is a transaction over Internet or an Extranet or even an Intranet or partly over an electronic network and partly otherwise. Under this concept transactions are also independent of the devices used and hence there is no difference between commerce conducted on computes, mobiles or any other device which processes data expressed in the form of electric, magnetic or electronic impulses.

Study of E Commerce therefore involves the study of the technology that enables exchange of goods through online communication and settlement through online means.

As regards laws applicable to E Commerce, we may appreciate that the origin of Cyber Laws itself can be credited to a felt international need for a legal base for Electronic Commerce, because of which UN came up with its model law on E Commerce (UNCITRAL Model Law on E Commerce-1996) which was adopted by the member countries like India into laws such as Information Technology Act 2000 (ITA 2000). The emerging laws such as the Data Protection Laws, the IoT laws, the Big Data laws, Artificial Intelligence laws, are all closely linked to E Commerce and related issues.

Further, study of Consumer behaviour in E Commerce transactions is a special branch of study and should be part of E Commerce study. Hence components of E Commerce management including "Advertising" in the E Commerce area, designing selling strategies, the governance of discounts, pricing are also specialized activities on their own.

Similarly, taxation of E Commerce poses challenges of its own due to the porous international borders through which E Commerce operates and introduces jurisdictional issues both under international taxation and local taxation under GST scenario.

Along with this, “Crimes” associated with “E-Commerce” are “Cyber Crimes” and could be a replica of physical society crimes in the online context or some new innovative crimes which have cross border implications.

“Goods” which are the subject matter of E Commerce themselves may be “Physical Goods” which need to be delivered from the seller to the buyer. Goods can also be “Soft Products” which can be delivered across the network itself. “Software” is an example of such a “Soft Product”. A Writer writing an article and delivering it online through e-mail or otherwise for a price is also selling a “Soft Product” and conducting E Commerce.

Money used in E Commerce could be “Cash” as in physical society (when Cash On Delivery) is used or digitally held cash as in online payments from bank accounts or mobile wallets or even pure digital money such as crypto currencies.

E Commerce is related to two other terms E-Business and E-Governance. E-Business is a term that may be used for conducting business using electronic documents. E-Commerce may be considered as a subset of E-Business. E-Governance is a term used when one of the parties to the transaction is a Government. E-Governance may like E-Business may always not relate to exchange of goods or money. In some cases it may involve the delivery of government services to the Citizens for a price, where it is nothing different from E-Commerce in the non-Government sector.

When a Government uses technology for internal management of its affairs the activity is often called E-Government whereas E Governance is a term restricted for use when a Government to Citizen Interaction takes place with the use of Electronic Documents.

In the Corporate scenario also we have a scenario where a Company uses software to conduct its internal Governance. Fortunately we do not have a confusing terminology like E Government Vs. E Governance to contend with regarding digitized corporate management.

Under E Commerce, E-Banking, E-Stock Trading, E-Insurance etc. are huge business segments and may require an in depth study. Also subjects such as E-Advertising, E Taxation E Procurement, E Governance, Raising funds for E Commerce etc. also require an in depth discussion. Accordingly some of these topics are discussed in greater detail in the following chapters/segments.

## Components of E Commerce

The Components of E Commerce include

a) Virtual Place where the Buyer and Seller meet and exchange services

b) Sourcing Products or Services to sell or buy

c) Delivery and Logistics management Systems

d) Setting up Payment Systems

e) Customer Acquisition including Advertising, Pre Purchase Negotiations

f) Post Purchase Service management including dispute resolution

g) Managing financial requirements from raising venture capital funds, innovative strategies to boost sales, borrowing or crowd funding etc.

h) Managing E Contracts

i) Management of Taxation Issues

j) Management of Information Security Issues

k) Management of Privacy and International legal issues

## A Virtual Business place

Just as a physical business has to have a place to set up a factory and a place to set up the administrative and marketing office, an E Commerce company has to identify the virtual place to set up and conduct its business. This could be a "Website" or a "Mobile App" and ideally both.

The name of the website or the App has a relation to the "Brand" name of the product and the company and is part of the early decision making of the E Commerce company.

Whether the hosting has to be in the cloud or in servers of a particular country or service provider, whether the mobile App has to be on Android or iOS or both are also decisions that establish the E Presence.

Many times, E Commerce companies after establishing their brand could be confronted with debilitating challenges on their domain names that could cause a serious hurt to the business. The Data Protection laws as they are emerging have an impact on the hosting decisions since once established, systems will be difficult to migrate from one server system to another.

Trademark, Copyright or Patent laws often interfere with the selection of domain names or support technologies and they need to be addressed right at the beginning.

## Products and Services

E Commerce provides opportunities to source products and/or services from different suppliers. Many E Commerce companies specialize being "Market Places" and provide a platform for their members to sell collecting some service charges. Often in such circumstances, the E Commerce companies find the need to pitch in with their own brand value to afford credibility to a product and this develops a few "Trusted Supplier Tag" to some of the sellers.

In order to improve delivery and cut on service delay, some E Commerce companies may like to maintain inventory in their own name or in their own godowns in space leased out to the suppliers. Whether an organisation is merely a "Market Place" and not does a supplier may be necessary from taxation view point besides other managerial considerations.

Often an E Commerce service provider adds value to the product by not only the normal business strategies used by a large distributor but because of the technology. For example, many products can be configured and customized online from components sourced either from the same supplier or from different suppliers.

Financially innovative payment terms can be provided to change the perception of the product itself and make it look like a different product. Aggregation of supply sources can be used to create perceptions of value.

Hence "Sourcing" in E Commerce companies can be more than mere "Purchase Management".

## Delivery and Logistics management

Delivery of products and managing logistics is an important aspect of efficient management of E Commerce. When this is outsourced, problems of inefficiency and frauds at the sub-contractor level also have to be managed with appropriate security and monitoring including insurance.
Sometimes availability of better delivery options gives raise to development of new products and services such as "Uber Eats".

"Preferential Delivery" can also be a revenue generator like "Amazon Prime".
Since "Availability" of product is the key for many purchase decisions, efficient delivery management is often the parity breaker when a consumer is evaluating purchase from one E

Commerce supplier or the other. Products which are part of “Impulse purchases” would depend heavily on “Next Day Delivery” or “Same Day Delivery”. For products such as “Food” such as “Swiggy”, very quick delivery is the USP.

Hence logistics and delivery management is an important component of E Commerce.

## Payment Systems

E Commerce sometimes adopts the “Cash on Delivery” model where the payment system is de linked from the transaction. In such cases E Commerce may be run on an E-Ordering” mode with lesser financial risk for the consumer.

However full service E Commerce has to include the online option which could be through transfer of money from the Bank account of the customer or from his prepaid wallet accounts or the debit or credit cards or prepaid cards.

Some of the major E Commerce players have either taken over other payment solution companies or are setting up branded payment solution companies themselves. Ola Money, Amazon Pay are examples of such in house branded payment solutions. Companies like Uber have presently stuck to outsourced payment options such as PayTM.

Since E Commerce companies need to remain neutral to the consumer preference for the choice of payment systems, it is imperative that E Commerce Companies need to provide multiple payment options and not restrict themselves to a single payment option though they may have some preferences due to internal tie ups, low charges etc.

Hence most E Commerce companies make use of intermediary services called “Payment Gateways” and allow multiple payment options. The payment gateway service providers develop their own relationship with Banks to accept bank transfer, with VISA/Master/Amex to accept credit cards or debit cards. In India the NPCI is promoting RuPay and UPI apps and provides the payment gateway services.

The Payment gateways have “Merchant Relationship” with the E Commerce Companies and in the back end use the services of VISA etc. to verify the availability of funds in the card holder’s account and settle payment with the Card Issuing Banks.

Card Issuing Banks maintain the Banker-Customer relationship with the Card Holder and after settling the payment to the Merchant Banks, settle the payment with the customer with its own payment terms.

E Commerce transactions which are conducted online are classified as "Card Not Present" transactions since the merchant establishment does not have physical card of the customer in its possession. Hence, the identity of the customer has to be established only in the virtual environment.

Initially, card companies were using what was called the CVV number which is printed on the back of a physical card and its entry in the E Commerce payment gateway was considered an indication that the customer was in possession of the Card.
RBI has now made it mandatory that E Commerce Companies should use at least a 2 Factor authentication where apart from the entry of the CVV number, a second identification which could be a PIN sent through mobile or e-mail or a separate additional password set by the Card Company or VISA/Masters.

However, disputes do arise many times since CVV may be spoofed through technology intervention or through phishing/vishing. These need to be settled as "Frauds" as per the laws applicable.
Sometimes E Commerce Companies face issues related to non-supply of goods by the sellers or selling of substandard goods or return of goods. In such cases the E Commerce Companies need to "Reverse" or raise a "Charge Back Request". When the E Commerce companies itself raises a reverse transaction, the Card issuing bank considers it as a cancellation of order and automatically credits the money back to the customer's card account.

However, if the "Charge Back" request is made to the card issuing bank, then there is some times a resistance from the Credit Card issuing bank since it has to deal with the Banker-Customer relationship at the customer's end and the Business relationship with the E Commerce company or the Payment Gateway.

The law in such matters is clear that the Credit Card relationship between the Customer and the Card issuing bank is one of "Banker Customer" and supported additionally by the Card issuing contract. Since most of the time this is a "Standard Form Contract" and is in conflict with the Banker Customer relationship, disputes need to be settled in the Courts or by the regulator. More about this is discussed in subsequent chapter on E Banking.

From the E Commerce perspective, it is necessary for the organization to find out a reliable Payment Gateway service provider and enter into a good contract with him and also monitor the relationship.

Some payment gateways maintain good risk management systems that would flag fraud attempts at an early stage and prevent misuse of Cards. E Commerce Companies need to identify such service providers as part of their "Information Security Measures" which is also discussed in greater detail subsequently.

## Types of E Commerce

E Commerce may involve transactions of a business entity, and a consumer, or a Government. Accordingly E Commerce transactions can be classified into the following categories:

1. B2B: Business to Business
2. B2C: Business to Consumer
3. C2C; Consumer to Consumer
4. G2C: Government to Citizen
5. C2G: Citizen to Government

B2B transactions involve two business entities completing their buying and selling of goods online. E-Tendering, E-Procurement are part of the B2B transactions. Consumer Protection Laws do not affect B2B transactions.

In B2B transactions, both parties are knowledgeable and both have the capability to adopt appropriate security measures.

When contracts are entered into between the parties, it is possible for them to use advanced technical measures such as the Digital Signatures. Since there is no "Dominant Party", the operation of a "Dotted Line Contract Principle" or "Standard Contracts" or "Unconscionable contract" (explained later) is less likely.

In a B2C transaction however, one is a dominant party and may present a contract which is unconscionable and containing onerous clauses which the other party may be forced to accept.

At the same time the consumer is less knowledgeable about the product and hence would depend on the "Warranty" provided by the seller or place reliance on the "Brand Reputation".

In a C2C transaction both parties are individuals who use a platform of an E Commerce service provider. In such a case the E Commerce Service Provider is an "Intermediary" and is bound by the legal responsibilities hoisted on the intermediary to ensure fair e-commerce transactions.

In the G2C or C2G transactions, there are serious legal rights that are created such as when a tax payment is made to the Government etc. If the transactions fail, constitutional rights may get infringed and serious consequences may follow.

In terms of Privacy Rights also, dealings with the Government give raise to constitutional issues different from the issues that arise in a transaction with a business entity. The discussion on the use of Aadhaar in India and the Supreme Court decision in the Puttaswamy Judgement[i] is indicative of this differential application of law.

Thus the status of the parties entering into transaction has a significant effect on the E Commerce business. Similarly, the residential status of the person conducting an E Commerce transaction will have impact on whether the transaction becomes an Import or Export or have different implications in terms of taxation. All these factors need to be taken into account when E Commerce business is structured.

## Online Contracts

Online Contracts are contracts that are entered into with the exchange of the offer and acceptance documents online. A detailed discussion about Digital Contract is out of scope of this section. We can however recall some salient features of digital contracts as are relevant to online contracts.
The law of "Digital Contracts" in India are derived out of the Indian Contract Act 1872 (ICA) read along with the provisions of Information Technology Act 2000. (ITA 2000)

Under the ICA, a contract is an agreement enforceable under law. A Contract is entered into between two parties who are competent to contract (i.e.: not a minor, undischarged insolvent or of unsound mind) for a legal objective, under a free consent and for a valid consideration.

Contracts can be "Oral" or "Documentary". However all online contracts are "Documentary" since even recordings of spoken words are electronic documents.

In the ICA, there is no legal difference between Oral and Documentary contract except the hurdles the "Oral Contract" places in terms of "Evidence" to resolve disputes particularly in terms of detailed covenants in the contract.

Oral Contracts need to be often proved with the presentation of "Witnesses" who can prove the agreement or its covenants as specifically stated by the parties in their presence. They will be "Eye Witnesses" for the Contract formation.

Contracts can also be "Implied" by the conduct of the parties and are called "Implied Contracts". Implied contracts could be formed when there is no documentation and when there are no "Eye Witnesses".

Documentary contracts are entered into with an "Offer Document" issued by one of the contracting parties which is "Accepted" by the other. Where the recipient of the offer document does not agree with the offer document in its entirety, he raises the counter suggestions which becomes a "Counter Offer". The "Offer" and "Counter Offer" will continue until all the terms of one version of the offer/counter offer becomes acceptable to the other party and he conveys his acceptance.

The conveyance of acceptance to an offer brings the contract to life.

In the world of "Online Contracts", an offer document can be sent by e-mail and the acceptance can be provided by a return e-mail.

However, often online contracts are concluded by one party displaying his terms on a web page to which the other party accepts by clicking on a button which may say "Accepted" or "I Agree" etc. Under the ITA 2000 as amended in 208 (ITA2000/8) an Electronic Contract can be concluded by an offer and acceptance documents exchanged with digital/electronic signatures of both parties. Since an electronic document (Other than the excluded documents under Section 1(4) of ITA 2000/8) are equivalent to paper documents and an authentication as per Section 3 or 3A of ITA 2000/8 is equivalent to a "Signature", an electronic offer with a digital/electronic signature and an electronic acceptance with a digital/electronic signature is a valid documentary contract in India
In the case of online contracts where undigitally signed e-mails are used as "offer" and "Acceptance", or when the "I Agree" button is clicked on the webpage, the formation of contract does not fulfil the terms of a written documentary contract.

Such contracts therefore do not have the equivalence of a written documentary contract.
The Contract formation through the clicking of a button ("I Agree") is often referred to as "Click-Wrap" contract and may have recognition in US. However, in India, "Click-Wrap" contracts are as good as "Implied Contracts" only.

It can however be accepted that the E Commerce industry has made it a practice to make use of "Click Wrap" contracts and for ordinary E-Commerce contracts, it has become an accepted business practice though we do not rule out such contracts being rejected by an Indian Court when challenged.
As an "Implied Contract", Click-Wrap contracts can be strengthened by firstly making the "Click" a "Consent based on some affirmative action". Example could be to tick a check box, or enter a Captcha or enter an OTP etc.

The "Implied Contract" can also be fortified with collection of "Meta Data" associated with the activity.

However Click-Wrap Contract will remain a form of contract which in India will be subject to questioning.

It may be considered therefore be technically considered as a "Voidable" contract.

Another problem of "Click-Wrap" contracts in the E Commerce scenario is that such contracts are almost always "Standard Form Contracts" or "Dotted Line Contracts". In such contracts, one of the parties which is in a "Dominant" position, gives a "Take it or Leave it" offer to the other who has no option but to accept it as it is or refuse the contract and the attendant service in toto.
This is certainly the case in the B2C transactions though it may not be so true of B2B contracts though if the formation of contract is through "Click-Wrap" method, the "Dotted Line Argument" can always be produced as a defence to invalidate the contract.

In India the law on such contracts has been clearly laid down in many of the Supreme Court decisions on "Unconscionable contracts" including the CERC Vs. LIC of India (1995 AIR 1811, 1995 SCC (5) 482) and the related citations. In such contracts, it is the duty of the dominant party to sufficiently highlight what could be an unfair one sided covenant of the contract and obtain specific consent from the other party, failing which the contract may suffer from "Lack of meeting of minds".

Indian law had permitted the use of "E-Sign" as a digital signature equivalent for real time transactions which could be used for obtaining valid signatures on online forms by any contracting party. Unfortunately, without appreciating the benefit of this system, the honourable Supreme Court in its Aadhaar Judgement of September 26, 2018 virtually banned the use of e-Sign by private companies. Hence this option for validating the online contracts was lost.

However, UIDAI (Unified Identity Authority of India) has come up with a scheme of "Virtual Aadhaar ID" as well as "Offline Aadhaar Authentication" which could be used in conjunction with the activity of a "Certifying Authortiy" to issue one time digital signing certificates as in the case of e-Sign. (Appropriate notifications in this regard are awaited as on the date of this writing).
A work around to the problem of obtaining valid signatures on online forms in the absence of e-Sign has been provided in the private sector in the form of CEAC-EDB (CEAC-Evidence Drop Box) [ii] which uses the provisions of Section 65B of Indian Evidence Act, where a third party can provide witness to an electronic event by certifying the electronic documents that evidence the activity.

## Shrink-Wrap Contracts

Shrink-wrap contract is a term which is used in cases where an acceptance of a contract is recognized with the event when the acceptor opens a shrink wrapped package without fully being aware of the terms of offer and being aware of only a few salient features.

An example of such a contract is when a software is delivered on a shrink-wrapped CD with the condition that "If the shrink-wrap" is opened, the software is deemed to have been accepted as per the terms of the End User License Agreement (EULA) contained within the document.

The accepted norm in such cases is that the outer package should indicate the presence of a detailed contract inside and the user is presented with the electronic contract immediately when the CD is inserted into the user's computer and consent obtained say by registration of the product or otherwise before the software becomes operational.

## Digi-Meta Contracts

In the context of "Digital Contracts", wecan also recognize a new type of contracts which is a "Hybrid Digital Contract".
The definition of a hybrid "Digi-Meta Contract" as Naavi[iii] defines is a Contract where any one of the components of the contract formation instrument is rendered in electronic form and the other in paper form.

In other words, a Contract where either the "Offer", "Acceptance", "Performance", "Consideration" or any other component is in electronic form while some other component is in paper form can be classified as a "Hybrid Contract" or more specifically a "Digi-Meta Contract".

An example of a Digi-Meta Contract is

l) An offer is sent by paper and acceptance is sent by e-mail with unmistakable reference to the paper offer. Or vice versa.

m) The contract is made on paper but the object of the contract and the performance is in the form of an electronic document. E.g.: Contract for designing and hosting a website

n) Contract is made on paper but the payment is made through online payment

o) Consideration for a contract is paid in Crypto Currencies

p) Authentication to an electronic document is expressed in terms of a hash value written in a paper document with appropriate reference which is physically signed. (hybrid authentication)

q) A person becomes a member of a website, pays money online by converting his physical cash such as Rupees or Dollars and acquires some digital rights/properties.

r) A Contract which may be an ordinary oral or paper based documentary or an implied contract or a digital contract or a digi-meta contract where the dispute resolution is mandated through an Online Dispute Resolution mechanism.

The Digi-Meta contract is identified as a type of contract because of the difference in the formation of such contracts. Otherwise the inter-se liabilities of the parties are determined by the Indian Contract only.

The specific areas where the Digital Contracts need to be especially distinguished are in terms of the "Evidence" to be produced to prove the formation of the contract and the applicability of the different covenants in the contract.

## ITA 2000/8 on Online Contracts

In online contracts in an E Commerce context, quite often, the consumer responds to an E Commerce Company through a website and a server of the E Commerce Company which sends automated responses on behalf of the company.

The response could be as mundane as an "Acknowledgement" in respect of a complaint or a request etc. or a more detailed "Counter Offer".

In some instances the service is offered by a website through a "Terms and Conditions" document which carries the button "I Agree" which the customer clicks in acceptance. The wordings used in the document and how the system is configured subsequently, determine if the document is an "Offer" or an "Invitation to Offer".

An “Offer” is converted into a contract if the customer “Accepts” by the Clicking of the button “I Agree”. On the other hand, an “Invitation to offer” when “Accepted” will generate an “Offer Document” from the customer which needs to be accepted by the E Commerce service provider before it becomes a contract.

If the Terms indicate that “Registration” of the software or the client is “ mandatory”, then when the customer submits a registration request, it is like a “Offer” based on the “Invitation to offer” contained in the Terms. When the Registration is confirmed and the contract becomes operational, key to use the service gets generated and is sent to the consumer. The irrevocable acceptance of the contract occurs when the key is actually “received” by the consumer.

In the above process, there are several automated responses that are generated by the server without any manual intervention. Some of these can go into a dispute.
Further when we distinguish between the “Offer” and “Invitation to offer”, we also introduce an element of doubt as to when did the final irrevocable acceptance happen and where did it happen? This can have implications in a dispute.

Hence the law of online contracts need to define how the automated responses of servers are to be accounted for and how the time and place of formation of a contract need to be established.
Fortunately, the Indian Cyber Law in the form of Information Technology Act 2000 as amended (ITA 2000/8) clarifies on all these aspects.

ITA 2000 had provided equivalence of paper and electronic documents so that contract formation could be recognized when the offer and acceptance in a contract was done through an electronic document. However in the amendments of 2008, a further clarification was added in terms of Section 10A to confirm that

“Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.”

ITA 2000 itself had provided clarification on how the automated server responses as well as the time and place of a contract can be determined.

Accordingly, under Section 11, “Attribution” to an electronic document is defined as

"An electronic document shall be attributed to the originator if it was sent by the originator himself, or by a person who had the authority to act on behalf of the originator in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically"

The law therefore recognizes an "Originator" for every electronic message and the "Originator of a message that constitutes the Acceptance in the case of an online contract is the person to whom the acceptance is attributed and is deemed to be the contracting party".

If a server is programmed to send a message on behalf of the originator automatically, then the person who causes the system to behave automatically becomes the originator.
The "Owner" of the automated device therefore becomes the originator.
In view of this provision, in Indian law, the E Commerce website/facility owner is always the "Originator" of an automated server response. This argument holds good even when an automated "Chat Bot" answers on behalf of the E Commerce service provider or even a humanoid robot like "Sophia"[iv] operates the responses on behalf of the service provider.

ITA 2000/8 also provides clarifications on how to determine the "Time and Place" of a contract "if the contracting document does not specify otherwise".

According to section 13 of the ITA 2000/8[v] an online contract occurs when the final acceptance message leaves the sender's system and enters the receiver's system.

There are a few uncertainties that we need to deal with in this transmission of the message since the sender's electronic system may be in some geographical jurisdiction and the receiver's electronic system may be in some other geographical jurisdiction and the transmission has to travel from one system to other through many intermediary systems.

In this transmission, the message may be lost or delayed or even tampered with.

What Section 13 states is that a message is deemed to have been sent as soon as the message leaves the system of the sender. Hence it becomes an irrevocable communication as soon as the message leaves the sender's system.

At the same time, the time of receipt by the receiver is recognized as the time of entry into his system. Here the law makes another distinction. If the Receiver has multiple systems, has designated a specific system to which the communication is to be sent, and the message is sent to

such a designated system, then receipt occurs at the time the message enters the system. However, if when such a designated system exists in the contract, the sender sends the message to a different system (also owned by the receiver), the receipt occurs when the receiver opens the message.

If therefore a dispute occurs on when the message was received, the fact whether a system (e.g.: an email address say xyz@gmail.com or xyz@yahoo.com) had been designated by the receiver and whether the sender sent the message to the designated address or not becomes relevant.

As regards the jurisdiction to be applied for a contract, in order to determine the place where the final acceptance to an online contract is provided, ITA 2000 provides the following guideline.

a) In the case of individuals the place of residence is deemed to be the place of usual residence.
b) In the case of Business entities, the usual place of residence is the "Principal place of business"
c) In the case of Non Business organizations, (e.g.: NGOs) usual place of residence is the "Registered Office"

ITA 2000 also clarifies the effect of and the need for the recipient to send an "Acknowledgement" of a message to make it effective.

Under Section 12 of ITA 2000/8,

a) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
b) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Where the originator has stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by – any

communication by the addressee, automated or otherwise; or any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

We may reiterate that the above provisions may be overridden by specific mention in the contract.

However, we have already stated that in the Indian Context Click Wrap contracts are not recognized and an undigitally signed contract is only an "Implied Contract". Hence the default provisions of the ITA 2000/8 under sections 11, 12 and 13 would be applicable in derogation of any specific mention of the attribution, acknowledgement, time and place or jurisdiction mentioned in the online terms and conditions document.

Some may refer to this set of provisions as well as the liabilities of intermediaries to the transmission discussed in the following paragraphs as a "Mail Box Rule".

## Intermediaries in Transmission

We have discussed above that the formation of an electronic contract is influenced by the time of receipt of the final acceptance. The jurisdiction for dispute resolution arising out of an online contract may also depend on the place where the offer and acceptance are exchanged.
However, technically speaking, after a message leaves the control of the sender and until it reaches the receiver, it is floating around in the Cyber Space. In fact it would have been broken into multiple data packets which may take different routes to ultimately come together at the destination and re-assemble themselves.

In this process of transmission, there are multiple intermediaries and any of them may commit mistakes which affect the contract. An acceptor might have sent the acceptance and immediately cancelled the acceptance but it might have reached the other party. Similarly, sender of a message might have requested for an acknowledgement and the acknowledgement message could have been lost in transit.

In all such cases, we have a situation where there is a dispute to find out who is responsible for the mistake.
The Cyber Law recognizes a role for "Intermediaries" who act as carriers of messages. According to section 2(w) of ITA 2000/8, an "intermediary" is defined as follows:

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to

that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

Simultaneously Section 79 of ITA 2000/8 and the accompanying rules define the "Due Diligence" to be followed by an "Intermediary" in order not to be held liable.

Though the definition of an "Intermediary" can be applied to the "Data Transmission Intermediaries" who carry the online offer and acceptance messages, the Section 79 is drafted more to address the requirement of Privacy protection when the intermediary comes to handle personal data. As per the terms of Section 79, the data transmission intermediaries which include ISPs, MSPs etc will not assume any legal liability for data transmission loss. The Internet technology has an inherent check within its protocol to ensure that all the data packets sent from one source do reach the other source. The SMTP service providers and E Mail service providers also follow certain systems where by unsuccessful transmissions are flagged and reported back to the sender.

Hence there would be residual disputes that remain to be settled between the sender and the receiver of an online contracting party.

In such a situation, one additional parameter that comes into relevance is "Is the intermediary an agent of the sender or the receiver"? If the intermediary is an agent of the sender, then any deficiency of service of the intermediary is the responsibility of the sender. If the intermediary is the agent of the receiver, them the responsibility for any deficiency of his service shifts to the receiver.
This is part of the rule which is followed when two people in the physical society use the services of a courier or a post office to exchange documents.

If therefore a person visits voluntarily a website and does some act, it may be considered as his voluntary action in virtually visiting the electronic space of the website and actions done there in are under the rules set by the website. If therefore an e-mail is generated by the server and sent to the visitor, then the E Mail transmission is the responsibility of the website. If however, a person leaves the website, goes back to his electronic space and sends an e-mail, then the E mail transmission is the responsibility of the sender.
We must recognize that Cyber Jurisprudence on Online Contracts is still under development in India and at present even Courts are often mis-directed by the dominant industry practices and commercial constraints.

The adversarial system of our judicial system also makes Courts incapable of coming to an interpretation of law unless it is brought to their attention by the counsels.
What is presented above is the popular school of thought and could be subject to further academic debate for developing the Cyber Jurisprudence in Online/Digital Contracts.

## Privity of Contract

In a situation where there is a contract between two parties, one of whom or both use the services of sub-contractors who are "Agents", a question arises as to whether a contracting party can hold the downstream contractor of the counter party liable for any wrongful loss caused to him.
In such cases it becomes necessary to establish if any "Privity of Contract" exists between the party which raises the dispute and the party on whom the liability is hoisted.

It is a common principle which is called the "Privity of Contract" which states that "No one but one of the parties can go to court and enforce the contract even if the contract was to operate to a third party's benefit"

Sometimes such "Privity" gets established through the contractual document itself. If for example, an agent signs a contract but discloses that the contract is being signed on behalf of another party who is his principal, the other contracting party may sue the principal though the principal himself has not signed the contract.

In such cases the principal may defend himself to say that the conduct of the agent was prima facie indicative that he had no such rights to bind the principal. This would be a fact to be established in a given case.

For example, if a director of a company signs a contract and binds the company, then even if he may not have a "Resolution" backing such a power, the principle of law of "Lifting of Corporate Veil" may be used to invoke liabilities on the Company.

If however a contract is signed by an "Undisclosed Agent" then the principal may say hold out that there was no privity of contract with the party raising the dispute and hence he should not be dragged into the litigation.
In most of the cases where an agent has to enter into such agreements with third parties, the back to back contract with the principal may have an "Indemnity Clause" which may determine if the agent has to absorb the liability himself or it is borne by the Principal. As regards the third party

who invokes the contractual obligation against the signer (agent), the proceedings will lie only with the agent and not the principal who is behind the scene.

Another exception allowed is under special laws such as Negotiable Instrument Act applicable to Cheques or Bills of exchange or Promissory Notes. In these cases, enforcement rights are created between non-signatories as the cheque exchanges hands, from one bank to another or from one person to another.

Similarly, contracts that restrict or impact upon the use of land (e.g.an easement) may be enforceable upon the next land-owner, even though they were not privy to the original contract. This is an old exception to the rule of "privity of contract" that is still applicable today.

Also, the law of trusts, where a person may contract to the benefit of another, operates to convey certain rights to the third party even though, in fact, this third party was not party to a contract which created the trust.

The Court may however have the discretion on the basis of the circumstances of the case to allow party who may not appear to have the privity of contract to be brought into the litigation.

## Jurisdictional Issues in E Commerce

Jurisdiction issues in E Commerce are also under constant discussion. Every country incorporates the extra-territorial jurisdiction in its laws and so also has India. Section 75 of ITA 2000/8 makes contravention of any of the provisions of ITA 2000/8 also applicable to persons outside the geographical boundaries of India as long as at least one computer in India has been used in the commission of the contravention.

Though Section 75 of ITA 2000 appears to restrict itself to contraventions and offences, the principle of Section 75 should be also extendable to the formation of contracts, application of Section 11 to parties and automated systems outside India, as much as to the liabilities of intermediaries outside the country.

The data protection laws (e.g.: Proposed Personal Data protection act 2018 draft or GDPR) often speak of "Data Localization" to reinforce the jurisdiction of local laws to the activities related to the processing of personal data. Russia is now in the process of actually segregating the "Russian Network" by law into a domain with sovereign control of the Russian Government. China practices it within the current set of their laws.

It is therefore reasonable to expect that the extra territorial jurisdiction under Section 75 of ITA 2000/8 stands extended to all aspects of ITA 2000/8 including Sections such as 11,12,13,14 etc. In due course Judiciary may endorse this view when called for.

In the past there have been several discussions on international jurisdiction regarding E Commerce transactions. These have been under a regime where Internet was considered a "Border less society".

In the present circumstances where legal borders are getting introduced through the data protection laws, it is not clear whether the earlier concepts of jurisdiction actually apply.

In most cases Courts have taken a stand that if the interest of people in the local jurisdiction is affected by an action in Cyber Space, then the local Courts have a jurisdiction. If a website is in a particular language, if it has a customer contact office or if targets its services specifically to the citizens of a specific country, then the local jurisdiction cannot be avoided even if the contract with the customer may say so. In the case of "Taxation" there may be clarity but taxation jurisdiction does not always extend to jurisdiction regarding crimes.

Sometimes, the legal jurisdiction may be claimed because of the law but enforcement jurisdiction would still be an issue. The law enforcement authorities in one country may not get into another country to enforce their rights except under established international norms such as the support of a Treaty or other mechanisms through the Interpol.

The cases of Dmitry Sklyrov the Russian programmer who was arrested while on a visit to USA for violation of Digital Copyright Law of USA, is a case worth studying on how the enforcement jurisdiction is applied in practice. In India, the Bazee.com case was one where a US Citizen of Indian
Origin who was the CEO, was arrested in India and charged of an offence committed by a customer of the company on the website.

These issues of Jurisdiction will always remain a point of dispute but what businessmen should understand is that more than the law, it is the intention of providing a service to a specific group of people which becomes the benchmark for enforcing jurisdiction and unless special disclaimers are invoked, it is difficult to escape the jurisdiction of laws of other countries on the business set up in a designated country.

In respect of laws such as GDPR, it is therefore recommended that E Commerce companies in India carry a "GDPR Exclusion Clause"[vi] in their terms and conditions.

Similarly while framing the dispute resolution mechanism for their websites, if the E Commerce websites opt for Arbitration, then they will have to define not only the "Applicable Laws" but also "Place of Arbitration" in such a manner that the provisions are within the purview of the local laws.

## Electronic Data Interchange

EDI refers to "Electronic Data Interchange" which is a reference to the system of making data generated a processed in one system with another. This EDI compatibility is essential for ensuring transactions to be carried over to different systems without the need for manual data input by reading it out of one system and writing it into another system.

EDI can enable an invoice generated by the seller's system to be directly processed by the accounting system of the buyer.

In the initial days, the integration of data created in different systems was achieved through "Standards" being enforced in different industries.
One example was the Health insurance portability and Accountability Act (HIPAA) of USA which defined standards for coding medical transactions so that they can be easily ported from the hospital systems to the insurance company systems.

Internet itself was designed as "Platform Independent System" so that data interchange could be seamless. As a result, a web form completed on a browser running on an Apple Mac system can easily be transported into the back end server running on a Windows system.

Although what can now be called traditional E-commerce has not been limited to EDI and has included business practices built around computer- to-computer transmissions of variety of message forms, bar codes, and files, the use of EDI has arguably led to the most significant organizational transformations and market initiatives. Electronic integration, supported by EDI and other information technologies, drastically reduces time and space buffers that shelter a firm, but that also limit its competitive opportunities.

The main advantage of EDI was that it created a paper free system of inter-business communication, linking companies such as manufacturers, suppliers and transport providers.

In the absence of EDI, there would be a need for intermediary systems which has to convert one set of data to another set. This would involve additional costs and also add points where errors can creep in.

EDI therefore is a concept that combines multiple systems processing the same transaction into one integrated system. Depending on who owns and controls the different components, there could be legal issues, data protection issues, contracting issues etc., which need to be addressed. If properly used EDI can reduce costs and improve efficiency.

## Customer acquisition and E Advertising

"Customer acquisition" is an important aspect of business. In E Commerce, once the website is established, sellers are tied up, payment options are ready, and it becomes necessary to invite customers in sufficient numbers as to sustain a profitable business.

"Customer Acquisition" is an art and requires identification of prospective customers through market segmentation, potential customer profiling, product branding followed by advertising and other promotional efforts.

During this "Pre-Purchase" stage, in some product classes, there may be a need for negotiations so that preliminary enquiries are received on the website and there after it is followed up by sales personnel either on the phone or otherwise.

"Advertising" is an important component of marketing. It is a communication between the marketing company and the consumer highlighting the benefits of the product to the consumer and making him feel that he needs the advertised product. It is as much important for E Commerce as for the commerce in the physical society.

While "Selling" involves "Pushing a product", "Marketing" is "Creating a desire to buy". Creating a "Desire" involves first building an "Awareness" of the product and its benefits and then converting the awareness into "Interest" and then a "Desire". This process is achieved by the "Advertising".

Different products and services need different kinds of marketing and therefore different kinds of advertising. A Consumer Durable purchase is an informed researched purchase and requires the advertising to take care of the informational needs. Consumer non-durables purchase is often an "Impulse purchase" and requires creation of a quick "Urge" to experience the product.

Information content would be different for such products. Similarly, services require a different approach and financial products may require another approach.

Success of "Advertising" depends on the "Mental State" of the consumer when the advertisement is served. For example, an advertisement on tooth paste is fine in the morning hours while the advertisement of condoms is better in the night hours. A Zomato advertisement may work fine during lunch time while ice cream advertisement may work better in the evening.

Thus "Advertising" is an art to understand the rationale for the consumer to buy a product or service and it is created by the content of the advertising, the way it is advertised, the timing etc.
E-Advertising can be a term which is basically applied to "Cyber Advertising" while a small part of the E Advertising can happen through electronic sign boards or other means.
Cyber Advertising may happen on a website where a consumer visits and also through e-mails that may be sent to the consumer.

One of the advantages of Cyber Advertising is that the consumer can be effectively profiled and advertisement can be customized to the individual.

When a person visits a website, his location can be identified and advertisements relevant to the location can be served. There is no need to advertise a product which is available only in US to a consumer in India and hence as he visits the website, his IP address can be analysed and location determined to provide the appropriate advertising.

To enable such customised targeted advertising, "Ad Serving" companies equip themselves of real-time analysis of browsing and buying behaviour and serve appropriate ads from its bank.
This need for profiling a consumer creates issues such as "Privacy Infringement" and is the focus of data protection laws such as GDPR.

The platform where the advertisements are released is called the "Media". "Cyber Media" can be the web versions of the newspapers or You tube streaming of the TV programs. The Internet has provided such beautiful opportunities that a "Social Media" consisting of the Face Book, You Tube, WhatsApp, Twitter etc. have developed with content being contributed by individuals across the world. This is a powerful advertising media which can be cost effective and reach specific target audience.
Cyber Advertising can take many innovative forms which may include advertising for exposure where the advertiser pays for the number of "Exposures" or "Click Through Advertising" where the payment is made only when an advertisement link is clicked or "Success Based Advertising"

where payment is made only when a successful sale takes place through advertising referrals. The medium affords the technical measures to track such exposures, click throughs or purchases through referrals.

Advertising is a source of revenue to the "Publishers" and is largely responsible for the growth of the Internet as a low cost and often free service.
The Privacy activists however are opposing the collection of any personal information and their use in tracking the potential purchase behaviour of the public and placing hurdles after hurdles to stop such information collection through Privacy Protection laws.

As a result Web Advertising is becoming more and more difficult by the day. Though an attempt is made by the publishers to obtain "Consent" from the consumers to use their personal data for commercial marketing purpose, the resulting "Consent Fatigue" where a consumer using a mobile or internet has to negotiate hundreds of "Privacy Policy" consents every day has posed a huge compliance challenge.

Regulators of critical industries like the Banks, Stock Markets, Insurance, Health Services etc impose several compliance related restrictions for Cyber Advertising which imposes a demand on the Advertiser and Publisher to be vigilant all the time on the laws related to advertising in Cyber Space.
E Commerce Companies may have to use "Advertising" as a tool of their business promotion and often include promotions such as "Discounts", "Flash Sales", "Cash backs" etc to support the advertising of the products and also advertise about such incentives themselves.

Through all the advertising efforts, companies try to build a "Brand Value" around the product so that consumers perceive a "Value" for the product or service created entirely through the communication.
In this endeavour to create a "Brand" companies often use unethical means of communication trying to exaggerate the product benefits and sometimes even lie about the products. They also use psychological tricks to make people consume products that they do not need or products that are harmful to their wellbeing. In such circumstances, "Regulation" may become necessary.
In the physical world there is a strong and effective regulatory mechanism through an "Advertising Council" both in India and in international levels where industry develops advertising guidelines in consultation with the Government bodies. Similar agencies are yet to develop in the Cyber world since the "Publications" in the web space are not organized like the licensed TV channels or News Papers.

Recently, an attempt is being made in India to amend the "Due Diligence" requirements under Section 79 of Information Technology Act 2000 (ITA 2000) to include ban on advertising of cigarettes and liquor through the web. During the recent elections, the Election Commission persuaded social media houses such as "Face Book" to introduce accountability for online advertising on Face book pages so that advertising for political purposes can be accounted for the election candidates.

This trend indicates that in the coming days, unless the Web Publishing industry introduces a strong self-regulation mechanism, the Government bodies will through measures such as the "Intermediary Regulations" and "Privacy Regulations" put curbs on the Cyber Advertising industry.
The non-Cyber E-Advertising such as electronic banners on the roads, on the buildings, in trains and aircrafts etc are all similar to Cyber Advertising since the advertisement is served from a central server in electronic form and has all the characteristics of an advertising on a web page.

Advertising on E-Mail or Messages in WhatsApp or Instagram are slightly different from website advertising since unlike a website which is a "Publication" which is visited by the consumers, the E Mail and Personal Messaging systems take the content to the individual's private space directly. It is an intrusion into the private information space of the receiver and hence requires an explicit consent stronger than the advertising on the publications.

## Post Purchase Service management including Dispute Resolution

Once the purchase is completed and product delivered, the E Commerce company has to worry about the post purchase satisfaction of the customer. It is managerially necessary for the company to ensure that customer's remain loyal and conduct repeat purchases. For this purpose companies go to the extent of providing free returns for a specified period or exchange of defective goods. Managing the returns and further disposal of the returned goods is therefore part of the services that the organization needs to manage.

Additionally, an E Commerce company has to factor in a "Dispute Resolution Mechanism" to handle customer complaints of both technical natures as well as related to product warranties and services of intermediary players like logistic companies.

In India ITA 2000 makes it mandatory for every intermediary to designate a "Grievance Officer" and provide his contact on the website. The Data Protection Act proposed in India mandates a dispute resolution mechanism also.

Hence every prudent E-Commerce company offers a structured dispute resolution mechanism apart from the easy return policy. Such mechanisms may include a "Complaint Handling Officer", "Ombudsman" or "Mediation and Arbitration". The option to resort to legacy court system always exists as a last resort. If the E Commerce companies are able to provide online resolution through ODR mechanisms[vii] it would be most appropriate.

## Raising Capital for E Commerce Ventures

Managing funding is a part of every business and also E-Business/E Commerce.
In all industrial ventures there are two types of expenses namely the "Capital Expenditure" and "Revenue Expenditure". Capital expenditure is expenditure which is incurred for the long term requirement of the business and is funded normally by the Equity and Long term borrowings.
Revenue expenditure is expenditure incurred for short term benefit of the company within one accounting year and written off during the year from the revenue earnings leading to profits or loss for the period. Certain expenses whose benefit may cut across several financial years are normally written off over a few years and may be accounted as "Deferred Expenses". Revenue expenses are funded out of operating earnings and short term borrowings.

The cost of purchase of inventory from the seller is a revenue expenditure and proceeds of sale is a revenue earning. Cost of land, Building, Equipment etc. is a Capital Expenditure and their liquidation is capital earning. A lease contract with upfront payment may be an example of a deferred expense.
Accountants have their own logic for accounting expenses in to different categories and are bound by the accounting norms.

E Commerce Companies normally do not have large long term assets such as Land and Building or Machineries. Their main expenditure is on "marketing" which is revenue expenditure and does not create any assets that can be used for raising funds.

Hence it is difficult for them to borrow on long term basis since the funding agencies such as Banks may demand collateral securities. Therefore most of the E Commerce ventures have to be financed in terms of "Equity".

Equity is initially contributed by the promoters and once the project reaches a stage where outsiders can be convinced to invest, further equity can be raised. Equity normally comes in the

form of “Share Capital”. Based on the share of equity capital, holders get voting rights and therefore proportionate control to direct the operations of the Company.

Any person or group holding more than 50% of equity will have control to appoint or remove directors and thereby control the operations of the company.

Until a share is listed in a stock exchange, the value of the shares is only notional. Only when a share is listed and is traded widely, one can ascribe a reliable value to the shares.

The Capital structure of a company is built through “Authorized” capital with which it registers itself, out of which capital is issued and subscribed with payment of the share capital in one or more calls. The Capital may be issued at a given price which may be the “Face value” with which it is registered or a higher value. Amount collected in excess of the face value is normally credited to a reserve account while the face value when paid is reflected as “Paid Up value”. When share subscription is collected in instalments, unpaid calls become “Call in Arrears”. The actual cash that flows into the company through subscription of shares is when the shares are paid up.
Hence when a company is in a “Start Up” stage, for legal necessity, it may be registered with a certain authorized up capital e.g.: 1 crore shares of Rs 1 each . The total authorized capital here would be Rs 100 lakhs.

Out of this, Company may decide to “issue” 50 lakh shares. Then the issued capital would be Rs 50 lakhs.

For subscription, shareholders may be asked to pay only 50 paise per share issued and hence the 50 lakhs shares when subscribed may bring Rs25 lakhs to the Company as first call received on subscription.

Rs 50 lakhs is then called the Issued, Subscribedand Paid up capital. The balance sheet will however show only Rs 25 lakhs as share capital as “Partly called Up” capital. Partly called Up capital is the Paid Up capital until the “Uncalled Capital” is called. If calls have been made for the entire amount of the issued capital and some balance remain unpaid it will be shown as “Calls in Arrears”.

If the entire subscribed capital is fully paid up, then the capital of this company would be Rs 50 lakhs. If the entire authorized capital is issued, subscribed and paid up at the face value of Rs 1 the company would have a cash of Rs 1 crore coming into the company.

In any instance, entire Authorized capital may not be issued, entire issued capital may not be subscribed, entire subscribed capital may not be fully paid up. However once a share holder subscribes to the capital he is contractually bound to pay all the calls until it is fully paid up or be liable to forfeit the shares.

Sometimes, Promoters may also be issued "Sweat Equity" as a sort of compensation for their efforts not represented by the financial expenses accounted. There may not be any cash inflow for such sweat equity and it may be accounted as an expense.

Even some of the employees may be provided ESOPs (Employee Stock Options) through which they may be given rights to purchase equity at a future time at a pre-determined price from out of an ear marked stock of equity). In the case of ESOPs actual cash may come in when the employees exercise their options. On the balance sheet, ESOPs will not get reflected until they are actually purchased when it will be part of the paid up capital.

Normally entrepreneurs may start their venture with limited resources and grow over a period of time. After the promoters normally a few risk capital investors may fund the development of the project idea into a proof of concept and for initial marketing. This is referred to as "Incubation". During incubation, funds will be providing by the incubator and shares may be allocated to him in return based on the understanding with the promoters.

After the company starts commercial operations, more investors may come in either through private placement of additional shares that may be issued or shares that may be issued from the earlier holders like the promoters by transfer. These may be called "Venture Capital" funding.

When shares are transferred from the existing shareholders to the new shareholders, there may be no cash flow into the company but there may be change in the control. When new shares are issued by the Company, cash will flow into the company and the control may also change.

When shares are issued at different points of time, the price at which the shares are issued may vary and would reflect the valuation of the company at that point of time. Normally as the company grows from being a Start-up into a private company and thereafter into a listed company, the valuation of the shares will change from the face value at the time of inception to thousands of rupees later.
Hence 100% of the shares of a company with Rs 1 crore authorized capital may be issued, subscribed and paid up by the promoters at the face value ofRs1 each totalling to Rs100 lakh at the time of inception when promoters contribute their investment.

Subsequently, if the authorized, issued and subscribed capital is doubled to Rs 2 cores with a fresh issue of further 100 lakh shares of face value Rs 1 each, the new authorized and issued capital becomes Rs 2 crores.

Now if a new investor buys 100 lakh shares to acquire 50% control, he may not be allowed to invest at Rs 1 per share like the promoters. Let us say the value of the company is now placed at Rs 20 crores, then each of the 200 lakh shares would be valued at Rs 10 each and the new investor would actually pay Rs 10 crores to acquire 1 crore shares but he gets 50% of the controlling stake. If the valuation is Rs 400 lakhs instead of Rs 200 lakhs, the new investor would get only 25% stake for the same investment of Rs 10 crores.

This Rs 10 crore comes into the company's account and would be available for its business as "Capital Receipt".

Subsequently let us say the company is listed and the price at the time of listing is Rs 100 per share.
The company will have the option to further increase it's authorized, issued and subscribed capital and issue the shares to the public and the entire proceeds of such sale would come into the company for its activities.
Sometimes, existing shareholders may opt to sell their holding to public or to another investor. In such cases, the price negotiation would be entirely between the involved parties. The funds would not however come into the company. It will go to the earlier shareholders who make the "Offer of Sale". However, new management can bring in its own benefits to the company and its value may rise solely because of the association.

The above process of raising funds is a very rough indication of how the system of capital funding of an E Commerce organization occurs in practice.
When management control changes, the legacy business of the new partners may have its impact on the status of the E Commerce company for taxation purposes as it may become a group company of the new partner.

Similarly, if the investor is a foreign entity, there will be issues of Government permission and classification of the investment as "Foreign Direct Investment" (FDI) subject to special regulations thereof.

In India, FDI is allowed in "Automatic Route" without prior approval of the Government in certain cases and in other cases through the "Government Approval Route".
For the purpose of FDI, Business to Business e commerce is allowed to raise 100% FDI through automatic route.

The Retail E Commerce companies are divided into two categories namely "Market based Model" and "Inventory Based Model".

Inventory based model of E Commerce means E-Commerce activity where inventory of goods and services is owned by e-commerce entity and is sold to the consumers directly. Market based model of
E Commerce means providing of an IT platform on a digital network to act as a facilitator between buyer and seller.

In Market based model 100% FDI is permitted through automatic route and in Inventory based model no FDI is permitted as E Commerce.

Inventory of a vendor will be deemed to be controlled by the e-Commerce market place entity if more than 25% of purchases of such vendor are from the market place entity or its group companies.

An entity having equity participation by e-commerce marketplace entity or its group companies or having control on its inventory by e-commerce market place or its group companies will not be permitted to sell its products on the platform run by such marketplace entity.
Hence in designing the E Commerce business, and choosing the vendors, the delivery mechanism etc, the Company needs to simultaneously be aware of how its business policies affect the investment options.
(The FDI regulations are subject to change and subject to different interpretations and the students are requested to refer to the latest Government guidelines in this regard[viii])

One of the innovative financing methods used by some is the "Crowd Funding" strategy which is itself an e-commerce activity. In the Crowd funding, the customers of a product or service or the common man on the street provides the venture capital in small doses. This is a strategy for dis-intermediation of Banking institutions by directly raising funds from the consumers to the financing of the projects. This can perhaps be looked upon as "Distributed Venture Capital Funding" and deserves exploration.

## E-Auction

E-Auction is an interesting derivative of the e-commerce process. In e-auction, the consumers are allowed to make real time bids for a given product. The first to use such strategy were some airlines which sold tickets to the highest bidder on some routes which were going unsold at the normal prices.

Some information aggregators used the principle to aggregate sale offers from multiple e-commerce sites on a single platform so that the consumer can see the price differences if any for the same product across different e-commerce sellers.

This has also been used extensively in the used goods selling in C2C e-commerce where individuals could sell their used TV or Car or a Motorbike to the best bidder. Similar technique has also been used for selling property as well as rentals.

There has been some challenges on the system initially with Patent restrictions and hence the reverse auction system[ix]which was a popular consumer tool has not been much in use today. There are also frauds on OLX and Quikr networks which have posed challenges to genuine users of the system.

The responsibilities of the E Commerce website owners in case of E Commerce transactions where vicarious liabilities may arise out of an illegal activity of one of the users of the platforms was well revealed in the famous bazee.com case [x]in 2004 which got closed only in 2012.

## E Procurement

E Procurement is a term which can be used for any B2B purchase system initiated by an organization. However, it is more often used in the Government purchase program or a large government assisted project where the process of purchase is sacrosanct and the value is also high.

When a purchase decision has to be undertaken, if the goods are available off the shelf and the quantity required is not significant, it can be bought off the shelf through the normal E Commerce process.

But where the goods are to be custom built and is like a project which may be extended over time and is of high value, the E-Procurement process needs to be initiated.

E-Procurement also has a buyer and seller who interact with the electronic documents and hence all the issues connected with E Commerce are also relevant here. In most cases, payment may be settled outside the e-systems since the value is too large though there could be Bank to Bank or Bank to Treasury transfers wherever possible.

The distinguishing feature of E-Procurement however could be that it follows a "Tender" process sometimes at multi-level. In the first level the bidders are technically cleared and there after their financial bids are evaluated before a final decision is taken.

The offers from different persons may not be strictly comparable since there may be difference in the customization of the required solution offered for supply by different vendors. Sometimes the products or services are so complex that the buyer himself may not fully know how to fix the specifications.

Normally the intending buyer first releases a "Request for Proposal" with detailed specifications if available or description of the requirement to the extent possible and invites the bidders to send their proposals with specifications, time schedule and cost.

The bid may be received in separate closed offers with financial bids being separated from the technical bids and only after the technical bids are approved, if there are multiple parties passing the technical approval stage, the financial bids may be opened. Though the "Lowest Bid" may still be a dominant criteria for selection, if the proposals are not strictly comparable, there could be flexibility in adhering to the "Lowest Bid" principle.

When the Government departments moved from their current system to the E Procurement system, initially they replaced newspapers for publication of tender documentation to websites. Letters were replaced by E-Mails.

In most cases these documents were uploaded in the Government websites but were not sufficiently authenticated with digital signature to prevent tampering. Hopefully this lacuna would be removed over time as the Government departments refine their processes.
At the next level the tender documents have been "Uploaded" in encrypted (with the public key of the tender committee members) and digitally signed electronic document to the designated server. Opening of the tender was by the designated officials with their private key.
The financial bidding could also be through pre-uploaded documents or might be done like an "E-Auction" with real time bidding.

The real time bidding process has been often vitiated by denial of service attacks and hence could be used only for small value purchases.

In this entire process, the procedure for submission of documents through the e-tender process is part of the tender invitation information and becomes part of the contractual terms of the tender process.

The e-procurement process is meant to provide opportunity to a larger section of the business to participate in the tender process along with better transparency, reduced corruption and possibly reduced cost.

However, the e-procurement process has to ensure that technical uncertainties are properly addressed, bidders are properly educated and the legality of the process is ensured.

Technical issues are more in the case of real-time auctions since "Connectivity" and possible "Denial of Service Attacks" could pose issues.

In terms of legal enablement, ITA 2000 provides for legal recognition of electronic documents (Sec 4), legal recognition for electronic signatures (Sec 50, legal enablement of E –Governance (Sec 6,6A,7 and 8). A mandatory audit is also indicated under Section 7A. Hence there should be no legal difficulty in India for Government departments to adopt e-Procurement as a means of purchase.

Some challenges remain in respect of uploading of documents and conduct of e-auctions. One of the procedural problems in an e-procurement scenario came up for judicial attention in the case of ShapoorjiPallonji and Company (SPC) Vs Maharashtra Housing Development and Area Development Authority (MHADA). In this case, three bidders had submitted bids for a Rs 11500 crore project and the bid of SPC was rejected by the tender committee under the grounds that the documents had not been received by the tender committee. SPC argued that they had uploaded the documents to the NIC server but in the last stage did not click a "Confirm" button. SPC claimed that they did not get the screen showing the confirm button though no evidence was available for the same. As a result of the incomplete process the document had not reached the appropriate tender box in the system and hence the committee could not consider it. NIC contended that "No Acknowledgement was generated by the system" and hence the tender process was incomplete.

SPC went to Mumbai High Court and claimed that there was a "Technical Error" in the system and hence their bid should be accepted despite the faulty submission.

This was at the stage of the technical bids for preliminary short listing and not the final financial bid. The Court therefore took the excuse that no great harm would be done to other bidders if SPC was allowed to participate in the process and citing some strange logic that "Human spirit must prevail over technology" etc., allowed the faulty process of submission to be ignored. [xi]

Additionally, e-tendering is prone to other frauds such as impersonation, tampering of tender documents before or after submission, fake tender deposit submission, etc and needs to be secured and subjected to proper audit to retain its integrity.

## Concluding Remarks

Fintech Business, Security issues, Taxation issues and E Banking issues are covered in subsequent Chapters.

## References


1. https://en.wikipedia.org/wiki/Justice_K._S._Puttaswamy_(Retd.)_and_Anr._vs_Union_Of_India_And_Ors.
2. http://ceac.in/wp/ceac-edb/
3. https://www.naavi.org/wp/ita-2008-already-has-a-provision-if-sophia-breaks-our-law/
4. http://ita2008.in/ita_2008/ch4_2008.htm
5. https://www.naavi.org/wp/creating-protection-indian-companies-european-hegemony/
6. www.odrglobal.in
7. https://dipp.gov.in/sites/default/files/pn2_2018.pdf
8. https://patents.google.com/patent/US7996298B1/en
9. https://www.naavi.org/wp/closure-of-bazee-com-case-sharat-digumati-gets-relief-amidst-intriguing-precedents-created/
10. https://www.naavi.org/wp/the-e-tendering-issues-in-maharashtra-uploading-is-not-the-same-as-submitting-the-tender/


*P.S: Since the entire content has been drawn from dynamic resources in the Internet and most of the published books may not contain updated information, no reference to books have been provided. In the changing world of technology, the value of judicial precedence is also low. Every judicial decision has to be seen with the law and technology as applicable to a case on hand and hence excessive reliance on case laws in areas of E Commerce is better avoided. Hence it is recommended that students develop an insight into the legal interpretation from out of the current developments they may observe on the resources available on the Internet after due filtration for the credibility of the information.*

# Chapter II: Security and Evidence in E Commerce

**Syllabus:** Dual Key Encryption, Digital Signatures, Security issues in E-Commerce, Evidence related issues, UNCITRAL model law of E-Commerce, Indian Legal Position on E-Commerce. IT Act 2000/Indian Evidence Act/ Draft law on E-Commerce

**Learning Objectives**

In this chapter the student will learn about the Security and the legal issues applicable to E Commerce.

For the convenience of the students, the Chapter is divided into two parts. In Part A technical issues such as Encryption, Digital Signature etc. In Part B, students will discuss the Information Technology Act 2000 along with the evidentiary issues. After studying this chapter, students should be able to appreciate the "Risks" in E Commerce, the kind of frauds that may occur, the liabilities that may arise. Students would also be exposed to the technology of some basic security measures such as "Encryption" and "Access Control" and the legal aspects related to E-Commerce as applicable in India.

## Part A

## What is E Commerce Security?

E Commerce involves

Setting up an E Commerce Establishment

a) Pre-Sales Communication exchange between a prospective Buyer and a prospective Seller
b) Financial Transaction between the Buyer and Seller
c) Goods transport from the Seller to the Buyer.

"Security" essentially means "Protection of the Goals of Business". "Information Security" means protecting "Information" in such a manner that the Goals of Business are protected.

## Need for Security in E Commerce

Security is a requirement for E Commerce since the order is placed by an individual for a given product and payment is made online. In this process the order has to be captured correctly and there should be no monetary fraud that should occur. Until the order is successfully delivered and accepted by the customer, the information flow should be free from tampering.

In order to prevent a fraudster from committing a fraud with the knowledge of the transaction as also as a measure of privacy protection, the confidentiality of the transaction has to be ensured. In order to ensure that orders are placed when required and cancelled when not required, the service should be available.
Hence preservation of Confidentiality, Integrity and Availability of information are three important and relevant information security parameters for E Commerce. These are together recognized as the CIA principle of Information Security.

## Risk based approach to Security

"Security" of an asset can be achieved best by shutting off the use of the asset. For example is we own jewels and we are afraid of theft, one way is to lock up the jewels in say a Bank locker and hope that the locker would not be robbed.. It is definitely more secure than keeping it at home or wearing it into the market place or keeping in our hand bag and walking in the street or keeping it in the hotel room while we are on tour.

But keeping the jewel in the locker all the time may not serve the purpose for which the jewel is bought in the first place. If jewel cannot be worn to a marriage party, what is the use of investing in the jewel? Hence the owner of an asset is always in a dilemma about securing the asset while also ensuring that it is used optimally from time to time.

Hence "Security" managers do not try to go for security at the expense of usage. In order to ensure that the asset is available for use and at the same time is also "Secure", security managers adopt a "Risk Based Approach to Security".

What we mean by "Risk Based Security Approach" is that we make a reasonable assessment of what may go wrong and how an asset may get damaged during a type of its use and try to design security measures that are appropriate under the use cases identified

In this context, “Risk” to a business is “Any event that is likely to have an adverse effecton the Business Goal “. Since “Information” is an asset in the business context, “Information Security Risk” is any event that could adversely affect the “Information”.

An “Adverse” effect on the Information may be

a) Information is accessed by unauthorized persons and loses its confidentiality value
b) Information is deleted or Information is wrongfully modified
c) Information is not available to the decision makers when required though it is otherwise not damaged.

These three aspects are recognized as Preservation of “Confidentiality”, “Integrity” and “Availability” of the information.

It may be noted that Information may be accessed, deleted or modified from time to time for the business and hence only unauthorized access, deletion or modification is an issue of security.
This means that an organization has to first determine “Who is authorized to access, delete or modify” the information and that alone becomes the bench mark to determine if there is an “Unauthorized access, deletion or modification”.

All those who are not authorized to access, delete or modify the information do not have “Availability” of the information. Hence what we call “Preservation of Availability” in the CIA principle of security is “Availability to the authorized persons”.

Hence “Confidentiality”, “Integrity” and “Availability” is all relative to “Authorization” of who can access, delete or modify the information.

In a Risk Based approach to Information security, the “Risk” refers to the possibility that an unauthorized access or an unauthorized deletion or modification or an unauthorized denial of access to the information occurs.
The possibility of “Risk” arises because there could be an opportunity for such unauthorized activity and also because somebody may be lurking around to commit an unauthorized activity.
These two aspects that manifest a “Risk” are called the “Vulnerability of the organization” and the “Threat to the organization”.

If therefore there is a threat to information being damaged and the information is vulnerable to such a threat, we say there is a “Risk”.

For example, a Virus-X which could destroy some files is a "Threat". But if such a virus arrives at our systems and it can get through and start damaging the system, then we are vulnerable.
Where Threat and vulnerability meet, Risk" manifests. Threats are present in the environment and Vulnerability exists within us. We can avoid the risk either by moving out of the environment of threat or by eliminating our vulnerability.

For example, if we are handling a hot tea pot, a risk of burning our hands can be eliminated if we move to a distance from the hot tea pot or wear a heat protecting gloves to handle the hot tea pot. If we want to use the tea pot then the option is to assess the risk of taking up the tea pot and pouring the tea without burning our hands. If this can be done without the gloves, it is fine. Otherwise we need to acquire a glove or a substitute there of to prevent our fingers from being burnt.
We should realize however that in order to avoid the gloves, we pick up the pot with a piece of cloth and try to precariously manage the pouring, and then we may even drop the pot, break it and pour hot tea all over our body.

Sub optimal risk management solutions often result in such situations.

In all these four phases of E Commerce, we identified earlier, namely the "Setting up phase", "Pre Purchase phase", "Financial Transaction Phase" and "Goods Exchange phase", different threats may be present and if we are vulnerable, "Risks" are also present.

However, since we need to continue to do our business and not shut down, we need to "Manage the Risks" and not run away.

An E Commerce Business entity has to therefore learn how to manage the risks.
Identifying the Risks and taking remedial steps is therefore an integral part of E Commerce/E Business Management.

## Risk Management Principles

If we accept that "Data is an Asset" only if it is available for use, then we cannot run away from creating, processing, storing and transmitting data though the risk of loss of confidentiality, integrity and availability arises in each of these operations.

As long as there is “Value” to “Data”, there will be criminals who would like to steal or tamper data. Thieves are also technology experts and will be as innovative as the creators of software or the security professionals. Hence “Threats” will always exist and even grow.
Software developers are businessmen and often release software which is vulnerable ab-initio. These are the “Zero Day Vulnerabilities” and “Bugs” in software which makes exploitation of these vulnerabilities a possibility.

When “Bugs” are detected and patched, the users often do not apply the patches and the vulnerabilities continue longer than they should.

As a result while the Threats always are increasing, vulnerabilities are not decreasing. Hence “Risk” is unavoidable and there is no way “Risk” can be brought to Zero.
Hence “Risk Management” focusses more on “Risk Mitigation” than “Risk Elimination”.
However since it may be possible to re-organise business models, Risk Management recognizes “Risk Avoidance” as one of the options for a Company.

Risk Avoidance means that when an organization recognizes a “Risk” it evaluates if the Risk can be “Mitigated” to a level where even if the Risk manifests into damage, the organization can face the consequences. This ability to absorb the adverse effect of an event is “Risk Absorption Capability”.
Hence If Risk can be mitigated to the level of the organization’s Risk absorption capacity, the organization may opt to face the risk and continue. Sometimes it may be possible to find a “Risk Transfer Strategy” through which part of the Risk is transferred to another “Insurance Company”. This increases the Risk absorption capacity of the organization.

If the organization determines that a certain risk is going beyond its absorption capacity, it has to use its business prudence and “Avoid Risk” by suitably exiting the risk space that poses the unmanageable risk.

Thus Risk Management has four components namely, Risk Mitigation, Risk Transfer, Risk Absorption and Risk Avoidance.

Despite all the measures of Risk Management, organizations cannot still be complacent that Risk has been contained since there could be “Risks that the organization is not aware of”. Hence there will always be a “Residual Risk” which remains in business and has to be contended with.

Since there is always a cost to "Risk Containment", a business organization has to always be keeping the "Risk-Reward Trade off" and Return on Risk management Investment in the back of its mind while initiating Information security measures.

It is the reflection of the efficiency of Information Security Managers of an organization and the prudence of the business managers if an organization can bring down the risk to such a level that Risk-Return trade-off is profitable for the organization.

Implementation of Risk Management in an E Commerce/E Business Scenario is therefore a complex activity that has to take into account proper Threat Assessment, Vulnerability Management, Risk Mitigation and Risk Absorption capabilities.

## Risk Assessment

In the E Commerce scenario, information security risks arise because of frauds which may be committed by outsiders or insiders or, by technical faults that may arise from the use of technology.

Information Security should always be considered as a "Three Dimensional" challenge. The first dimension is the Technology related risks. The Second dimension is the "Regulatory/Legal "related risks. The third is the "People oriented risks" that arise from the way human beings behave in different circumstances.

## Technical Approach to Information Security

In the "Technical Approach to Information Security", we try to address the issue of preserving the "Confidentiality", "Integrity" and "Availability" of information by managing the technical controls such as Access Control, Intrusion Detection etc. The objective of the security is to prevent unauthorized access or modification of data. If however, due to some contingency the data is actually breached, then the Information Security Manager tries to keep a Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP). The DRP aims at restoring the damaged data with the least time delay. The BCP ensures that the customers of the organization do not feel the adverse impact of the breach.

DRP-BCP is therefore considered as the "End Objective" of the Technical approach to security.

In order to achieve the Technical Security Objective (TSO), an E Commerce organization has to take into accounts its systems and connectivity aspects.

The hardware purchase, the software selection, the security in the data storage system, whether data has to be stored in its own servers or on the cloud are all decisions that are relevant.

If own assets are used for the maintenance of the E Commerce platform , then the company should ensure that the systems are always updated with the latest security patches issued by the suppliers and also install appropriate Firewalls including anti-virus or anti malware system. Also they need to design suitable access rules and implement them so that only authorized persons have access to the data. As a precautionary step they also have to install Intrusion detection systems.

If the organization uses Cloud computing as is the trend, it has to ensure that appropriate service provider is used and security systems of the service provider is adequate.

If the employees are allowed to bring in their own devices or allowed to use the company network to connect to external network and internet, appropriate security measures are to be implemented even for that.

“Access Control” is an important strategy for managing security. Access Control includes regulation of “Physical Security” where the systems which are to be protected is physically guarded either with locks, door access controls, guards, cctv systems etc.

Then entry into systems is guarded by passwords or access cards or access hardware keys. Even after entering into the systems, additional access barriers may be placed on access to specific applications and finally access to data.

Access to data is controlled with the use of “Encryption” where data is stored in an encrypted manner and only authorized persons have the “Decryption Key”. The “Decryption Key” itself can be a “Password” or other “Software Keys” or hardware devices like smart cards, cryptographic keys, etc.

Access Control requires that the organization maintains an inventory of assets and inventory of people and mapping of who can access what supported by Firewalls which allow only the authorized persons to enter.

Creating multiple levels of authentication is a strategy to ensure “Defence in Depth”. Critical systems may be supported by multiple access keys controlled by more than one persons and hardware keys fortified by biometric and password combinations.

The security idea pursued in all these instances is to allow access on the basis of “What a person Knows”, “What he is”, “What he possesses” or a combination of any or all of these. It has also become a practice today in India to use “Dynamic Passwords” and also “Multi factor authentication” through different communication channels such as e-mail network and mobile network etc.

“Password” is the most popular access control which is checking of “What a person knows”. Where password is used, the user is allocated a “Log In ID” and a “Password” to be used in combination. Whenever the user requests access, he provides his log in ID and Password and a system checks it along with the stored data base and if there is a match, it allows access.

In order to make it difficult for attackers to guess the passwords or use “Brute Force” attack, password policies are set so that the passwords are reasonably complicated. Normally the user is forced to set the Password of his choice at the time of first log in and also change the password periodically. At the same time in order to prevent loss of password during usage when the password has to be input at the user end and has to reach the server through the internet, it is a practice to ensure that passwords are first converted into a “Hash Form” at the user end and transmitted only in “Hash Form” and also stored in the server as a hash value only. In other words the system at the E Commerce end does not know what is the password but knows only what is the hash value of the password and all verifications are done with reference to the hash value only.

“Brute Force” is a term used when an access system is challenged by a fraudster by trying different combination of passwords until the right password is found. For example if the password is a four digit numerical password, it has to be any one of the numbers from 0 to 9999. If these 10000 combinations can be tried one after another, then it is possible to break the password. The number of combinations will increase if the number of password digits is increased, if it is made a combination of numbers and letters, if the letters can be capital letters also, if special characters can be made part of the password etc. By “hardening” the passwords the security of access can be improved. However, at the server end irrespective of the complexity of the password what is received and verified is the hash value already registered and hence password can be broken if the server is challenged with the hash value.

Since if we eliminate the insider frauds, and the recklessness of the users in sharing their passwords, they can be stolen only during transit. To prevent the passwords being revealed during transit, when a password moves out of the user's system it is encrypted in such a manner that even if an eves dropper accesses the data that is going into transmission from the user's computer to the E Commerce server, he only gets access to encrypted data and not plain text data. "Encryption" therefore becomes the security tool to ensure that the password does not fall into wrong hands during transit.

Similarly, when data is in storage, if an unauthorized person gets access to the system and the data, in order to ensure that the access is rendered useless, data in storage is also "Encrypted".

If data is encrypted, one needs the "Decryption Key" to get the plain text behind the encrypted data and hence "Encryption" is considered an important security tool.

We shall therefore discuss the system of "Encryption" in greater detail along with different types of encryption and the system of digital signature.

## Cryptography

Cryptography is the science of hiding information. It uses methods to convert a "Plain Text" into a coded form of information which is referred to as "Cypher Text" and a method to reconvert the "Cypher Text" back to "Plain Text".
The purpose of Cryptography is to ensure that messages in transit are not read by unauthorized persons. Hence before a message is put into transit, it is encrypted using one of the means available to the sender. The recipient is informed how the encrypted information can be decrypted and converted into readable plain text.

## The Key

The means used for encryption and decryption is generically described as the "Key"
In the context of an electronic document, "Encryption" is a mathematical operation that transforms the original set of bits in a document into a transformed set of bits of the cipher document or vice versa.

## Encryption Systems

Digital documents are “Binary Documents”. Hence every digital document is a binary stream consisting of zero and one. Even the space in a text is a binary notation. Sound and Image or video is also a binary expression expressed in terms of zero and one.

The stream of Zero and Ones can also be also looked at as a representation of a “Number”.

For example, the binary representation of “X” is “01011000”. If the binary “01011000” is converted back to an ascii character, it yields “X”

At the same time, in a binary-number conversion, the binary “01011000” converts into number 88 and vice versa.

As a result, every electronic document which is an expression in binary is a number and mathematical operations such as addition, subtraction, multiplication or division can be conducted on them.
Also the binary expression (stream of zeros and ones) can be easily grouped into blocks of different sizes and/or transposed or exchanged amongst themselves individually or in blocks. All these techniques may be used in building an encryption algorithm which can transpose a plain text or sound file or image/video file into what may look as gibberish.
But if we know the encryption key, we can reverse the encryption and get back the original binary stream which can be viewed or heard in its original form before encryption. This reversal process is the “Decryption” process.

Encryption system normally is an algorithm and the process of encryption would consist of changing a binary stream into an encrypted binary stream using the algorithm.
The algorithm needs to have an ability to take a variable binary input which is the “Document” and another designated input which is the “Key” which is a designated constant for the time being used by the user.

This “Key” can be normally generated by the user himself through a Key Generation algorithm to which a user input is provided as a seed.

In Other words, the key is dependent on a user input. This user input is called the seed to generate the key. It is an input different from the document used for key generation. Also the key can be

generated once and used multiple times for different documents. The encryption output is dependent on the key and the document itself.

When we take the algorithm and input the variable which is the document to be encrypted and supply the second input which is the "Key", the result would be the encrypted binary stream of the original document.

Similarly, when the encrypted binary stream is the variable input and the decryption key is the second input, the result is the original document.

## Symmetric Key Encryption

In one form of encryption, the encryption method uses the same "Key" for encryption as well as decryption. Such a system is called a "Symmetric Key Crypto System".

In a symmetric key encryption, if Rama has to send a confidential message to Bhima he will encrypt the message using the designated symmetric key. The encrypted message can then be sent over an open network like the Internet without the fear of it being intercepted and read by an eavesdropper. But if Bhima has to decrypt the message, then he needs to have the copy of the symmetric key.

Hence Rama should not only send the encrypted message but also the key. Assuming that they need to correspond only through the internet, if the key is sent through the same insecure network over which the message is to be sent later, and if an eavesdropper is waiting to monitor all the communication, he would be able to get a copy of the key as well as the encrypted message and hence would be able to decrypt the message.

In view of the difficulty in ensuring confidentiality of decryption key in transmission, "Symmetric Key Encryption" is not a secure system for sending and receiving encrypted messages over the Internet.

Some of the popular Symmetric Cryptographic algorithms are AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard) etc.

## Security Aspect of Algorithms

The security of an encryption algorithm is a function of the difficulty in breaking the encryption. Encryption is often broken by finding out the key by studying the encrypted document and reverse engineering the generation of the original plain text document. Alternatively, the text itself may be analysed to find a pattern which may reveal the underlying plain text message.

Since the standard algorithms are known, the encryption algorithm is known to the attacker and only the "Key" is the unknown factor.

When several documents encrypted with the same key and same encryption algorithm is available for study, the attacker can try to extract similar encrypted sets of data and try to read meanings into it to identify the encryption.

Except for the problem of sharing of the "Secret key" in a symmetric key encryption, the encryption itself is considered strong and difficult to break. It is also fast for processing and is therefore used widely where Key exchange over open network is not required. It is also used in combination with the Asymmetric Cryptosystem described below to protect the key exchange system as in the SSL system. (Described later).

In Encryption, there are two basic systems known as "Stream Ciphers" and "Block Ciphers".

A stream cipher, the binary values of a document are sequentially altered under an algorithmic rule to produce the encrypted binary stream.(which is also a binary stream like the plain text stream but produces gibberish when it is passed through the reading programs since the stream has been changed.).

In Block Cipher, the binary streams are divided into blocks of some finite size and bits are transposed within each blocks and blocks with other blocks to generate the encrypted binary expression. While doing so, the blocks may be even padded up with additional binary inputs from the algorithm as part of the encryption system.

Though most of the processes are standards, variability is introduced through the "Key" which could be one of the variable elements that makes the encrypted output different for different keys. The security of an algorithm depends on how the encryption system handles the creation of

blocks, the key input, the complexity of the transpositions etc. In 3DES system three different keys may be used for each of the three iterations.

The length of the "Block" in a block cipher and the length of the "Key" also alter the security features of an encryption. Higher the key length more is the security. The block length is normally 64 bits, 128 bits or 256 bits etc.

Complexity of encryption can be increased by varying the various elements used in the encryption and increasing the block size and key size.

## Asymmetric Key Encryption

There is however an alternate encryption system which is called the "Asymmetric Cryptosystem". In this system there are two different keys. The algorithm is built in such a manner that a document can be encrypted with one of the pair of the keys and decrypted with the other key.

Normally one of the keys is called the Private Key and the other the Public Key. The Private Key is held confidential to the owner of the key pair. The Public key is distributed widely and put up in public repositories. It is not "Confidential".

In this system the sender of an encrypted message (Rama in our example) can use either the public key or the private key for encryption. But in order to exchange encrypted documents, both Rama and Bhim will use the Two Key system.

Both Rama and Bhima will first exchange their public keys. Now if Rama has to send an encrypted message to Bhima, he will use the Public key of Bhima to encrypt it. This encrypted document cannot be decrypted except with the private key of Bhima. Hence the communication becomes completely confidential between Rama and Bhima. Even if an eavesdropper gets hold of the encrypted message, without the private key of Bhima, it is not possible for him to decrypt it.

Note that Rama cannot use his public key or his private key for encryption of the document. If he uses his public key, it can be decrypted only with his private key which is not with Bhima. If he uses his private key then it can be decrypted by anybody with the public key and since it is not confidential, the eavesdropper can also decrypt the message.

RSA algorithm is the popular asymmetric encryption algorithm which is in use and was invented by three mathematicians, Ronald Rivest, Adi Shamir and Leonard Adlemen. RSA uses the

principles of “Modular Mathematics” and the difficulty in factoring a very large number into its two prime factors. The system contains two keys the Private Key and the Public Key each of which is itself a two number set. When the two numbers of one of the key is used in a mathematical formula with the document as the variable input, it produces a result which is the encrypted document. When the encrypted document is used as a variable with the other two numbers, it yields the original text through decryption.

## SSL System of Encryption

In web based communications between the browser of the E Commerce user and the E Commerce server, several confidential information including the credit card data is transmitted. Hence there is a need to ensure that the data in transmission is encrypted for security.

If the E Commerce customer has a Public and Private key pair along with the Server, then as in the case of Rama and Bhima, the customer can use the public key of the server and the server can use the public key of the customer for the purpose of exchange of information on both sides in an encrypted manner.

However, not all customers may have the dual key encryption capability and hence a hybrid method is used for encrypted transmission of data. This is called the “Secured Socket Layer” (SSL) encryption.

In SSL protocol, when the Browser connects to the Server, the server sends its public key to the browser as a part of the hand-shake procedure. Then the browser generates a random session key for symmetric encryption, encrypts the symmetric encryption key with the public key of the server and sends it back to the server. The server decrypts it using its private key and there after every packet exchanged between the server and the browser is encrypted with the session key under the symmetric system.

This is a hybrid Symmetric and Asymmetric encryption use which enables every server to correspond with the users in an encrypted data transmission mode. Where the server is equipped to use this mode, the URL displays “https” as the protocol instead of “http”.

## TLS (Transport Layer Security) Protocol

In order to strengthen the SSL system, security for exchange of data between two systems is enhanced with the TLS system. In this system, when a message is sent, the header information is fortified with a TLS header is inserted between the Internet Protocol (IP) header and the Transport Communication Protocol (TCP) header. The TCP header and the payload (the message)

is encrypted by TLS and the TLS header contains the encryption information to enable decryption at the destination.

The TLS Handshake Protocol is used to authenticate the participants of the communication and negotiate an encryption algorithm. This allows the client and server to agree upon an encryption method and prove who they are, using cryptographic keys before any data is sent between them. Once this has been done successfully, a secure channel (with encryption using a session key) is established between them.

After the TLS Handshake Protocol is used, the TLS Record Protocol ensures that the data exchanged between the parties isn't altered enroute. This TLS Record Protocol provides enhanced security using encryption methods like the Data Encryption Standard (DES). In doing so, it provides the security of ensuring data isn't modified, and others can't access the data while in transit

## Digital Signature System

Digital Signature System is one of the legally accepted system of authentication in many countries including India. The Digital Signature system is built on two components namely the "Hashing" and "Asymmetric Crypto System". A "Document" which requires to be authenticated by a "Person", is passed through two processes for obtaining the "Digital Signature" of the Document of the Person.

A Digital Signature as per Information Technology Act 2000(ITA 2000) is created by first calculating the Hash Value of a document using a standard approved hash algorithm and then encrypting the hash value of the document with the Private Key of the person issued under a Digital Certificate by a licensing Certifying authority.
For records, we can define the "Digital Signature of a Document of a Person as the hash value of the document encrypted with the private key of the person".

The Digital Signature is also an electronic document and after its generation, it is attached to the document and together they become a "Digitally Signed Electronic Document".

Technically, "Hashing" is a mathematical algorithm which takes the binary input of any electronic document as a numeric input and produces a "Hash Value" or a "Message Digest" through the specially created algorithmic process. The Hash Value is a smaller binary output which is

normally expressed as an alpha numeric value. The standard algorithms approved for use exhibit the following proven properties.

1. The hash value for a given electronic document (binary input) is always unique and no two documents produce the same hash value
2. The hash value for a given document is always consistent and the same hash value is produced every time the document is passed through the algorithm
3. The hash values of two documents which are different even by a dot, comma or space are significantly different.
4. The size of the hash value is always finite irrespective of the size of the original document. (Fixed length output)

The hash value is a one way process and can be produced from the document but the document cannot be re-created from the hash value. (It is considered computationally infeasible or difficult beyond reasonable expectation)

One of the popular hash algorithms used is MD5. But this is no longer recommended in legal standards in India. The other algorithms used are SHA1, SHA 256, SHA 512 etc. These are "Cryptographic Hash functions" as distinguished from ordinary hash functions such as CRC 32 which is used only to distinguish two dissimilar documents but does not contain all the properties of the hash functions mentioned above.

The Hash function enables checking of "Data Integrity" between two documents since even if one binary bit is changed, the resulting hash output changes significantly.

When a document is modified, even if the modification is insignificant or manually impossible to detect, the hash values of the modified document catches the modification instantly though it cannot determine what modification has been made.

In authentication of an electronic document, hash value determines what exactly was authenticated.

When the hash value of a document is encrypted with the private key of a person, since the "Private key" as a concept is the "Secret Encryption Key" used by the holder of the key pair, the resulting output namely the "hash value of the document encrypted with the private key of the person" is such an electronic document which has embedded within itself an identity of the document as well as the identity of the person. It is therefore called the "Digital Signature of the

person for the document". If the document changes, the digital signature changes since the underlying hash value changes. If the person is different then also the digital signature changes since the underlying private key changes.

When a signature is to be verified, the receiver of the digitally signed document decrypts the digital signature file to reveal the hash value as computed by the signer and then calculates the hash value of the received document himself using the same algorithm and checks if the two are same. For decryption, he uses the public key of the sender and successful decryption identifies that the earlier encryption could have been done only with the private key associated with the public key and therefore confirms the identity of the person. Since the two hash values tally, he confirms that the data has not changed. Hence the verification is a verification of the authentication of the signature.

To operate Digital Signature as a legally accepted form of authentication, the algorithms used for hashing and encryption must be an acceptable standard and there should be a method by which the "Public Key of a person" is confirmed to belong to a particular person by some independent authority.

When a person Rama sends a Public key to Bhima and says "This is the public key of Rama and if you have any encryption using the private key associated with it, you can consider it as the signature of Rama", Bhima needs to check if this information itself is trust worthy since it comes through the internet and could have come from a person who wants to impersonate himself as Rama.

Hence the legal systems accepting Digital Signature as a form of authentication, insist that there should be a confirmation of the public key of a person from a trusted authority.

In India we therefore have created an authority by law called the "Controller of Certifying Authority" (CCA)who licenses different Certifying Authorities and these licenced Certifying authorities (CA) issue "Digital Certificates" to digital signature users where in the public key is certified as belonging to a particular person.

Digital Certificate or Digital Signature Certificate (DSC) as it is often referred to is issued after a person subscribes to the DSC service of the CA to acquire a Digital Signature capability. For this purpose he makes an application with the necessary fees to the CA. The CA makes a verification of his identity with reference to the identity proof and address proof acceptable in law.

Then the CA invites the subscriber to generate the Public-Private key pair randomly in a computer session where the subscriber using his computer connects to the certifying authority's server. For the purpose of this Certificate issuing session, the CA creates a special log in page with a special password. Using this special log in page which normally is removed within 24 hours and using the special password (often sent through different secure channels), the subscriber "Picks up" the certificate during a certificate issue session. During this session, a random public-private key pair is generated in the computer of the subscriber (Not in the CA's server). After generation of the key pair and during the same session, the public key is sent to the CA's server. At the CA's server, the public key is received, it is wrapped into a Certificate which essentially says "This is the Digital Certificate issued to …… by ……. This contains the public key of …… associated with a private key which is in the custody of the subscriber. The algorithm used for creation of this key pair is ….. for encryption and … for hashing". This certificate will expire on ….." etc. (The particulars associated with the DSC are called the "Certificate Parameters".)

Before the session ends, the certificate is sent back by the server to the subscriber's computer and it gets stored. Then the session is closed.

If during the process, the session is interrupted, the process has to be repeated from the generation of a different set of public and private keys.

In the entire process, the private key never leaves the subscriber's control and it is stored within his control only.

Indian law recognizes that the private key is better secured if it is not stored within the subscriber's computer since the computer itself may be shared with someone else. Hence the system of storing the private key within the computer which is called "Soft Token" format is not recommended.

Instead, subscriber is encouraged to use a "Hardware Token" such as a USB based Cryptographic key or a Smart Card where the private key is stored and the token can be in the personal custody of the subscriber. When the certificate is picked up, the hardware token is connected to the computer so that the random key pair is generated within the hardware token and the private key remains there only while the public key comes out and goes to the CA server to be converted and returned as a DSC. After the session the token is removed and the private key remains within the token.

The token comes with software which does not allow the private key to go out of the token. However the Public key can go out during the CA issue process, the DSC can come in after the

issue by the CA and also exported subsequently whenever required. Immediately after the issue process is completed, a copy of the DSC is also stored in the computer so that there is no need to use the token only for the purpose of accessing the DSC/public key.

Further, the software comes into use whenever digital signature is to be applied. When a digital signature is to be applied on a document, the hash value of the document is calculated on the computer and is sent to the hard ware token. Within the hardware token the hash value is encrypted with the private key and converted into a "Digital Signature" which goes back into the main computer to be attached with the document to be signed.

At the time of the verification, only the public key of the signer is required and it is available in the DSC which is available outside the hard ware token.

(Students may refer to the E Book "Electronic Signatures made Easy" by Naavi"[xii])

Digital Signatures can be used in E Commerce for "Legally Accepted Authentication" of online contracts exchanged through e-mails.

India has also introduce an additional Electronic Signature system called e-Sign under Information Technology Act 2000/8, which can be used for real-time application of digital signatures on web based forms. It works on a one time use digital certificate issued by the CA at a very low cost and uses the Aadhaar based e-KYC system.

The e-Sign is an excellent option for validating online contracts for "Non Repudiable" authentication and may be considered by the E Commerce players.

## Encryption and Digital Signature for Data Security

In the above discussions we have discussed the use of encryption and authentication during transmission of messages. The same system can also be used for securing data under storage. An E Commerce entity needs to store confidential data of the customer including some times the sensitive data about the credit card numbers. In order to ensure that the stored data is not unauthorizedly accessed by hackers the data is normally stored in an encrypted manner using symmetric key encryption with the key being in the custody of the data manager.

It is also possible to use the Pubic Key Infrastructure (PKI) for encryption of stored data where the encryption may be done with the public key of the custodian by any person depositing the data

into a data store. Such data will be only available for decryption by the holder of the corresponding private key.

Handling of encryption of data in storage has to be handled with care since any loss of keys could mean loss of data even by the authorized users. Hence a proper system of key management including escrow of keys is part of the security management in such use cases.

## E Commerce Frauds

We have already discussed that the "Security Approach" in E Commerce or in IT in general is a "Risk Based Approach". Under this approach, an organization has to first make a "Risk Assessment" in which it captures the various possibilities of Risks that can arise to the information asset and accordingly design the security aspects.

In order to understand the risks in E Commerce business, let us very briefly recount some types of the E Commerce related frauds. The possibility of frauds are endless and include all types of frauds in which "Impersonation", "Hacking" or "Denial of Access" etc may be used. It is not possible to exhaustively list all such frauds but a few types of frauds are indicated below for records.

1. **Domain Name Related Frauds**

   Many of the E Commerce sites are known by the brand they create such as Flipkart or Amazon. Their respective official websites may be flipkart.com or amazon.com. One kind of fraud that people commit is to create confusingly similar domain names such as FLlPCART.Com or amazon.flashsales.com etc and invite consumers to the fake website, to either make fake sales or to steal the credit card credentials.

2. **Fake Vendors/Products**

   Fraudsters may register themselves as vendors of branded products on popular e-commerce sites and sell fake products. They may also release advertisements for direct sale or on non-genuine e-commerce entities, through Facebook or Twitter and cheat the consumers without delivering the product or delivering a fake product. There have been instances of logistic persons replacing original packages with fake packages/products also. There was also an incident of a courier of a food product vendor who consumed part of the food meant for delivery on the way to cheat the consumer of the full product.

3. **Modification of Order/Delivery Address**

If an attacker can compromise the website of the E Commerce, he can tamper with an order, to add unordered products to the order get delivery address modified, divert the payment through modification of the Banking particulars of the receiver etc. This could be more common in C2C transactions.

4. **Stolen Credit Cards**

It is common for attackers to use stolen credit cards, or debit cards or unauthorized Banking transfers to buy products on E Commerce websites and charge it to the card holder. These could be cases where "Phishing" or "Vishing" or other identity theft methods are used to commit a fraud subsequently on an E Commerce website.

5. **Refund Frauds**

Sometimes fraudsters may cancel genuine orders or fake orders paid where payment is in transit or has been faked and not finalized and claim refund from the E Commerce site owner. There have been instances of genuine offers in companies like FedEx such as "Refund if not delivered within a stated time" being misused and refund claimed when not due.

6. **Theft of Customer Data**

There have been many instances when insiders of an e-commerce company have stolencustomer data and directed enquiries received to a competitor**.** Stealing of Copyrighted digital works is also common. Infringement of Trademarkand Patent are also part of the E Commerce Frauds.

7. **Auction Related Frauds**

There are many instances of Auction related frauds where false bids are recorded to jack up the price so that the genuine bidder never wins the bid except at the price at which the seller wants.

8. **C2C E Commerce frauds**

C2C e commerce is prone to greater number of frauds since the verification mechanism for vetting the sellers and buyers may be weak. There are instances when buyers of OLX/Quikr paid by fake currency to the seller or used their visit to the prospective buyer

to make a recce for robbery or taking away a vehicle for test ride and vanishing etc. Selling of fraudulent goods is also an issue in C2C E Commerce frauds

A summary observation that can be made about the above types of frauds is that the problem basically arises because of the problem of identity on the internet. Use of trusted intermediaries and identity verification are therefore extremely essential along with the information security measures discussed earlier.

The legal issues in E-Commerce security are discussed separately in subsequent part of this lesson.

**********

## Part B:

**Introduction**

We have so far discussed the Business and Technical Aspects of E Commerce. In doing so, we have referred to many Legal issues. Now we shall discuss this aspect in greater details in this section.

# Indian Law of E Commerce

Computers were first used for scientific purpose in educational institutions initially to make complicated mathematical calculations. At that time computers were manly standalone systems in large computer labs. With the advent of desktop computers the era of "Personal Computing" dawned. With this, networking of Computers emerged and gradually expanded into "Internet". The Internet enabled sending of electronic communication over large distances and across geographical boundaries. Unlike the telephone which could only carry spoken words, Internet could carry long written messages. Internet later evolved in the 1980s along with the development of the computer OS systems like Windows and Apple Macintosh and could efficiently transmit sound, images and videos making it a total communication system.

Through this development of Computers, the E-Mail emerged as a useful tool of communication across distances and international borders. The expansion of E-Mail over Internet to the World Wide Web further changed the character of Internet communication and created "Websites" which could disseminate corporate information.

As long as Internet was used for personal communication and scientific use, there was no "Business" or "Financial" interest involved in the use of Internet. "Anonymity" was the rule and the object was to develop"Information Highway" or a "Global Repository of information" which could be easily accessed by all those who could connect to Internet with the use of the World Wide Web and E Mail.

However, considering the utility of the system as an efficient communication tool, the business community quickly started using it for communication replacing the system of letters and telephonic communication wherever possible. Initially money exchange was outside the Internet

and hence E-Business without the "Online Payment Systems" emerged. It was at this time that the Electronic Data Interchange as a system also emerged to enable data created in one format in one computer somewhere in the world could easily be imported and merged with the data in another computer using its own OS and formatting systems. As a result the business documents of different entities involved in commercial transactions could be easily merged.

At this stage, business realized that there could be technical errors and manual data input errors which could result in business disputes which could get into Courts for resolution. The need for a legal background therefore arose.

## UNCITRAL Model Law on E Commerce

Recognizing this need for developing a "Legal Base" for transactions done over a Network, the United Nations Commission on Trade Law (UNCITRAL) came up with a "Draft Model Law on E Commerce in 1996" and adopted a resolution in the UN on 30th January 1997 recommending interalia that all members of the UN should give favourable consideration to the said Model Law and enact operative law in their respective jurisdictions.

The member countries then started passing laws on these lines which were sometimes called the "E Commerce Act" and some time the "Computer Crimes Act" etc depending on the emphasis provided. Some Countries passed separate laws for "E Commerce", "Digital Signatures", and "Computer Crimes" etc.

The UNCITRAL Model law was intended to overcome obstacles arising from statutory provisions in different countries which were created for paper based transactions and did not recognize the electronic communications. It was therefore necessary to provide "Legal Recognition" to the electronic communication so that they could be considered as equal to paper based communication.

Additionally it was important to provide legal recognition to some method by which an electronic document could be authenticated so that the documents could be admissible in Courts of law as valid contractual commitments.

The need to enable the law to define Cyber Crimes and set up Information Security obligations etc was not paramount.

Details of how UNCITRAL Model law on E Commerce[xiii] developed can be found in the website of UNCITRAL. Presently this is relevant for the study of the legislative history since what is relevant for operations is the law as passed by the sovereign countries.

In India, the first manifestation of the UNCITRAL Model law on e-commerce was the "Electronic Commerce Act"[xiv] which was the first draft of the law taken up for discussion. This was an act which consisted 62 sections spread over XIII chapters.

This draft was converted into Information Technology Bill 1999 and presented in the Parliament in December 1999 and then passed as Information Technology Act 2000 (ITA 2000) and notified with effect from 17th October 2000.

ITA 2000 therefore is the first law on E Commerce in India and incorporated the legal recognition of electronic documents, digital signatures. It therefore provided the foundation for "Contracts" which could be constructed with the use of electronic documents which was essential for E Commerce. Additionally the law went on to define a few offences and contraventions as well as the dispute resolution mechanism such as Adjudication and Cyber Appellate Tribunal, to provide legal protection to E Commerce related activities.

India did not however pass separate law for "Domain Names" and let disputes arising therefrom to be handled under the Trademark related interpretation of the Domain Name Contracts. Copyright and Patent issues related to E Commerce were left to be handled by the respective laws which were amended from time to time for the purpose.

ITA 2000 also brought in consequential amendments to other Acts such as the Indian Penal Code (IPC), Indian Evidence Act 1872 (IEA), the Bankers Book Evidence Act 1891 and RBI Act 1934.

No amendment was however made to the Indian Contract Act 1872. (ICA)

However, ITA 2000 through Section 4 extended the applicability of all legacy laws to "Electronic Documents" and hence it was not necessary to amend individual laws such as the ICA. While extending the applicability of legacy laws to the use of Electronic Documents, a few types of documents such as "Negotiable Instruments", "Power of Attorney", Trust Deed", "Will" and "a document that transferred title in an immovable property" were excluded. (P.S: Cheques were removed from the exclusion list in 2003 by an amendment).

In 2008, major amendments were made to ITA 2000 and were notified with effect from 27th October 2009. The amended version came to be known as ITA 2008 and incorporated "Cyber Security" concepts and also expanded the offences section of the law. It also brought in the "Data Security" concept in greater clarity through the introduction of Section 43A and 72A and he rules on Reasonable Security Practice and Due Diligence for Intermediaries.

Today ITA 2000/8 is therefore the law that defines the E Commerce operations in India. Further the Tax laws have been amended from time to time including the GST and regulations regarding FDI have necessitated some E Commerce guidelines to be issued. They have therefore become supplementary laws affecting E Commerce.

Following the introduction of Digital Payment systems in the Indian Banking scenario, the RBI came up with the "Payment and Settlement Act" which has an impact on the Digital Payment industry which is closely associated with E Commerce.

Aadhaar Act which has an impact on digital payment systems and establishing the identity of an aadhaar user in India also has an impact on the E Commerce industry.

With the increased attention to "Privacy Protection" and the judgement of Supreme Court to uphold Privacy as a "Fundamental Right", India has now drafted a new law titled "Personal Data Protection Act". This will seriously affect E Commerce players and make substantial changes to the ITA 2000/8 as it applies to E Commerce Companies.

All these legislations therefore determine the legal foundation for E Commerce in India and we shall try to discuss some of the salient features of the principle legislation namely ITA 2000/8 in the following paragraphs.

## Online Contracts

One of the key aspects of law that has an impact on E Commerce is the way law treats online contracts. In India we need to look at ITA 2000/8 along with ICA 1872 to derive the law related to E-Contracts or Cyber Contracts or Digital Contracts, whichever term we would like to use.

Under the ICA, a contract is an agreement enforceable under law. A Contract is entered into by one party (or more than one) making an offer and another party (or more than one) accepting the offer.

Online Contracts are contracts that are entered into with the exchange of the offer and acceptance documents online. A detailed discussion about Digital Contract is out of scope of this section. We can however recall some salient features of digital contracts as are relevant to online contracts.

A Contract is entered into between two parties who are competent to contract (i.e.: not a minor, undischarged insolvent or of unsound mind) for a legal objective, under a free consent and for a valid consideration.

Contracts can be "Oral" or "Documentary". However all online contracts are "Documentary" since even recordings of spoken words are electronic documents.
In the ICA, there is no legal difference between Oral and Documentary contract except the hurdles the
"Oral Contract" places in terms of "Evidence" to resolve disputes particularly in terms of detailed covenants in the contract.

Oral Contracts need to be often proved with the presentation of "Witnesses" who can prove the agreement or its covenants as specifically stated by the parties in their presence. They will be "Eye Witnesses" for the Contract formation.

Contracts can also be "Implied" by the conduct of the parties and are called "Implied Contracts". Implied contracts could be formed when there is no documentation and when there are no "Eye Witnesses".

Documentary contracts are entered into with an "Offer Document" issued by one of the contracting parties which is "Accepted" by the other. Where the recipient of the offer document does not agree with the offer document in its entirety, he raises the counter suggestions which become a "Counter Offer"or the new "Offer". The "Offer" and "Counter Offer" will continue until all the terms of one version of the offer/counter offer becomes acceptable to the other party and he conveys his acceptance.

The conveyance of acceptance to an offer brings the contract to life.
In the world of "Online Contracts", an offer document can be sent by e-mail and the acceptance can be provided by a return e-mail.

However, often online contracts are concluded by one party displaying his terms on a web page to which the other party accepts by clicking on a button which may say "Accepted" or "I Agree" etc.

Under the ITA 2000 as amended in 208 (ITA2000/8) an Electronic Contract can be concluded by an offer and acceptance documents exchanged with digital/electronic signatures of both parties. Since an electronic document (Other than the excluded documents under Section 1(4) of ITA 2000/8) are equivalent to paper documents and an authentication as per Section 3 or 3A of ITA 2000/8 is equivalent to a "Signature", an electronic offer with a digital/electronic signature and an electronic acceptance with a digital/electronic signature is a valid documentary contract in India
In the case of online contracts where undigitally signed e-mails are used as "offer" and "Acceptance", or when the "I Agree" button is clicked on the webpage, the formation of contract does not fulfil the terms of a written documentary contract.

Even when documents are exchanged in PDF format and there is a "Signature" which Adobe calls as a digital signature, it is still not a "Digital/Electronic Signature" as per the definition of ITA 2000/8.
Contracts entered into with such documents therefore do not have the equivalence of a written documentary contract.

Further if the contract is a for a purpose which is though legal falls into the category described under Section 1(4), it would not be a recognized contract since Section 4 (Legal Recognition of electronic document) as well as Section 5 (Legal Recognition of Electronic/digital signature) is not applicable to such documents.

The Contract formation through the clicking of a button ("I Agree") is often referred to as "Click-Wrap" contract and may have recognition in US. However, in India, "Click-Wrap" contracts are as good as "Implied Contracts" only.

It can however be accepted that the E Commerce industry has made it a practice to make use of "Click Wrap" contracts and for ordinary E-Commerce contracts, it has become an accepted business practice though we do not rule out such contracts being rejected by an Indian Court when challenged.

As an "Implied Contract", Click-Wrap contracts can be strengthened by firstly making the "Click" a "Consent based on some affirmative action". Example could be to tick a check box, or enter a Captcha or enter an OTP etc. The "Implied Contract" can also be fortified with collection of "Meta Data" associated with the activity.

However Click-Wrap Contract will remain a form of contract which in India will be subject to legal questioning.

It may be considered therefore be technically considered as a "Voidable" contract.
Another problem of "Click-Wrap" contracts in the E Commerce scenario is that such contracts are almost always "Standard Form Contracts" or "Dotted Line Contracts". In such contracts, one of the parties which is in a "Dominant" position, gives a "Take it or Leave it" offer to the other who has no option but to accept it as it is or refuse the contract and the attendant service in toto.

This is certainly the case in the B2C transactions though it may not be so true of B2B contracts though if the formation of contract is through "Click-Wrap" method, the "Dotted Line Argument" can always be produced as a defence to invalidate the contract.

In India the law on such contracts has been clearly laid down in many of the Supreme Court decisions on "Unconscionable contracts" including the CERC Vs LIC of India (1995 AIR 1811, 1995 SCC (5) 482) and the related citations. In such contracts, it is the duty of the dominant party to sufficiently highlight what could be an unfair one sided covenant of the contract and obtain specific consent from the other party, failing which the contract may suffer from "Lack of meeting of minds".
Indian law had permitted the use of "E-Sign" as a digital signature equivalent for real time transactions which could be used for obtaining valid signatures on online forms by any contracting party. Unfortunately, without appreciating the benefit of this system, the honourable Supreme Court in its Aadhaar Judgement of September 26, 2018 virtually banned the use of e-Sign by private companies. Hence this option for validating the online contracts was lost.

However, UIDAI (Unified Identity Authority of India) has come up with a scheme of "Virtual Aadhaar ID" as well as "Offline Aadhaar Authentication" which could be used in conjunction with the activity of a "Certifying Authority" to issue one time digital signing certificates as in the case of e-Sign. (Appropriate notifications in this regard are awaited as on the date of this writing).

A work around to the problem of obtaining valid signatures on online forms in the absence of e-Sign has been provided in the private sector in the form of CEAC-EDB (CEAC-Evidence Drop Box) [xv] which uses the provisions of Section 65B of Indian Evidence Act, where a third party can provide witness to an electronic event by certifying the electronic documents that evidence the activity.

## Shrink-Wrap Contracts

Shrink-wrap contract is a term which is used in cases where an acceptance of a contract is recognized with the event when the acceptor opens a shrink wrapped package without fully being aware of the terms of offer and being aware of only a few salient features.

An example of such a contract is when a software is delivered on a shrink-wrapped CD with the condition that "If the shrink-wrap" is opened, the software is deemed to have been accepted as per the terms of the End User License Agreement (EULA) contained within the document.

The accepted norm in such cases is that the outer package should indicate the presence of a detailed contract inside and the user is presented with the electronic contract immediately when the CD is inserted into the user's computer and consent obtained say by registration of the product or otherwise before the software becomes operational.

## Digi-Meta Contracts

In the context of "Digital Contracts", we can also recognize a new type of contracts which is a "Hybrid Digital Contract".

The definition of a hybrid "Digi-Meta Contract" as Naavi[xvi] defines is

> *"a Contract where any one of the components of the contract formation instrument is rendered in electronic form and the other in paper form"*

In other words, a Contract where either the "Offer", "Acceptance", "Performance", "Consideration" or any other component is in electronic form while some other component is in paper form can be classified as a "Hybrid Contract" or more specifically a "Digi-Meta Contract".

An example of a Digi-Meta Contract is

- An offer is sent by paper and acceptance is sent by e-mail with unmistakable reference to the paper offer. Or vice versa.
- The contract is made on paper but the object of the contract and the performance is in the form of an electronic document. E.g.: Contract for designing and hosting a website
- Contract is made on paper but the payment is made through online payment
- Consideration for a contract is paid in Crypto Currencies

- Authentication to an electronic document is expressed in terms of a hash value written in a paper document with appropriate reference which is physically signed. (hybrid authentication)
- A person becomes a member of a website, pays money online by converting his physical cash such as Rupees or Dollars and acquires some digital rights/properties.
- A Contract which may be an ordinary oral or paper based documentary or an implied contract or a digital contract or a digi-meta contract where the dispute resolution is mandated through an Online Dispute Resolution mechanism.

The Digi-Meta contract or the e-Contract is identified as types of contract because of the difference in the formation of such contracts. Otherwise the inter-se liabilities of the parties are determined by the Indian Contract Act only.

The specific areas where the Digital Contracts need to be especially distinguished are in terms of the "Evidence" to be produced to prove the formation of the contract and the applicability of the different covenants in the contract.

## ITA 2000/8 on Online Contracts

In online contracts in an E Commerce context, quite often, the consumer responds to an E Commerce Company through a website and a server of the E Commerce Company which sends automated responses on behalf of the company.

The response could be as mundane as an "Acknowledgement" in respect of a complaint or a request etc. or a more detailed "Offer" or "Counter Offer".

In some instances the service is offered by a website through a "Terms and Conditions" document which carries the button "I Agree" which the customer clicks in acceptance. The wordings used in the document and how the system is configured subsequently, determine if the document is an "Offer" or an "Invitation to Offer".

An "Offer" is converted into a contract if the customer "Accepts" by the Clicking of the button "I Agree". On the other hand, an "Invitation to offer" when "Accepted" will generate an "Offer Document" from the customer which needs to be accepted by the E Commerce service provider before it becomes a contract.

If the Terms indicate that "Registration" of the software or the client is " mandatory", then when the customer submits a registration request, it is like a "Offer" based on the "Invitation to offer" contained in the Terms. When the Registration is confirmed and the contract becomes operational, key to use the service gets generated and is sent to the consumer. The irrevocable acceptance of the contract occurs when the key is actually "received" by the consumer and used to activate the software.

In the above process, there are several automated responses that are generated by the server without any manual intervention. Some of these can go into a dispute.

Further, when we distinguish between the "Offer" and "Invitation to offer", we also introduce an element of doubt as to when did the final irrevocable acceptance happen and where did it happen?. This can have implications in a dispute.

Hence the law of online contracts need to define how the automated responses of servers are to be accounted for and how the time and place of formation of a contract need to be established.
Fortunately, the Indian Cyber Law in the form of Information Technology Act 2000 as amended (ITA 2000/8) clarifies all these aspects.

ITA 2000 had provided equivalence of paper and electronic documents so that contract formation could be recognized when the offer and acceptance in a contract was done through an electronic document. However in the amendments of 2008, a further clarification was added in terms of Section 10A to confirm that

> "Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose."

There is therefore no issue in accepting the contract formation when the offer and acceptance is in the electronic form.
ITA 2000 itself had provided clarification on how the automated server responses as well as the "time and place" of a contract can be determined.

Accordingly, under Section 11, "Attribution" to an electronic document is defined as

> "An electronic document shall be attributed to the originator if it was sent by the originator himself, or by a person who had the authority to act on behalf of the originator

in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically"

The law therefore recognizes an "Originator" for every electronic message and the "Originator of a message that constitutes the Acceptance in the case of an online contract is the person to whom the acceptance is attributed and is deemed to be the contracting party".

If a server is programmed to send a message on behalf of the originator automatically, then the person who causes the system to behave automatically becomes the originator.
The "Owner" of the automated device therefore becomes the originator.

In view of this provision, in Indian law, the E Commerce website/facility owner is always the "Originator" of an automated server response. This argument holds good even when an automated "Chat Bot" answers on behalf of the E Commerce service provider or even a humanoid robot like "Sophia"[xvii] operates the responses on behalf of the service provider.

ITA 2000/8 also provides clarifications on how to determine the "Time and Place" of a contract "if the contracting document does not specify otherwise".

According to section 13 of the ITA 2000/8[xviii] an online contract occurs when the final acceptance message leaves the sender's system and enters the receiver's system.

There are a few uncertainties that we need to deal with in this transmission of the message since the sender's electronic system may be in some geographical jurisdiction and the receiver's electronic system may be in some other geographical jurisdiction and the transmission has to travel from one system to other through many intermediary systems.

In this transmission, the message may be lost or delayed or even tampered with.
What Section 13 states is that a message is deemed to have been sent as soon as the message leaves the system of the sender. Hence it becomes an irrevocable communication as soon as the message leaves the sender's system.

At the same time, the time of receipt by the receiver is recognized as the time of entry into his system. Here the law makes another distinction. If the Receiver has multiple systems, has designated a specific system to which the communication is to be sent, and the message is sent to such a designated system, then receipt occurs at the time the message enters the system. However, if when such a designated system exists in the contract, the sender sends the message to a

different system (also owned by the receiver), the receipt occurs when the receiver opens the message.

If therefore a dispute occurs on when the message was received, the fact whether a system (e.g.: an email address say xyz@gmail.com or xyz@yahoo.com) had been designated by the receiver and whether the sender sent the message to the designated address or not becomes relevant.
As regards the jurisdiction to be applied for a contract, in order to determine the place where the final acceptance to an online contract is provided, ITA 2000 provides the following guideline.

d) In the case of individuals the place of residence is deemed to be the place of usual residence.
e) In the case of Business entities, the usual place of residence is the "Principal place of business"
f) In the case of Non Business organizations, (e.g.: NGOs) usual place of residence is the "Registered Office"

ITA 2000 also clarifies the effect of and the need for the recipient to send an "Acknowledgement" of a message to make it effective.
Under Section 12 of ITA 2000/8,

c) Where the originator has stipulated that the electronic record shall be binding only on

receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

d) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Where the originator has stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by – any communication by the addressee, automated or otherwise; or any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

We may reiterate that the above provisions may be overridden by specific mention in the contract. However, we have already stated that in the Indian Context Click Wrap contracts are not recognized and an undigitally signed contract is only an "Implied Contract". Hence the default provisions of the ITA 2000/8 under sections 11, 12 and 13 would be applicable in derogation of any specific mention of the attribution, acknowledgement, time and place or jurisdiction mentioned in the online terms and conditions document.

Some may refer to this set of provisions as well as the liabilities of intermediaries to the transmission discussed in the following paragraphs as a "Mail Box Rule".

## Privity of Contract

In a situation where there is a contract between two parties, one of whom or both use the services of sub contractors who are "Agents", a question arises as to whether a contracting party can hold the downstream contractor of the counter party liable for any wrongful loss caused to him.
In such cases it becomes necessary to establish if any "Privity of Contract" exists between the party which raises the dispute and the party on whom the liability is hoisted.
It is a common principle which is called the "Privity of Contract" which states that "No one but one of the parties can go to court and enforce the contract even if the contract was to operate to a third party's benefit"

Some times such "Privity" gets established through the contractual document itself. If for example, an agent signs a contract but discloses that the contract is being signed on behalf of another party who is his principal, the other contracting party may sue the principal though the principal himself has not signed the contract.

In such cases the principal may defend himself to say that the conduct of the agent was prima facie indicative that he had no such rights to bind the principal. This would be a fact to be established in a given case.

For example, If a director of a company signs a contracts and binds the company, then even if he may not have a "Resolution" backing such a power, the principle of law of "Lifting of Corporate Veil" may be used to invoke liabilities on the Company.
If however a contract is signed by an "Undisclosed Agent" then the principal may say that there was no privity of contract with the party raising the dispute and hence he should not be dragged into the litigation. In such cases, the agent may be held liable for the contract. In a contract where

the agent has disclosed that he is only the agent of a named principal, the principal is bound by the terms of the contract.

In the case of a Minor, there is no liability on the minor. But in e-contracts, "Minority" is not easily recognizable as in the physical contract scenario and hence poses a challenge.

In most of the cases where an agent has to enter into such agreements with third parties, the back to back contract with the principal may have an "Indemnity Clause" which may determine if the agent has to absorb the liability himself or it is boarne by the Principal. As regards the third party who invokes the contractual obligation against the signer (agent), the proceedings will lie only with the agent and not the principal who is behind the scene.

Another exception allowed is under special laws such as Negotiable Instrument Act applicable to Cheques or Bills of exchange or Promissory Notes. In these cases, enforcement rights are created between non-signatories as the cheque exchanges hands, from one bank to another or from one person to another. (Eg: Drawer or an endorsee is liable to a subsequent holder in due course)
Similarly, contracts that restrict or impact upon the use of land (e.g.. An easement) may be enforceable upon the next land-owner, even though they were not privy to the original contract. This is an old exception to the rule of "privity of contract" that is still applicable today.

Also, under the law of trusts, where a person may contract to the benefit of another, operates to convey certain rights to the third party even though, in fact, this third party was not party to a contract which created the trust.

The Court may however have the discretion on the basis of the circumstances of the case to allow a party who may not appear to have the privity of contract to be brought into the litigation.

## Jurisdictional Issues in E Commerce

Jurisdiction issues in E Commerce are also under constant discussion. Every country incorporates the extra-territorial jurisdiction in its laws and so also has India. Section 75 of ITA 2000/8 makes contravention of any of the provisions of ITA 2000/8 also applicable to persons outside the geographical boundaries of India as long as at least one computer in India has been used in the commission of the contravention.

Though Section 75 of ITA 2000 appears to restrict itself to contraventions and offences, the principle of Section 75 should be also extendable to the formation of contracts, application of

Section 11 to parties and automated systems outside India, and as to the liabilities of intermediaries outside the country.

The data protection laws (e.g.: Proposed Personal Data protection act 2018 draft or GDPR) often speak of "Data Localization" to reinforce the jurisdiction of local laws to the activities related to the processing of personal data. Russia is now in the process of actually segregating the "Russian Network" by law into a domain with sovereign control of the Russian Government. China practices it within the current set of their laws.

It is therefore reasonable to expect that the extra territorial jurisdiction under Section 75 of ITA 2000/8 stands extended to all aspects of ITA 2000/8 including Sections such as 11,12,13,14 etc. In due course Judiciary may endorse this view when called for.

In the past there have been several discussions on international jurisdiction regarding E Commerce transactions. These have been under a regime where Internet was considered a "Border less society". In the present circumstances where legal borders are getting introduced through the data protection laws, it is not clear whether the earlier concepts of jurisdiction actually apply.

In most cases Courts have taken a stand that if the interest of people in the local jurisdiction is affected by an action in Cyber Space, then the local Courts have a jurisdiction. If a website is in a particular language, if it has a customer contact office or if targets its services specifically to the citizens of a specific country, then the local jurisdiction cannot be avoided even if the contract with the customer may say so. In the case of "Taxation" there may be a clarity but taxation jurisdiction does not always extend to jurisdiction regarding crimes.

Sometimes, the legal jurisdiction may be claimed because of the law but enforcement jurisdiction would still be an issue. The law enforcement authorities in one country may not get into another country to enforce their rights except under established international norms such as the support of a Treaty or other mechanisms through the Interpol.

The cases of Dmitry Sklyrov the Russian programmer who was arrested while on a visit to USA for violation of Digital Copyright Law of USA, is a case worth studying on how the enforcement jurisdiction is applied in practice. In India, the Baazee.com case was one where a US Citizen of Indian Origin who was the CEO, was arrested in India and charged of an offence committed by a customer of the company on the website.

These issues of Jurisdiction will always remain a point of dispute but what businessmen should understand is that more than the law, it is the intention of providing a service to a specific group of people which becomes the benchmark for enforcing jurisdiction and unless special disclaimers are invoked, it is difficult to escape the jurisdiction of laws of other countries on the business set up in a designated country.

In respect of laws such as GDPR, it is therefore recommended that E Commerce companies in India carry a "GDPR Exclusion Clause"[xix] in their terms and conditions.
Similarly while framing the dispute resolution mechanism for their websites, if the E Commerce websites opt for Arbitration, then they will have to define not only the "Applicable Laws" but also "Place of Arbitration" in such a manner that the provisions are within the purview of the local laws.

## Domain Name Contracts

The "Domain Name" is often an important part of E Commerce since it establishes the "Brand" identity of the Company or product. If therefore the domain name is changed then there could be loss of business. Improper domain names can also give room for legal suits on Trademark related issues.

Hence even before an E Commerce company intends to launch its business, it has to secure a good domain name. Having identified a good domain name on which the company is proposing to invest money to build a brand, the  Commerce operator has to be alive to the possibility that the domain name may be confusingly similar to another established domain name or a treademark. If this issue is not examined early and resolved, the E Commerce business would be adversely affected on a later date if some body challenges the use of the domain name.

Hence it is necessary for the E Commerce company to be fully conversant with the law of domain names and factor in legal issues involved in the registration of domain names.

Domain names are registered on a first cum first served basis by registrars accredited by ICANN. (Internet Commission on Assigned Names and Numbers". ICANN is a self-regulatory, non-Government body that controls the technology of the internet and also the IP address allocations and domain name allocations.

Though domain names are allocated on availability to the first person who tries to register the selected name, the registrars get an online "Contract" executed on a "Click Wrap Basis" which includes the terms under which the domain name is registered and in case of a dispute on a later date, how the rights of the registrant would be settled.

The domain name contractual terms may be different for different TLDs, (Top Level Domain Names), between Generic names managed by ICANN directly and the Country Code domain names (such as .in, .cnetc) which are administered by respective countries, and between one type of TLD an other such as .com, .info,etc.

All domain name contracts are subject to a Dispute Resolution Process. .com/.org/.net type of domain names are governed by what is known as the "Uniform Dispute Resolution Policy" (UDRP) and .in domain name disputes are governed by what is known as "INDRP" (Indian Domain/Dispute Resolution Policy).

The UDRP disputes are resolved by designated dispute resolution organizations registered with ICANN and INDRP dispute resolution is handled by NIXI. Both are "Arbitration" mechanisms for which necessary procedures have been prescribed.

E Commerce companies which may have a huge stake in the domain name need to ensure that at the time of registration, a proper care is taken to chose a non-controversial name and subsequently monitor if there is any other similar site coming up and take action both to defend its name rights and prevent others from encroaching its name space by initiating offensive action.

Services such as "Verify For Look Alikes"[xx] verifying and providing disclaimers for any competing domain names may be explored as the first line of defence against such domain name related disputes.

## Intermediary Guidelines

ITA 2000 considers E Commerce entities as "Intermediaries" under Section 2(w) of the Act. Apart from the applicability of various provisions of the Act as are applicable to any "Person" including a "Body Corporate", the responsibilities of the intermediaries is specially mentioned under Section 79 of the ITA2000/8.

Section 79 of ITA 2000/8 is a provision which is often mis-understood. The section states as follows:

**Chapter XII. Intermediaries Not To Be Liable In Certain cases**

**Section 79: Exemption from liability of intermediary in certain cases**

(1)Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.

(2)The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf

(3)The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

An intermediary as defined under Section 2(w) means as follows:

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any

> service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

The section 2(w) unambiguously quotes “Online market places” which are some of the popular E Commerce entities, along with other entities such as telecom service providers, webhosting companies, online payment sites etc as “Intermediaries”.

Section 79 speaks of situation where the “Intermediary is not liable” for any contravention of law arising out of third party information, data or communication link hosted by him.

In an E Commerce scenario, the E Commerce website/service hosts both second party and third party information on its website. For a transaction between the E Commerce site and the Customer who may be a “Buyer”, the “Seller” or a contracted service provider such as a payment gateway, is a third party though there is a privity of contract directly between the E Commerce site owner and the “Seller” or “Contractual Service Provider”.

Does this mean that if a seller on a market place provides some false information and makes a sale to the customer, the market place is not liable?

If we analyse the Section 79, one of the conditions under which the intermediary can escape liability is that the

> “function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored”.

This condition applies without doubt to an Internet Service Provider or a Hosting Service Provider. But it becomes difficult to accept that an E Commerce service provider (Even the market Place) can be considered to have limited its function only to make the information available to the customer and nothing more.

Though the conditions of Section 79(3) can be presumed in most cases, conditions of Section 79(2(b) is difficult to be established and condition of “Due Diligence” under Section 79(2(c) is broad enough to make the life of an E Commerce entity difficult in invoking protection under this section.

It is business prudence if the E Commerce entity considers that any Offence or contravention of law if it can be traced or attributed to an information in the custody of the E Commerce entity, then there will be liability assigned to the entity.

Further, with the operation of Section 85 of ITA 2000, an offence attributable to a corporate entity can be further get attached on the persons in charge of business including the CEO/Directors if they cannot provide the defence of "Due Diligence" or "Lack of Negligence".

Section 43A of ITA 2000/8 separately requires a "Body Corporate" handling "Sensitive Personal Information" to exercise "Reasonable Security Practices" failing which the liability arising thereof can be hoisted on the Company and thereafter on the managerial persons.

It is therefore necessary that every E Commerce entity takes full responsibility to comply with all the provisions of ITA 2000/8 so that it can prove that it was in compliance of law as and when it is challenged with a liability under ITA 2000/8.

This ITA 2008 compliance requirement is the "Techno Legal Security Compliance" that every E Commerce organization is expected to fulfil.

With the advent of Personal Data Protection Act (PDPA) which is presently in draft stage, the responsibilities of all organizations handling "Personal Information" will increase several folds.

Under ITA 2000/8, designation of a "Grievance Officer" was mandatory. Under PDPA, the designation has to be upgraded to "Data Protection Officer".

The E Commerce entity should not only take all reasonable steps in compliance based on a risk assessment, but also maintain adequate documentation of its efforts to escape liability.

It is for this reason that every E Commerce entity need to consider "Law Compliance" as an integral part of its business and take suitable steps to be compliant always.

## Dispute Resolution on Transaction

Despite the best efforts of an organization, disputes with customers cannot be avoided. In case of an E Commerce entity which acts an intermediary between several suppliers and the consumer buyers, the possibility of disputes is even higher.

ITA 2000/8 expects that every intermediary have in place a suitable Dispute Resolution Mechanism. Such Dispute Resolution Mechanism may not be limited to a " Help Desk" that resolves the technical and functional issues. It has to incorporate ability to handle disputes which are in the border of legal disputes. Hence a responsible "Grievance Redressal Officer" should filter all incoming complaints and where there is a need for resolving it with an application of a legal mind, refer it to the Grievance Redressal team other than the technical help desk. Some times the dispute may have to be escalated to the legal help desk after the technical help desk has reported completion of its resolution.

The legal help desk may consist of an "Ombudsman" who tries to resolve the dispute using his own respectable status. But if the resolution is not successful, higher levels of dispute resolution such as "Mediation" and "Arbitration" may have to be tried before the consumer is forced to resort to external judicial solutions.

In this process availability of a fair and easy to access system such as an ODR (Online Dispute Resolution)[xxi] would help.

Judicial resolution is subject to the "Jurisdictional Issues" and expensive besides being time consuming.

## Evidence Related Issues

When E Commerce related disputes arise, there will be need for both the consumer and the E Commerce merchant to produce appropriate evidence to substantiate their point of view.

As regards the online contracts, we have already discussed that India does not recognize Click Wrap contracts except as "Implied Contracts" and hence cannot be invoked by the E Commerce entity particularly when detailed contractual terms are involved.

Law provides for use of "Digital Signatures" if the E Commerce entity enables the use of approved form of digital/electronic signature. The e-Sign is an effective form of low cost authentication that can be obtained for online contracts though it is not being used by the E Commerce entities in India since they are driven mostly by their international experience and may either not be fully conversant with the law as it prevails in India or would like to ignore them.

As regards the Consumers, they often make purchases in an E Commerce website based on the information they see on the site at that moment. Once the purchase is concluded, the information about the product may also get removed from the e-commerce site.

Hence if a dispute arises subsequently, the Consumer may not have any evidence of what the product offering stated and what were the warranties. The E Commerce merchant may have a copy of the same along with the version of any online terms he might have presented to the consumer at any point of time. If however the terms or the warranties are not produced by the E Commerce merchant, it is not easy for the consumer to force their presentation. More often they may not exist since they could have been deleted.

Under the circumstances, evidence of an e-commerce transaction as acceptable in a dispute resolution entity such as a formal Court is hard to find particularly for the Consumer.

However, Indian law has a special provision called the Section 65B of Indian Evidence Act which can provide a work around for the system. According to this provision, any electronic document is an "Admissible" evidence in a Court of law if it is produced with a proper certification as indicated in Section 65(B) of Indian Evidence Act 1872 as amended when ITA 2000 was notified on 17$^{th}$ October 2000.

The essence of Section 65B of IEA lies in the recognition that an "Electronic Document" is a stream of binaries captured by a digital capturing device and stored in a digital storage device and interpreted for human consumption by a set of software and hardware. Hence what we call as Evidence is what a human being sees, hears or reads is dependent on the manner in which the binary stream is converted into human experience through the output devices. The hard disks or pen drives or CD ROM s or Memory cards that we normally hold in hand are mere containers of the electronic document and not the "Original Electronic Document" as many of us may loosely refer to. Containers may change but the relevant evidence remains within it and the judiciary should be able to take cognizance of the evidence irrespective of the container in which it is presented.

Hence Section 65B defines a "Computer Output" as the form in which electronic evidence can be presented for "Admissibility" and such Computer output can be either in print form or in electronic form and become admissible if it is rendered with a certificate that contains the identified evidence, the process by which it was obtained, the devices used for its production and the particulars of the person who rendered it, along with his signature.

The strength of the Section 65B is that while the owner of an electronic document can always print out his own electronic document and sign it just like a letter where he uses the computer as a type writer, a person who is not the owner of an electronic document contained inside a computer can also print out the document and sign it along with the Section 65B certificate and make it admissible. This is the typical process used in the Bankers Book Evidence Act also where the current Bank official may sign an extract of a ledger created by an earlier Bank official and certify it for production to a judicial requirement.

Such a Certified copy of the electronic document is admissible even when the original document might have been removed subsequently.

Under these provisions, the consumer can capture the online contract or the product information as is visible as an electronic document preferably by a trusted third party certification and use it as an admissible evidence in a Court if there is any dispute in future.

A Service called CEAC-Evidence Drop Box[xxii] also enables the dropping of an electronic document as provisional/contingent evidence which can be retrieved later if required.

The correct legal position of the Section 65B has been explained by the Indian Supreme Court in the P.V.AnvarVsP.K.Basheer[xxiii] case. Some confusion has been created by a subsequent judgement of a smaller bench in the case of Shafi Mohammed[xxiv] which needs to be placed in its own perspective.

The correct position is that a properly certified copy of an electronic document as per Section 65B may be produced in a Court either in print form or in electronic form and is admissible without the production of the original. The admitted evidence may however be challenged by the defence with its own evidence supported by any forensic records if any which also has to certified properly with its own Section 65B certificate. The Court also has the freedom to invite its own "Expert" who is accredited as a "Digital Evidence Examiner" as per Section 79A of the ITA 2000/8.

[P.S: A more detailed discussion on Section 65B is out of scope of this lesson. Interested students may refer the Book : "Section 65B of Indian Evidence Act Clarified" by Naavi[xxv]]

**References:**


1. https://www.naavi.org/wp/ita-2008-already-has-a-provision-if-sophia-breaks-our-law/
2. http://ita2008.in/ita_2008/ch4_2008.htm

3. https://www.naavi.org/wp/creating-protection-indian-companies-european-hegemony/
4. http://www.lookalikes.in/
5. http://www.odrglobal.in/
6. http://ceac.in/wp/ceac-edb/
7. http://ceac.in/wp/2017/04/25/basheer-case-judgement-and-section-65b-of-indian-evidence-actcyber-jurisprudence-develops/
8. http://ceac.in/wp/2018/04/19/the-tragedy-of-shafhi-mohammad/
9. http://www.naavi.org/ebook2011/index.htm
10. https://www.naavi.org/wp/index-of-articles-on-bitcoin-the-currency-of-the-criminals-by-the-criminals-for-the-criminals/
11. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0
12. https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=243
13. http://www.naavi.org/cl_editorial_11/ggwg_rbi_circular.pdf
14. http://www.naavi.org/archives/archive_2011/comments_ggwg.htm
15. http://www.naavi.org/cl_editorial_11/ggwg_rbi_circular.pdf
16. https://www.naavi.org/wp/umashankar-judgement-upheld-by-tdsat/
17. https://www.naavi.org/wp/a-note-for-the-attention-of-smes-on-cheque-disincentivisation/
18. https://m.rbi.org.in/Scripts/FAQView.aspx?Id=24
19. http://www.naavi.org/importantlaws/it_rules_compendium/adj_off_notification_goi.pdf
20. http://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf
21. https://www.naavi.org/wp/umashankar-judgement-upheld-by-tdsat/
22. http://naavi.org/uploads_wp/new/juy_72017_limited_liability.PDF
23. https://www.naavi.org/wp/zero-liability-is-there-a-fine-print-that-depositors-should-be-wary-of/
24. https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
25. https://www.iso.org/isoiec-27001-information-security.html
26. https://www.naavi.org/wp/india-to-be-the-hub-of-international-personal-data-processing-objective-of-pdpsi/
27. https://www.mea.gov.in/Images/pdf1/S7.pdf
28. https://www.incometaxindia.gov.in/Pages/i-am/non-resident.aspx?k=Introduction
29. http://www.cbic.gov.in/resources//htdocs-cbec/gst/51_GST_Flyer_Chapter42.pdf;jsessionid=1ED151DA92373BD69A16E314BC731BED

*P.S: Since the entire content has been drawn from dynamic resources in the Internet and most of the published books may not contain updated information, no reference to books have been provided. In the changing world of technology, the value of judicial precedence is also low. Every judicial decision has to be seen with the law and technology as applicable to a case on*

*hand and hence excessive reliance on case laws in areas of E Commerce is better avoided. Hence it is recommended that students develop an insight into the legal interpretation from out of the current developments they may observe on the resources available on the Internet after due filtration for the credibility of the information.*

# Chapter III: E-Banking and Legal Issues

**Syllabus:** Electronic Money, Regulating e-transactions, Role of RBI and Legal issues Transnational Transactions of E-Cash Credit Card and Internet Laws relating to Internet credit cards Secure Electronic Transactions

**Learning Objectives:** In this chapter, students will learn about the concept of E Banking, Different types of Digital Banking, the legal definition**,** Laws applicable for Internet Banking in India, RBI guidelines, Frauds in E Banking scenario etc.

## E Banking and Electronic Money (E-Money)

E Banking is seen in different forms. The most visible form of E banking is in the form of Internet Banking and Mobile Banking. But one of the earliest mode of E Banking may be the ATM banking itself. In the current generation, we have new age systems like the BHIM, UPI, PayTM wallet, GPay, Hashtag banking through twitter, USSD, Voice response USSD banking etc.

However the legal definition of Banking has to be drawn from the definition of banking itself. Banking is defined under Law and Banks are institutions that are engaged in the business of Banking.

We have already discussed that the Cyber law in India is focused on defining the law in terms of use of "Electronic Documents" and not necessarily on the basis of devices which we may call Computers or Laptops or Mobiles. In other words, E Banking is better defined not as Banking done through Internet or use of computers or use of ATMs etc. It is better defined as Banking conducted with the use of Electronic Documents.

The legal definition of "Banking" in India is contained under Section 5(b) of the Banking Regulations Act 1949 (BR Act) which states as follows.

> *"Banking" means the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawable by cheque,d raft, order or otherwise.*

Extending the definition, a "Banking Company" is any company which transacts the business of banking [Section 5(c) of BR Act] and does not include a Company engaged in the manufacture of Goods or Carries on any trade and which accepts deposits of money from the public merely for the purpose of financing its business as such manufacturer or trader.

Under Section 7 of BR Act, the term "Bank" is permitted to be used only by Companies involved in the business of Banking as defined in the BR Act and not otherwise.
Over a period of time, the Banks developed several ancillary businesses including say issue of Demand Drafts and Money transfer instruments, Foreign Exchange, Services related to collection, acceptance, discounting of Bills of Exchange, Issue of Letters of Guarantee or Letters of Credit, safe deposit lockers, Issue of Travellers Cheques, Security custody etc. These were all considered "Ancillary" services and not "Banking Services".

Banks entered the era of Digital Banking first by use of computers in the back office operations such as account reconciliation, later with the use of ATMs and finally the Internet Banking. By the time ITA 2000 was enacted, Banks in India had already started limited use of Computers for accounting and were even issuing statements of account as computer print outs with the note "This is a computer generated document and does not require signature", (Which practice continues wrongly even after the ITA 2000 coming into existence. The first Internet Banking service of ICICI Bank was already available before 17th October 2000 when ITA 2000 was notified. In the last few years after the advent of Mobile Banking, Concept of Wallets etc, the money in the Bank was slowly getting perceived as "Digital Money". Bank also came to be perceived as an organization that was handling Digital Money or E Money.

This gave rise to an erroneous perception in certain circles that E Banking means dealing with E Money. This is an incorrect perception and has to be dispensed with.

E-Banking can only be interpreted as "Banking" conducted with "Electronic Documents" and nothing else.

As regards money in the Bank accounts, they retain their earlier character, whatever it was before the advent of E-Banking.

The classic definition of the Banker-Customer relationship is that of a "Debtor-Creditor" relationship. When a customer deposits money, he is lending his savings to the bank and therefore

in the books of the Bank he is a “Creditor”. When he takes a loan from the Bank, he is a “Debtor” in the books of the Bank.

The money deposited in the bank becomes money owned by the Bank and it can lend it to any person of his choice. The money once it passes into the hands of the banker, becomes fungible with its own cash and the depositor has no right except to demand repayment as per the terms of deposit.

This specific characteristic of “Banking” remains true even in the E Banking era.

What we normally call as “Balance in the account” which appears in the Internet Banking page or shows up on the Banking app, is not “E-Money”. It is only an account of “Outstanding loan given by the customer to the bank”.

The money in PayTM or PhonePeetc are also “Digital account of money kept for a specific purpose” and not “E-Money”.

The term E-Money is perhaps applicable only in the case of “Crypto Currencies” such as “Bitcoin”.
A Crypto currency like “Bitcoin” is “Mined” through a digital process and just gets created on the computer based on a successful completion of a digital exercise. For example, in a Bitcoin Mining activity, a ledger of all Bitcoin transactions is maintained in a distributed ledger accessible to many. When new transactions are reported, all those who are interested in playing the “mining game” (The activity whose successful completion is rewarded with issue of new Bitcoins), try to add the new set of transactions to the existing ledger and create an extended ledger. They then try to calculate the hash value of the ledger after adding a variable (Nonce value) of their choice. The objective of the game is to try different variable nonce values to be added to the Block Chain (Previous Block plus the now added transactions) one by one so that the resulting hash value is lower than the minimum set by the algorithm. Whoever succeeds is credited with some bitcoins by the algorithm and he becomes the owner of this “Created E-Money”.

Bitcoin or other similar Crypto coins (More than 1000 such systems exist in the world) therefore have an existence distinct from the physical currency that a person may have in the form of Rupees or Dollars etc., which is either held in Cash form or in the form of deposits with Banks.

The balances of depositors that we normally come across in Digital Banking is a “Digital Representation” of Physical money. When we go to a Bank branch and remit Rs 1 lakh in cash,

then this “Money” in circulation is absorbed in the Bank and reflects as an additional account balance in the Internet Banking account. This is different from the Bitcoin scenario where the E-Money is “Created” out of a process. When the balance in the Bank account is liquidated by the depositor making say, an NEFT transfer to another person, then the money moves from one Bank account to another without increasing the “Physical Currency” in circulation.
In all our future discussions, if we use the term “E-Money”, it may be a reference to the “Digital Account Balance” and not the “Crypto Currency”. Presently there is no legal definition of E-Money. The nomenclature of E-Money gained popularity with the use of “Wallets”. “Wallets” initially started as “hardware devices” like the Prepaid cards of today. Now there are “Software Wallets” like the “Mobile Wallets”. In this avatar, E Money is the “Stored Monetary Value” on a hardware or software device.

In India, RBI regulates the banking system in general. By extension of its powers, RBI also regulates transactions of digital money in the form of Prepaid Cards or mobile wallets or any variation there of. For the purpose of such regulations, a separate law called Payment and Settlement Systems Act was enacted in 2007.

The Credit Cards are also often called “Plastic Money” because it enables the holder to spend money using the card. But the nature of “Credit Card” is different from the “Prepaid Instruments” as well as “Debit Cards”. A Credit Card represents an ID of the customer to whom a “Credit Limit” has been granted by the Card Issuing bank.

On the other hand, “Debit Card” is an ID of the customer which allows him to withdraw money from his account through the merchant outlets so that the money can be applied for payment of expenses or for drawing cash through an ATM. Prepaid Cards are instruments that may have money ear marked for the card and used for expenses in merchant outlets. These Prepaid Cards may have an identity of the owner of the funds in some cases and in some cases may be issued like a bearer instrument.
In comparison, each debit on a Credit Card is like a new request for loan which is approved by the Card issuing Bank like every debit in an overdraft account.

The legal aspects of transactions involving Credit Cards in which the Card owner, the Card issuing bank, the Merchant and the Acquiring Bank are parties to a contract, is determined by the contract under which the Card is issued to an applicant of the Card.
The legal aspects of Debit Card transactions however may be determined by the Account opening contract itself where use of ATM and the Debit Card may be the channels through which money can be withdrawn in addition to cheques.

The Payment and Settlement Act may determine the Inter Bank regulations in this regard at least to the extent of transactions between the Banking entities. The consumer related aspects may have to be determined more in tune with the general Banking law that determines the Banker-Customer relationship, the Consumer protection law etc. These are part of the RBI regulations. More about the RBI regulations of Prepaid Cards is discussed later.

## Regulation of Crypto Currencies

There has been an ongoing discussion in India about the regulation of Bitcoins. Bitcoin is an electronic document. However, in practical usage, Bitcoin is perceived as and promoted as "Currency" in substitution of physical currency.

There is one school of thought that demands that Bitcoin has to be allowed to be used without any Government regulation. At the same time they also expect that trade circles should recognize it as a currency and use it for E Commerce transactions.

Some of the countries in the world have officially recognized Bitcoin as a currency and allowed its free conversion to legacy currency. As a result any holding of Bitcoin can be converted into a legacy currency and brought into the circulation like any physical currency. Also there are more than 1000 different Crypto Currencies and Bitcoin is fungible with any of these currencies. Hence Bitcoin is part of a family of instruments that can be considered as a replacement of physical currency.

Since Crypto currencies are basically not within the regulation of the Central banks and its ownership is confidential, Crypto Currencies are like "Digital Black Money"[xxvi] and it creates a parallel economy.

The total market capitalization of Bitcoins is around $124 billion out of over $211 billion of all crypto currencies put together. This is equivalent to around 13,30,300 crores. As against this, the total rupee currency in circulation with the public is of the order of Rs 20,52,000. If Bitcoin is recognized as an official tender, then the money circulation in India would nearly double up, inflation is expected to reach 50% plus per annum and create havoc to the economy. Besides the Digital Black money would be usable by criminals and terrorists to fund illegal activities and there is an expectation that criminal activities will raise.

Hence there is another school of thought that Bitcoins and the Private Crypto Currencies should be banned.

If however, a Crypto Currency is issued by the Central bank of a country under its "Currency issuing capacity" as defined by the accepted international monetary principles and backed by appropriate securities, such Government backed Crypto Currencies would be part of the physical currency stock and would not adversely affect the economy. Their effect would be similar to "Printing of Notes" and increasing the physical cash in circulation. This can be monitored and regulated like the physical currency regulation.

However, Crypto Currencies are prone to frauds of all kinds and the public as well as the Central bank should be aware of the risks before any such decision is taken. The block chain algorithm that has to manage such a Government backed Crypto Currency needs to be creatively structured to ensure that the Central bank does not lose track of Crypto Currencies officially issued and prevent any fake Crypto Currencies coming into circulation.

Crypto currency regulation falls in between RBI and SEBI. If Bitcoin is considered as an "Electronic Document" as recognized under ITA 2000, and it is bought and sold for value, it appears like a "Commodity Trade" and its regulation falls under SEBI. If however, as per the perceived popular belief, Bitcoin is "Currency" then it should come under regulation of RBI since according to RBI Act, RBI alone has the power to issue currency.

Regulation of Crypto Currency needs to be distinguished from Regulation of Digital money (Balance in banks withdrawable through digital means) or Regulation of e-Transactions of non financial nature (E-commerce). The challenges in Crypto Currency regulation is different and complicated.
At present Supreme Court is considering a petition about legalization of Bitcoins and it has sought the opinion of the RBI and the Government. Government has formed an expert committee to frame guidelines.

Despite the Government of India having strong views on prevention of black money in India, having resorted to measures like demonetization of high value currencies in the recent past, there is a strong lobby in support of Bitcoins in India and hence there has been a delay in taking a decision on whether Bitcoin should be banned or regulated strictly or recognized as legal tender.

The author is one of the strong advocates for not only banning of Bitcoins but also imposing strong penalties for its usage.

A decision in this regard from the Government is expected to be announced some time in 2019.

## Transnational Transactions of E-Cash

As long as we consider E-Cash as balance of money held by citizens in the legacy Banking systems which can be operated through Internet, Mobile or other digital devices and means, Transnational transactions are nothing different from normal foreign exchange transactions.

Currently RBI has FEMA (Foreign Exchange Management Act) that regulates the foreign exchange and the same will be applicable to the E-Cash transactions as well. In other words the "Authorized Dealers of Foreign Exchange" maintaining the Foreign Currency accounts with foreign banks will act as the conduits for conversion of Indian currency to foreign currency and vice versa. The Sale and purchase of Foreign Exchange is regulated based on the purpose of its use and the foreign exchange rates of conversion is determined by international monetary considerations and regulated by RBI. The Import and Export of commodities involving exchange of Rupee to a foreign currency and vice versa is regulated by appropriate policies applicable for such trade.

As regards Crypto Currencies, the holding of Crypto Currencies such as Bitcoins by individuals is through "Bitcoin Wallets". The wallet is like an account much like getting a new gmail identity. The wallets are registered through anonymous information supplied by the registrant and are identified by a "Private Key".

The holder can access the wallet which is encrypted with his public key by using his private key. The key pair is not issued by any "Licensed Certifying Authority" like the digital signature certificates issued by companies in India registered with Controller of Certifying Authorities. It is issued by the Bitcoin wallet issuer.

The encryption algorithm used is as strong as or better than what is used by the digital signature certificate issuing authorities, but it is purely a technology issue and is not governed by any regulations. The wallet will contain information such as a distinct ID and the balance of holding of the crypto currency along with its transactions. The entire information is encrypted with the public key of a key pair, the private key of which forms the Wallet ID used by the user confidentially to access the information. There could be some variations of this implementation and even hardware storage devices may be used to hold a bitcoin wallet.

Issue of a new wallet has to be done through the internet and may have to use an e-mail ID also. Hence the wallet may be technically traceable to the e-mail ID and IP address used at the time of

its registration. However if the Wallet Company deletes the meta data after creation of the ID or the user uses other means of hiding his identity, then it becomes impossible to trace the wallet owner's physical identity. The only other way of identification is to analyze different transactions linked to the same wallet ID. If however the user is intelligent and does not use the same ID for multiple transactions, it becomes difficult to trace him.

Since such Bitcoin wallets can be opened on any Internet Service provider, the bitcoin holdings seamlessly move across physical borders just like how our e-mails move across. Hence the question of regulating "Trans national" transactions lose meaning in the context of Crypto Currencies.

The actual Crypto Currency transactions are handled by "Crypto Currency Exchanges" which work like our stock markets buying and selling different crypto currencies against legacy money transfers. Such transactions can be traced to the bank accounts from which money can be transferred.

Exchanges being visible business entities are often under regulatory radar but they often operate from countries where the regulation is friendly. Off late, India RBI mandated that no Banking support should be given to such exchanges. It also mandated that the exchanges should adopt accepted KYC norms to identify their clients. Hence many of the exchanges closed their business in India and moved to other countries including Singapore.

These exchanges however deal with transfers of crypto currencies in and out of wallets and hence cater to trans-national transactions without meaningful regulation.

In the context of Crypto Currencies therefore, the very nature of the Crytpto Currency, the manner of their administration, trading, storing etc., makes it completely immune to regulations.

The only regulation that can be applied is to the "Business Entity Registrations", "Banking Transactions of these Exchanges", physical "hosting of servers" and physical location of "Administrative offices". Transactions however are not amenable for proper tracing and hence if the entities are legalized, then they will be allowed to conduct transactions with legal sanction but not be able to help the regulatory agencies significantly in making the trans-national transactions as accountable as regulatory agencies would be comfortable with.

## Virtual banking

In countries like USA, the concept of "Virtual banking" came out even before Internet Banking. The difference between "Virtual banking" and what we know as "Internet Banking" is that Internet banking is Banking by legacy Banking institutions using Internet as a medium of communication. Virtual Banking on the other hand is banking transaction (accepting deposits and lending) without the presence of physical banking infrastructure. In India since Banking is regulated by licensing, "Virtual banking" was not adopted and RBI straightway went for Internet Banking stating that only Banks with a Banking license can conduct Internet Banking business.

There are many Internet Based games in which certain "Loyalty Points" or "Currencies to be used during the game" are generated and used. Some of these points may be purchased by legacy currency. In certain cases, the game owners may allow the balances to be withdrawn in the legacy currency or transferred to another person. Normally such transactions take place between a member of the game site and the game site owner and/or different members of the game site. They are like the "Chips" used in a Casino where Chip stock is purchased on entry, spent in the casino, earned in the games and later exchanged back to legacy currency. One example of such currency is "Linden" used by secondlife.com.
Such "Game Currencies" if sufficiently popular, may have a nature of currency just like the crypto currency like Bitcoin. But they are not regulated by the Central Banks of countries and hence have their own limited legal validity. Such Game entities actually provide a Banking function where by a person may park his legacy cash, use it for limited purpose and take them back later. Some of the game entities provide easy conversion to Bitcoins also. Such transactions are capable of being used or are being used for money laundering purpose.

Virtual Banking however is a term which should be used only for those organizations which are regulated by the Central Banks but not have physical outlets. Such organizations are however not permitted in India since Internet Banking can be done only by the licensed Bankers. Even the "Cash Cards" or "Food coupons" operated by non Banking organizations are regulated by RBI under its Prepaid Card regulations.

## Internet Banking Regulations

Banking being regulated by RBI under the BR Act 1949, regulation of Internet Banking also comes directly under the RBI's powers.

Immediately after ITA 2000 was enacted with effect from October 17, 2000, RBI constituted an expert group on Internet Banking under the chairmanship of Mr S.R.Mittal. The S.R.Mittal group recommendations which were notified by RBI on 14th June 2001[xxvii]. The copy of the report published as S R Mittal Group based on which the notification was issued was also published by RBI[xxviii]. Thi is the fundamental document that describes the RBI policy on Internet Banking.

When the ITA 2000 was amended in 2008, RBI again constituted another working group under the Chairmanship of Mr G Gopalakrishna which gave its report in January 2011. The recommendations in a slightly modified form were adopted by RBI on April 2011. [xxix]. This report is a comprehensive report on E banking Security and Cyber Frauds.

Additionally, RBI has issues annual guidelines on Frauds which includes Cyber Frauds.
On June 2, 2016, RBI issued another comprehensive guideline on Security of E Banking transactions through what was called the "Cyber Security Framework" (CSF). On 2017, RBI issued the "Limited Liability Circular" which brought in several significant regulatory guidelines that affect E banking. In between there have been the committees like the Damodaran Committee and the Banking Ombudsman guidelines which also have provided its own guidelines.

Non-Banking Finance Companies (NBFCs) which are licensed separately have been regulated under similar guidelines on security.
RBI has also provided separate licenses for "Payment Banks" which are not full fledged Banks but may be allowed to accept Deposits and pay interest to the depositors with the money available for expenditure but not for lending.

E Banking Regulations in India therefore is a compendium of many regulations and a gist of these regulations are discussed below.

## Internet banking Guidelines 2001

The Internet Banking Guidelines 2001 was issued through a circular dated June 14, 2001. This circular made a specific reference to the detailed report of the S.R.Mittal Working group which was also published by RBI in full on 22nd June 2001. (Refer links provided at the end of the lesson).

The guidelines highlighted three specific parts of the report namely the Technology and Security Standards, the Legal Issues and the Regulatory and Supervisory issues.

Under the legal issues it was specifically mentioned as follows. (P.S:Para numbers mentioned here refer to the para in the S.R.Mittal group detailed report):

**Legal Issues**

a. Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer. (Para 7.2.1)

b. From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk. (Para 7.3.1)

c. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers‘ accounts. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risks. (Para 7.5.1-7.5.4)

d. In Internet banking scenario there is very little scope for the banks to act on stop-payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted. (Para 7.6.1)

e. The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks’ liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks. (Para 7.11.1)

The point (a) was later modified through a circular dated December 10, 2012, according to which "Introduction" is not necessary for opening of accounts but KYC as per the norms specified is mandatory as part of the Anti Money Laundering regulations. Since Aadhaar was available as a KYC instrument, it is now possible for the process of KYC to be completed online. Many Banks are aggressively promoting accounts opened online with a "Single Click". In the process there have also been many frauds where the Aadhaar based KYC was misused with fraudsters stealing the aadhaar data and some times also collecting OTP for use of Aadhaar for opening accounts through either "Vishing" (impersonated phone call to get the OTP) or "Virus injection into mobiles".

The guideline clearly recognized that "Digital Signature" should be used as a form of authentication in replacement of physical signatures and also suggested that Cyber Insurance is mandatory for Bankers.

On the technology front, the guidelines specified that adequate security policy should be implemented, PKI is the most favoured technology for authentication etc. These security measures have been further elaborated in the GGWG guidelines and the CSF in subsequent years.
The circular further clarified

"The Reserve Bank of India have decided that the Group's recommendations as detailed in this circulars should be adopted by all banks offering Internet banking services, with immediate effect. Even though the recommendations have been made in the context of Internet banking, these are applicable, in general, to all forms of electronic banking and banks offering any form of electronic banking should adopt the same to the extent relevant."

## GGWG Recommendations

The GGWG (Gopala Krishna Working Group) which was officially called "Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds" was constituted after the ITA 2000 was amended in 2008 to revise the earlier guidelines contained in the Internet Banking guidelines of 2001.

The first version of the report was released in January 2011 and contained some significant changes to the legal aspects as recommended in the Internet Guidelines of 2001. The author however ran a high level campaign to oppose some of the proposed changes as documented at Naavi.org[xxx]. Consequently, a new version of the report was released as the final report in April 29 2011[xxxi] in which Chapter 9 on Legal issues was significantly modified.

In the first version, attempt had been made to suggest that the Two Factor Authentication by OTP using a mobile should be considered as equivalent to "Digital/Electronic Signatures" for authentication. This was rejected and the report retained the earlier recommendations of the Internet Banking guidelines.

The final version which was approved by RBI and notified o 29th April 2011 contained a chapter on Legal Issues which contained the following:

The Information Technology Act, 2000 (IT Act, 2000) was enacted to handle certain issues relating to Information Technology. The IT Amendment Act, 2008 has made further modifications to address more issues such as cyber crimes. It is critical that impact of cyber laws is taken into consideration by banks to obviate any risk arising there from.

The legal function within the bank needs to advise the business groups on the legal issues arising out of use of Information Technology with respect to the legal risk identified and referred to it by the Operational Risk Group.

The IT Act, 2000 as amended, exposes the banks to both civil and criminal liability. The civil liability could consist of exposure to pay damages by way of compensation upto 5 crore under the amended Information Technology Act before the Adjudicating Officer and beyond five crore in a court of competent jurisdiction. There could also be exposure to criminal liability to the top management of the banks given the provisions of Chapter XI of the amended IT Act and the exposure to criminal liability could consist of imprisonment for a term which could extend from three years to life imprisonment as also fine. Further, various computer related offences are enumerated in the aforesaid provisions.

Legal risks need to be incorporated as part of operational risks and the position need to be periodically communicated to the top management and Board/Risk Management Committee of the Board.

As the law on data protection and privacy, in the Indian context are in an evolving stage, banks have to keep in view the specific provisions of IT Act, 2000 (as amended in 2008), various judicial and quasi judicial pronouncements and related developments in the Cyber laws in India as part of legal risk mitigation measures. Banks are also required to keep abreast of latest developments in the IT Act, 2000 and the rules, regulations, notifications and orders issued there under pertaining to bank transactions and emerging legal standards on digital signature, electronic signature, data protection, cheque truncation, electronic fund transfer etc. as part of overall operational risk management process.

It can therefore be observed that the GGWG committee has recognized the need for compliance of ITA 2000/8 by Banks. A specific reference was also made to the decision of the Adjudicator of Tamil Nadu, in the case of S.UmashankarVs ICICI Bank, in which the adjudicator held the Bank liable to repay loss suffered by the customer on account of Phishing.

> (P.S:This decision later went on appeal and recently on 3rd April 2019, TDSAT disposed off the appeal upholding the Adjudicator's decision subject to some adjustments regarding the compensation that had been granted on account of out of pocket expenses incurred by the complainant that had been asked to be refunded.[xxxii])

## Extension of the Internet Banking Guidelines

The Internet banking guidelines as well as the security prescriptions first implemented for scheduled Banks have since been extended to Cooperative Banks as well as Regional Rural Banks subject to consequential adjustments. Hence all the guidelines mentioned above may be considered applicable to Cooperative Banks and Regional Rural Banks.

Most of the larger Cooperative Banks who provide Internet Banking services maintain their own Core Banking systems. Some of the smaller Banks may not be providing internet Banking facilities for their customers.

In certain cases, smaller Banks operate their own Banking requirements for clearing and other inter banking requirements through current accounts opened with larger Banks. These larger Banks may treat the cooperative Banks as their customers.
In certain cases, the larger banks may offer Core Banking services for the smaller Banks as a "Value Added Service". Such operations are conducted through contractual bindings which may determine the inter-se liabilities for functional as well as fraud situations.

One such service is being operated by NABARD. More than 200 State and District level Cooperative Banks with nearly 7000 branches from over 20 different states and union Territories are on this CBS platform.

## Digital Banking Ecosystem in India

One of the important segments of Internet Banking is the system for transfer of funds between Banks. The main interbank fund transfer between Indian Banks happen through their respective RBI accounts.

International fund transfers are done between Banks in India and their agency Banks abroad through the SWIFT (Society for Worldwide Interbank Financial Telecommunications.) SWIFT is essentially a messaging network that financial institutions use to securely transmit information and instructions through a standardized system of codes.

SWIFT is also used for transfer of funds at the instruction of the customers of the bank.
Within India, Customers are allowed funds transfer through the Internet banking system essentially through Electronic Payment products namely NEFT, RTGS and IMPS,, besides NECS and ECS variants. Customers are also provided different services such as Cards, Wallets, Prepaid Instruments, UPI systems as well as Banking through Twitter, Face Book etc. Private companies have also introduced services of their own such as GPay, WhatsApp Pay, Amazon Pay etc by linking with the UPI system.

We can briefly understand these different Electronic Payment Products to get a hang of the Digital banking eco system that is presently prevalent in India.

The Payment and Settlement Act 2007 (PSSA) legislated in 2007 and the Payment and Settlement Regulations 2008 (PSSR) effective from August 12, 2008, regulate the entire system of Prepaid Payment Instruments, Card Schemes, Cross Border Money Transfers, ATM networks and Central Clearing arrangements.

## Paper Based Payments

Despite the popularity gained by the digital systems, use of paper-based instruments (like cheques, drafts) still constitute for nearly 60% of the volume of total non-cash transactions in the country. In value terms, the share is however lower and is presently around 11%.

One of the first digitization efforts that RBI introduced in the Banking system was the introduction of Magnetic Ink Character Recognition (MICR) technology for speeding up and bringing in efficiency in processing of cheques. Though the use of cheques is on the wane the system of Cheques may co-exist with the electronic systems for some time to come

Towards achieving its objective of increasing the share of digital transactions, Banks have been dis-incentivising the use of paper based instruments. Initially this was done by incentivising the digital systems but gradually RBI appears to be favouring penalization of the use of paper as an additional measure to reduce the use of paper based instruments.

However, the policies of RBI regarding dis-incentivising the use of paper based payment system introduces its own conflicts with the banking law[xxxiii]. It is necessary for RBI to proceed with caution before taking steps which disturb the fundamental legal status of Banking as an industry.

## Electronic Payments

The initiatives to introduce and popularise the use of electronic means of payment started with the ECS (Electronic Clearing Service) where the customers could initiate push and pull transactions by standing instructions placed with the banks. These were meant to handle bulk and repetitive payment requirements (like salary, interest, dividend payments) of corporates and other institutions.

In September 2008, RBI launched National Electronic Clearing Service (NECS), at National Clearing Cell (NCC), Mumbai. NECS (Credit) facilitated multiple credits to beneficiary accounts with destination branches across the country against a single debit of the account of the sponsor bank. The system has a pan-India characteristic and leverages on Core Banking Solutions (CBS) of member banks, facilitating all CBS bank branches to participate in the system, irrespective of their location across the country.

After NECS, RECS (Regional Electronic Clearing Service) has been launched during the year 2009. RECS, is confined to the bank branches within the jurisdiction of a Regional office of RBI. Under the system, the sponsor bank will upload the validated data through the Secured Web Server of RBI containing credit/debit instructions to the customers of CBS enabled bank branches spread across the Jurisdiction of the Regional office of RBI. The RECS centre will process the data, arrive at the settlement, generate destination bank wise data/reports and make available the data/reports through secured web-server to facilitate the destination bank branches to afford credit/debit to the accounts of beneficiaries by leveraging the CBS technology put in place by the bank. Presently RECS is available in Ahmedabad, Bengaluru, Chennai and Kolkata

## Electronic Clearing Service (ECS) Debit

The ECS (Debit) Scheme was introduced by RBI to provide a faster method of effecting periodic and repetitive collections of utility companies. ECS (Debit) facilitates consumers / subscribers of utility companies to make routine and repetitive payments by ‘mandating’ bank branches to debit their accounts and pass on the money to the companies. There is no limit as to the minimum or maximum amount of payment. This is also available across major cities in the country.

## National Electronic Funds Transfer (NEFT) System

In November 2005, a system was introduced for facilitating one-to-one funds transfer requirements of individuals / corporates. Available across a longer time window, the NEFT system provides for batch settlements at hourly intervals, thus enabling near real-time transfer of funds. Certain other unique features viz. accepting cash for originating transactions, initiating transfer requests without any minimum or maximum amount limitations, facilitating one-way transfers to Nepal, receiving confirmation of the date / time of credit to the account of the beneficiaries, etc., are available in the system.

## Real Time Gross Settlement (RTGS) System

RTGS is a funds transfer systems where transfer of money takes place from one bank to another on a "real time" and on "gross" basis. Settlement in "real time" means payment transaction is not subjected to any waiting period. "Gross settlement" means the transaction is settled on one to one basis without bunching or netting with any other transaction. Once processed, payments are final and irrevocable. This was introduced in in 2004 and settles all inter-bank payments and customer transactions above Rs 2 lakh.

## Pre-paid Payment Systems

Pre-paid instruments are payment instruments that facilitate purchase of goods and services against the value stored on these instruments. The value stored on such instruments represents the value paid for by the holders by cash, by debit to a bank account, or by credit card. The pre-paid payment instruments can be issued in the form of smart cards, magnetic stripe cards, internet accounts, internet wallets, mobile accounts, mobile wallets, paper vouchers, etc.

Subsequent to the notification of the PSS Act, policy guidelines for issuance and operation of prepaid instruments in India were issued in the public interest to regulate the issue of prepaid payment instruments in the country.

The use of pre-paid payment instruments for cross border transactions has not been permitted, except for the payment instruments approved under Foreign Exchange Management Act,1999 (FEMA).

Under the Master Directions for PPIs (MD-PPI), three types of PPIs are recognized namely

a) Closed System PPIs

b) Semi-Closed System PPIs

c) Open System PPIs

Closed System PPIs are those PPIs which are issued by an entity for facilitating the purchase of goods and services from that entity only and do not permit cash withdrawal. As these instruments cannot be used for payments or settlement for third party services, the issuance and operation of such instruments is not classified as payment systems requiring approval / authorisation by the RBI.

Semi-closed System PPIs are those PPIs which are used for purchase of goods and services, including financial services, remittance facilities, etc., at a group of clearly identified merchant locations / establishments which have a specific contract with the issuer (or contract through a payment aggregator / payment gateway) to accept the PPIs as payment instruments. These instruments do not permit cash withdrawal, irrespective of whether they are issued by banks or non-banks,

Open System PPIs are those PPIs which are issued only by banks and are used at any merchant for purchase of goods and services, including financial services, remittance facilities, etc. Banks issuing such PPIs shall also facilitate cash withdrawal at ATMs / Point of Sale (PoS) / Business Correspondents (BCs).

PPIs may be "Reloadable" or "Non Reloadable". Some PPIs may permit "Cross Border outward Transactions" and some may not. PPIs may also be issued against inward remittance to the beneficiaries under Money Transfer Service Scheme of RBI. Some PPIs may be denominated in Foreign Exchange also.

PPIs may be issued as cards, wallets, and any such form / instrument which can be used to access the
PPI and to use the amount therein.

PPIs may be issued under Co-Branding arrangements. If one of the Co Branding partners is a Bank and the other is a Non Bank, the Bank will be the PPI Issuer. If both are non Bank institutions, or both are Banks, then one of them shall be designated as the PPI issuer.

Paper based prepaid meal instruments were discontinued from December 31, 2017 and semi closed PPIs shall be issued for such purpose.

## The Regulations on PPIs

Most of the regulations in the Master Directions relate to Semi Closed PPIs.

According to the guidelines, PPIs upto a monthly usage limit of Rs 10000/- can be issued on the basis of self declaration of name and an ID along with OTP on a mobile. Essentially these are non_KYC compliant instruments.

Funds in these non KYC PPIs can be used only for purchase of goods and services and money cannot be transferred back either to Bank accounts or to other PPIs.

These PPIs need to be compulsorily converted into KYC type within 1 year. If KYC is not provided, no further credit would be allowed but the balance can be used.

The PPI issuers need to ensure that same category PPI is not issued against the same mobile number.
PPIs for transaction uptoRs 1 lakh are KYC compliant PPIs. Money can be transferred to own bank account or Back to source.

"Pre registered beneficiaries" can be allowed for these KYC PPIs and money can be transferred to them upto the limit of Rs 1 lakh per month.
Fund transfer limits in the case of non pre-registered beneficiaries is limited to Rs 10,000/- per month.

## Open PPI Systems

The "Open" systems are permitted only to be issued by Banks and with KYC. Here also there can be pre-registered beneficiaries and others and transfer to others is restricted to Rs 10000/- per month.
The only difference between the Pre-closed and open systems is that Funds transfer for Open PPIs shall also be permitted to other open system PPIs, debit cards and credit cards as per the limits such as Rs 10,000/- except to pre-registered beneficiaries.

## Gift and MTS PPIs

Other than the above three main categories of PPIs, specific PPIs such as Gift Instruments (Maximum value Rs 10,000/- without cash-out or refund or reloading).

But KYC would be required on a risk based approach if multiple Gift cards are required to be issued to one person.

PPIs can also be issued for Mass Transit Systems which may be Semi Closed PPIs usable only for the transit systems and allied merchants. They are re loadable with a maximum outstanding or Rs 3000/- at any point of time.

## The PPI Ecosystem

The Prepaid Instrument Eco System in India under the Payment and Settlements Act 2007 has licensed several "Payment System Operators" under the Act.

The list consists of Two Financial Market Infrastructure operators namely the Clearing Corporation of India Limited and the National Payments Corporation of India (NPCI), 5 Card payment networks including the Amex, Diners, VISA, Master, etc., 9 inbound Cross border Money Transfer Systems including Western Union etc.,6 ATM Networks.,55 Prepaid Instruments.,9 White Label ATM Operators, One Instant Money transfer system of Empays Payment Systems, Three Trade Receivables Discounting Systems and Eight Bharat Bill Payment Operating Units

The entities who have been issued "Payment Bank" licenses such as Airtel Payment Bank Ltd, India Post Payments Bank Ltd, Paytm Payments bank Ltd, and Fino Payments bank Ltd are other entities in the Digital payment domain.

Licensed Scheduled Banks are also in the digital payment system with their UPIs, Wallets, Virtual and Physical Prepaid Cards, Debit Cards, Credit Cards etc. (Refer article in livemint). It appears that out of the eleven provisional licenses issued for Payment Banks, others have not yet operationalized their licenses.

The October 11, 2017 master directions of RBI apply to the 55 Prepaid Instrument operators which includes Aircel, Amazon Pay, Mannapuram, Muthoot, Mobikwick, Oxigen,PhonePe, Jio money, Sodexo, m-Pesa,etc.

On March 9, 2017, the Ministry of Information Technology had issued certain draft guidelines constituting "Reasonable Security Practices" applicable to the e-PPI instrument issuers. It was called "Information Technology (Security of Prepaid Payment instruments Rules 2017-Draft.
Now the Master Direction of RBI of October 11, 2017 is a follow up of this and represent among others the "Reasonable Security Practice" to be followed by these e-PPI operators.

## Mobile Banking System

Mobile phones as a medium for providing banking services have been attaining increased importance. Reserve Bank brought out a set of operating guidelines on mobile banking for banks in October 2008, according to which only banks which are licensed and supervised in India and have a physical presence in India are permitted to offer mobile banking after obtaining necessary

permission from Reserve Bank. The guidelines focus on systems for security and inter-bank transfer arrangements through Reserve Bank's authorized systems. On the technology front the objective is to enable the development of inter-operable standards so as to facilitate funds transfer from one account to any other account in the same or any other bank on a real time basis irrespective of the mobile network a customer has subscribed to.

ATMs / Point of Sale (POS) Terminals / Online Transactions

ATMs were introduced in India even before ITA 2000 came into existence. Initially it was an add on service to the physical banking service to improve the accessibility to Cash withdrawal requirements. Presently it is developing into a paid service of its own and serious disincentives are being introduced to first reduce the foot falls in the banking premises and then the number of free transactions in ATM. In the process, ATMs have become a symbol of how technology is first introduced as a promised cost reduction and convenience feature and gradually become a more expensive replacement of manual services. ATMs are also a convenient tool for fraudsters to withdraw money with 24X7 convenience and across the country and are almost always used to commit frauds using debit cards, credit cards.
At the same time banks are expanding the services of ATM by introducing additional services including passing on small requests like cheque book request etc through the ATM.

ATM like devices are also slowly coming up for Cheque deposits, Passbook entries etc so that these “Techno Mechanical Devices” will keep replacing human interaction with Customers. Recently experiments are being conducted for introduction of robotic assistants at branches to take the elimination of personalized Banks to the next level.

RBI is also allowing Bank agents to use devices to enable cash payments across many merchant establishments by introducing POS terminals which are normally used for purchase of goods.
In order to reduce the risks in Card Not present transactions, RBI has also mandated the two factor authentication system involving generation of OTP through the mobile/email channels both for supporting Internet Banking as well as for other types of payments.

## Payment and Settlement Act

Payment and Settlement Act 2007(PSSA) was enacted on 20$^{th}$ December 2007. According to this act, “No Person other than RBI can operate a payment system except in accordance with an authorization”. A system was introduced for licensing of such operations. The Act also

determined the system by which netting of transactions and settlements could be arrived at. A system for resolving the disputes between the participants were also introduced.

According to PSSA, "payment system" means a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange. For the purposes of this clause, "payment system" includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations;

PSSA recognizes that it addresses the electronic payment systems similar to the paper based systems where the payment and settlement is addressed through the Negotiable Instruments Act 1881. (NI Act) and therefore addresses the conflicts as well.
NI Act itself was amended first in 2003 and thereafter in 2015 affecting the electronic transactions and E Banking. In the 2003 amendment, the concept of "Cheques in Electronic Form" and "Truncated Cheques" were introduced. "Truncated Cheques" addressed the operation of the clearing of paper cheques and did not affect the basic system of cheques as payment instruments. "Cheques in Electronic Form" could have made some changes but did not find traction in practice and remained only as a provision.

The NI Act amendment of 2015 effective from 15th June 2015, however redefined "Cheques in Electronic Form" and included an instrument that could fit in to the following description:
"a cheque in the electronic form" means a cheque drawn in electronic form by using any computer resource and signed in a secure system with digital signature (with or without biometrics signature) and asymmetric crypto system or with electronic signature, as the case may be.

As a result,

> "any instrument in writing in electronic form containing an unconditional order to a specified Banker directing the Bank to pay on demand a certain sum of money only to or to the order of a certain person or to the bearer of the instrument"

is a Cheque (in electronic form) as per NI Act.

In view of this, an Electronic Payment Instruction from the customer to his Banker through NEFT/RTGS/IMPS can be considered as a "Cheque". It will take some time for Cyber Jurisprudence to develop in this matter but the indications are that a class of "Virtual Negotiable Instrument" may be recognized in due course in the form of "Cheques in Electronic Form" and an equivalent "Structured instruction under EFT system".

This view is further supported by Section 25 of PSSA which defines "Dishonour of EFT" just like dishonour of cheques under NI Act.

It is worth reproducing Section 25 of PSSA in full which states as follows:

> **Section 25: Dishonour of electronic funds transfer for insufficiency, etc., of funds in the account**
>
> (1) Where an electronic funds transfer initiated by a person from an account maintained by him cannot be executed on the ground that the amount of money standing to the credit of that account is insufficient to honour the transfer instruction or that it exceeds the amount arranged to be paid from that account by an agreement made with a bank, such person shall be deemed to have committed an offence and shall, without prejudice to any other provisions of this Act, be punished with imprisonment for a term which may extend to two years, or with fine which may extend to twice the amount of the electronic funds transfer, or with both:
>
> Provided that nothing contained in this section shall apply unless—
>
> (a) the electronic funds transfer was initiated for payment of any amount of money to another person for the discharge, in whole or in part, of any debt or other liability;
>
> (b) the electronic funds transfer was initiated in accordance with the relevant procedural guidelines issued by the system provider;
>
> (c) the beneficiary makes a demand for the payment of the said amount of money by giving a notice in writing to the person initiating the electronic funds transfer within thirty days of the receipt of information by him from the bank concerned regarding the dishonour of the electronic funds transfer; and
>
> (d) the person initiating the electronic funds transfer fails to make the payment of the said money to the beneficiary within fifteen days of the receipt of the said notice.
>
> (2) It shall be presumed, unless the contrary is proved, that the electronic funds transfer was initiated for the discharge, in whole or in part, of any debt or other liability.
>
> (3) It shall not be a defence in a prosecution for an offence under sub-section (1) that the person, who initiated the electronic funds transfer through an instruction, authorisation, order or agreement, did not have reason to believe at the time of such instruction, authorisation, order or agreement that the credit of his account is insufficient to effect the electronic funds transfer.
>
> (4) The Court shall, in respect of every proceeding under this section, on production of a communication from the bank denoting the dishonour of electronic funds transfer,

presume the fact of dishonour of such electronic funds transfer, unless and until such fact is disproved.

(5) The provisions of Chapter XVII of the Negotiable 26 of 1881 Instruments Act, 1881 shall apply to the dishonour of electronic funds transfer to the extent the circumstances admit. Explanation — For the purposes of this section, "debt or other liability" means a legally enforceable debt or other liability, as the case may be.

The PSSA uses the term "Beneficiary" instead of the word "Payee or the holder in due course" in Section 138 since the EFT instruction cannot be "Endorsed". It is clear from the similarity of the words used in Section 25 of PSSA with Section 138 of NI Act that Electronic transactional instruction from the customer to the bank is legally considered equivalent to a "Cheque".
This should automatically consider that the Transferring Bank would be like a "Paying Bank" and the Transferee Bank would be like a "Collecting Bank". As a result it can be argued that the concept of Payment in due course under Section 10 of NI Act and Collecting Bank's responsibilities under Section 131 of NI Act are also relevant for EFT.

In the case of "Payment of a Cheque" the demand is made by a person who is in possession of a cheque. On the other hand EFT is a push transaction where the instrument reaches the collecting bank from the paying bank and he dons the hat of the beneficiary to record a demand and credit the amount to the account as per EFT.

Along with Section 138, Sections 139 to 142 of NI Act will also be applicable to the extent the circumstances admit.

This equivalence of NI Act provisions to the PSS Act provisions is a matter which requires debate and probably jurisprudence will evolve.

These thoughts were used when the arguments were placed in the historic S.UmashankarVs ICICI Bank adjudication/TDSAT proceedings by Naavi (author). However, the finer points of law as discussed here emerged after the NI Act amendment in 2015 and could not be judicially analysed in the Umashankar case.

## UPI System

In 2016, RBI introduced a new system of payment called the "Unified Payment Interface"(UPI) and implemented it through the National Payments Corporation of India (NPCI). After the introduction of the Two Factor Authentication including the OTP over a mobile network, most of

the Bank Customers had a "Registered Mobile Number" associated with a Bank account. The mandatory "SMS Alerts" for E Banking and Card transactions which RBI introduced also made it necessary for every customer of a bank to link a unique mobile number with the bank account.

With this infrastructure of mobile linking to every bank account, NPCI introduced the UPI system acting as an exchange house to clear the transactions between Banks. Under the UPI system, each bank could introduce an app and allocate an ID called "Virtual Payment Address" which was Bank specific. Using these IDs, customers could send and receive moneys using the specific virtual payment address.

Further a Universal App called the BHIM app (Bharat Interface for Money) was also introduced where an individual bank account of a customer could be linked to an UPI ID. This was a universal ID across Banks. NPCI again acted as an exchange house for such transactions by maintaining a mapping of BHIM ID to a given Bank account.

As a result of this system, an ID like X@SBI would be a unique ID for the account of Mr X at SBI. Whoever wanted to make a payment to Mr X could send it with BHIM ID X@SBI. Similarly using the BHIM App, X could send payment to other BHIM IDs.
Thus Indian E Banking system is having many innovative payment instruments that has made the dream of "Digital India" possible.

## Miscellaneous E Banking Systems

In recent days some Banks have introduced innovative Banking terms such as "Twitter banking", "Face Book Banking", "USSD Banking" etc.

Basically in these systems, different channels are used to send structured electronic messages to the banking server which will be executed by the server as an instruction received from the customer.
For example, different hashtags of Twitter message sent to a designated twitter ID of the bank may be interpreted as different instructions such as "What is my balance"? "Transfer Rs …. From my account to ….." etc. The destination ID may be designated in the form of a Twitter ID or Face Book ID etc. In such cases, the account numbers may be pre-registered to the social media ID and the conversion of the social media ID to the real account ID is done by the service provider.

Unlike the BHIM system, the mapping of the real Banking ID to the social media ID is done by a private sector service company and is prone to frauds and data breach risks of a higher order. In

view of the easy availability of BHIM and UPI systems, the necessity of such social media banking channels is questionable.

In USSD (Unstructured Supplementary Service Data) system, the message is sent through the mobile network instead of the Internet with different codes being assigned different instructions to be read by the bank. USSD code based passing of instructions can be also linked to a voice response system where the caller is instructed…."If you want to know the balance press 1. If you want to transfer money to another account, Press 2…..etc". In these instances the customer's manual action is converted into electronic instructions at multiple levels before it reaches the Bank's server for necessary action.

Similarly, most banking Apps running on a mobile provide the option to log in using h a four digit Pin or fingerprint instead of the log in ID and password as in the internet log in. In such cases also, the input received in one form is converted into a structured message and sent to the banking server.

Considering that the password system itself is not recognized in Indian law, these alternate systems are even less secure and going by the principle of the RBI's Internet Banking guideline of June 2001, the legal risk in case of frauds in such cases must be boarne by the Bank.

Since the access to the Bank is through a customer owned device and with the use of devices of intermediary service providers, the legal liabilities arising out of the transaction between the banker at one end and the customer at the other end becomes complicated. The question of "At whose request the intermediary was used"?. "Is it an agent of the bank? Or an agent of the Customer?" becomes relevant to determine the legal liabilities if some thing goes wrong. In such cases perhaps we may have to invoke the "Mail Box Rule" discussed earlier.

RBI has clarified that in its definition of "End Point Security" and the obligations of the banks, the intermediary electronic systems are also included as part of one single chain from the customer to the Bank. It is therefore reasonable to consider that except for the user's own computer and mobile, responsibility for every other device is that of the Banker.

In the BYOD (Bring your own device) scenario of corporates, there are measures that the companies adopt to ensure that irrespective of the user's control over the access device, the security of the back end system to which it connects within the corporate network is maintained by the use of appropriate log in protocols. It is therefore reasonable to expect that Banks should also be considered as responsible to ensure a proper VPN type connectivity with the use of appropriate log in protocols that irrespective of the user's control over their device and the

vulnerabilities such as virus etc affecting the user's device, the Bank may still be able to manage a "Reasonable level of security".

These are part of the discussion of what is the responsibility of Bankers under "Reasonable Security Practice" or "Due Diligence" as per section 43A of ITA 2000/8. The level of "reasonableness" in such circumstances is always a decision to be arrived at on a "Case to Case Basis" whenever a data breach or a cyber crime calls such due diligence into question in a court of law.

## Other Regulated Financial Bodies

Indian Financial system regulated by RBI has also defined other activities which have some similarities to Banking activities and tried to regulate them as has been explained earlier in the form of Prepaid card issuers. One such entity is "Non Banking Finance Companies". Other is "Payment Banks".

### NBFC

A Non-Banking Financial Company (NBFC) is a company registered under the Companies Act, 1956 engaged in the business of loans and advances, acquisition of shares/stocks/bonds/debentures/securities issued by Government or local authority or other marketable securities of a like nature, leasing, hire-purchase, insurance business, chit business but does not include any institution whose principal business is that of agriculture activity, industrial activity, purchase or sale of any goods (other than securities) or providing any services and sale/purchase/construction of immovable property.

A non-banking institution which is a company and has principal business of receiving deposits under any scheme or arrangement in one lump sum or in installments by way of contributions or in any other manner, is also a non-banking financial company (Residuary non-banking company).

Financial activity as principal business is when a company's financial assets constitute more than 50 per cent of the total assets and income from financial assets constitute more than 50 per cent of the gross income. A company which fulfils both these criteria will be registered as NBFC by RBI.

Though NBFCs lend and make investments there are a few differences with Banks such as

i. NBFC cannot accept demand deposits;

ii. NBFCs do not form part of the payment and settlement system and cannot issue cheques drawn on itself;

iii. deposit insurance facility of Deposit Insurance and Credit Guarantee Corporation is not available to depositors of NBFCs, unlike in case of banks

Housing Finance Companies, Merchant Banking Companies, Stock Exchanges, Companies engaged in the business of stock-broking/sub-broking, Venture Capital Fund Companies, Nidhi Companies, Insurance companies and Chit Fund Companies are NBFCs but they have been exempted from the requirement of registration under Section 45-IA of the RBI Act, 1934 subject to certain conditions.

Housing Finance Companies are regulated by National Housing Bank, Merchant Banker/Venture Capital Fund Company/stock-exchanges/stock brokers/sub-brokers are regulated by Securities and Exchange Board of India, and Insurance companies are regulated by Insurance Regulatory and Development Authority. Similarly, Chit Fund Companies are regulated by the respective State Governments and Nidhi Companies are regulated by Ministry of Corporate Affairs, Government of India. Companies that do financial business but are regulated by other regulators are given specific exemption by the Reserve Bank from its regulatory requirements for avoiding duality of regulation

## Payment Banks

Payments banks is a new model of banks conceptualised by the Reserve Bank of India (RBI). These banks can accept a restricted deposit, which is currently limited to □100,000 per customer and may be increased further. These banks cannot issue loans and credit cards. Both current account and savings accounts can be operated by such banks. Payments banks can issue services like ATM cards, debit cards, net-banking and mobile-banking.

The objectives of setting up of payments banks will be to further financial inclusion by providing (i) small savings accounts and (ii) payments/remittance services to migrant labour workforce, low income households, small businesses, other unorganised sector entities and other users.
The scope of activities of a Payment Bank are

1. Acceptance of demand deposits. Payments bank will initially be restricted to holding a maximum balance of Rs. 100,000 per individual customer.

2. Issuance of ATM/debit cards. Payments banks, however, cannot issue credit cards.

3. Payments and remittance services through various channels.

4. (Business Correspondent) BC of another bank, subject to the Reserve Bank guidelines on BCs.

5. Distribution of non-risk sharing simple financial products like mutual fund units and insurance products, etc.

The permitted Deployment of funds are

1. The payments bank cannot undertake lending activities.

2. Apart from amounts maintained as Cash Reserve Ratio (CRR) with the Reserve Bank on its outside demand and time liabilities, it will be required to invest minimum 75 per cent of its "demand deposit balances" in Statutory Liquidity Ratio(SLR) eligible Government securities/treasury bills with maturity up to one year and hold maximum 25 per cent in current and time/fixed deposits with other scheduled commercial banks for operational purposes and liquidity management.

## Fintech Companies

Fintech Companies are other categories of companies who provide services associated with finance such as Loan negotiation platforms such as MoneyTap, Early salary etc.

Broadly speaking, FinTech (financial technology) is anywhere technology is applied in financial services or used to help companies manage the financial aspects of their business, including new software and applications, processes and business models.

FinTech includes the new applications, processes, products, or business models in the financial services industry, composed of one or more complementary financial services and provided as an end-to-end process via the Internet. The main purpose of a Fintech company is integration of technology into offerings by financial services companies/Banks in order to improve their use and

delivery to consumers. It primarily works by unbundling offerings by such firms and creating new markets for them.

There is a thin line that divides these FinTech companies as being merely "Intermediaries" and NBFCs themselves. The regulation may differ according to the classification based on the service profile of each of these companies. In fact RBI may be interested in bringing "peer to peer lending services" promoted by a few Fintech companies under the NBFC regulations. We need to therefore carefully watch how regulations develop in this field.

## Regulatory Sandbox for Fintech companies

RBI has come out with an innovative concept called "Regulatory Sandbox" which is now being also tried by SEBI. Under these plans the companies who are regulated will be granted certain facilities and flexibilities to experiment with fintech solutions in a live environment and on real customers.

On 18th April 2019, RBI released a draft "Enabling Framework for Regulatory Sandbox", which indicates a very innovative approach by the regulator to keep pace with the innovators in the technology arena.

In July 2016, RBI had set up an inter-regulatory working group (WG) to report on the Fintech industry regulation. The report had been released for public comments in February 2018 and recommendations were taken note of. One of the key recommendations of the WG was to introduce an appropriate framework for a regulatory sandbox (RS) within a well-defined space and duration where the financial sector regulator will provide the requisite regulatory guidance, so as to increase efficiency, manage risks and create new opportunities for consumers. The Regulatory framework released as a draft on April 18 was a follow up of this initiative.

A regulatory sandbox (RS) usually refers to live testing of new products or services in a controlled/test regulatory environment for which regulators may (or may not) permit certain regulatory relaxations for the limited purpose of the testing. The RS allows the regulator, the innovators, the financial service providers (as potential deployers of the technology) and the customers (as final users) to conduct field tests to collect evidence on the benefits and risks of new financial innovations, while carefully monitoring and containing their risks. It can provide a structured avenue for the regulator to engage with the ecosystem and to develop innovation-enabling or innovation-responsive regulations that facilitate delivery of relevant, low-cost financial products. The RS is potentially an important tool which enables more dynamic,

evidence-based regulatory environments which learn from, and evolve with, emerging technologies.

The RS provides an environment to innovative technology-led entities for limited-scale testing of a new product or service that may or may not involve some relaxation in a regulatory requirement before a wider-scale launch.

The RS is, at its core, a formal regulatory programme for market participants to test new products, services or business models with customers in a live environment, subject to certain safeguards and oversight.

The proposed financial service to be launched under the RS should include new or emerging technology, or use of existing technology in an innovative way and should address a problem, or bring benefits to consumers.

The setting up of an RS can bring several benefits, some of which are significant and are delineated below:

First and foremost, the RS fosters 'learning by doing' on all sides. Regulators obtain first-hand empirical evidence on the benefits and risks of emerging technologies and their implications, enabling them to take a considered view on the regulatory changes or new regulations that may be needed to support useful innovation, while containing the attendant risks. Incumbent financial service providers, including banks, also improve their understanding of how new financial technologies might work, which helps them to appropriately integrate such new technologies with their business plans. Innovators and FinTech companies can improve their understanding of regulations that govern their offerings and shape their products accordingly. Finally, feedback from customers, as end users, educates both the regulator and the innovator as to what costs and benefits might accrue to customers from these innovations.

Second, users of an RS can test the product's viability without the need for a larger and more expensive roll-out. If the product appears to have the potential to be successful, the product might then be authorized and brought to the broader market more quickly. If any concerns arise, during the sandbox period, appropriate modifications can be made before the product is launched in the broader market.

Third, FinTechs provide solutions that can further financial inclusion in a significant way. The RS can go a long way in not only improving the pace of innovation and technology absorption but

also in financial inclusion and in improving financial reach. Areas that can potentially get a thrust from the RS include microfinance, innovative small savings and micro-insurance products, remittances, mobile banking and other digital payments.

Fourth, by providing a structured and institutionalized environment for evidence-based regulatory decision-making, the dependence of the regulator on industry/stakeholder consultations only is correspondingly reduced.

Fifth, the RS could lead to better outcomes for consumers through an increased range of products and services, reduced costs and improved access to financial services.

This approach of RBI indicates the flexibility that the regulatory is willing to bring in so that innovation in Fintech is not curbed.

There will be a criterial for participation in this program and responsibilities that the participants need to fulfil. The outcome of the approach and whether the industry will take advantage of the system needs to be watched.

## Payments and Settlements in India Vision 2019-2021

The Reserve Bank of India on 15th May 2019, released a document titled "Payment and Settlements in India Vison 2019-2021" outlining the road map for the Digital Payment industry for the next three years. The document recognized the positive outcomes of the developments in the immediate past and also pointed out the new challenges that have arisen now.

The core theme of the vision is to empower every Indian with access to a bouquet of e-payment options that is safe, secure, convenient, quick and affordable. Towards this objective, while the pursuit towards a 'less cash' society continues, accompanied by the ambition to have a less-card India as well, the endeavour is to also ensure increased efficiency, uninterrupted availability of safe, secure, accessible and affordable payment systems as also to serve segments of the population which are hitherto untouched by the payment systems.

The decade to follow is expected to witness a revolutionary shift in the way Indian citizens use digital payment options and will also empower them with an e-payment experience that will be exceptionally safe, secure and truly world class.

To achive this, the Vision envisages four goal-posts (4 Cs) – Competition, Cost, Convenience and Confidence.

We may therefore expect substantial changes in the policies to be adopted by the RBI to achive the objectives set in the vision document.

## E Banking Frauds

What we have discussed so far on how the E Banking system in India is structured and the regulatory framework that surrounds it is important for legal professionals in the context of E banking frauds that take place from time to time and a victim of the fraud tries to recover his loss through the judicial system.

The E Banking frauds are part of the discussion of Cyber Crimes in other lesson modules and what we discuss here is a brief description of E Banking frauds.

The E Banking frauds may be of two types. In the most common type, the loss would have been suffered by a customer of a Bank through some fraudster accessing his account and transferring the money to his own or his accomplices accounts through the normal fund transferring mechanisms such as NEFT/RTGS. In such cases the log in ID and Password of the customer could have been stolen through a social engineering attack or through the implanting of virus/Trojans in the customer's device. It is also possible that some insiders in the Bank may either directly access the account with their own credentials and commit a fraud or steal the credentials of the customer during a normal transaction. Those having the access to the systems may have innumerable ways of accessing the account fraudulently.

In such cases, money gets transferred from the victim's account to some other account which may be in the same Branch or another branch of the same bank or some other bank. In that bank, the account would have been opened with fake KYC documents by either the fraudster who transfers the money himself or his accomplices who work for a commission. The money may be transferred in the dead of the night and withdrawn through ATMs before the customer has time to recognize the fraud.

Most of the times the password compromise may happen because of a "Phishing" e-mail sent by the fraudster to which the customer may respond or at least open and allow a key logger virus to get automatically installed.

Where there is a need for 2FA (Two factor authentication) and the PIN from a mobile or e-mail is required, fraudsters either clone the SIM cards also or hack into the e-mail accounts or use social engineering methods of "Vishing" (Voice based Phishing).

There are also special malware some of which lurk in the computer of the customer and access the bank when a genuine session is established by the customer. They are called Coat tailing viruses and they enter the server when the customer is doing some normal transactions and place additional fund transfer instructions without the knowledge of the customer. Some viruses adopt the "Man in the Browser attack" where the instructions for a genuine fund transfer is diverted to a false account by manipulating the input form data after the customer hits the "Submit" button. Some viruses plant accomplice viruses in the mobiles when a mobile is connected to the computer and ensure that OTP (One time Password) sent through the mobile is compromised.

Some frauds may involve the cloning of Debit/Credit cards by stealing the card information at the usage points. The data may be used to place transactions for purchase of goods in e-commerce websites.

Where SIM card cloning or third party e-commerce sites are involved in the commission of the fraud, the Mobile service companies and the e-commerce companies become accomplices to the crime and may become legally liable.

Other than this customer related frauds, there may be a direct fraud on the Bank such as when an ATM is compromised and money withdrawn without being debited to any customer account, or money being transferred from the Bank's own account with RBI to anther account through SWIFT etc. In such cases the loss may be that of a Bank and no customer is involved.

When there is a loss to the customer, the customer has different options to recover his loss.
First option available is through the RBI's Ombudsman scheme. The second option is to approach the Consumer Forum and the third option is to approach the "Adjudicator" under ITA 2000. Additionally writ option to High Court may also be available.

The Banking Ombudsman is an officer of RBI and under the banking Ombudsman Scheme 2006 [xxxiv] (updated from time to time). He is authorized to resolve some of the customer's complaints mainly related to failure of the Bank to follow RBI instructions. This is not normally meant for resolving E Banking fraud cases which involve examination of evidences and evaluation of a crime. However in some cases, Banking Ombudsman have provided partial or full relief to the

victim customers where the loss can be identified to some direct failure of following RBI instructions.

The Banking ombudsman scheme is like a "Mediation" where the designated RBI official tries to bring a resolution between the customer and the bank. However, most of the times, the proceedings are handled more like a summary arbitration and award is dispensed with on the basis of documents submitted. This is not the recommended mode of recovery of money where the cause of action is a "Cyber Crime" involving contravention of an Act like ITA 2000.

The second option is to invoke the "Consumer Protection Act" and approach a Consumer forum where the cause of action is "Deficiency in Banking Service". This is also not the right forum for addressing a loss arising due to a Cyber Crime as in the case of E Banking frauds.

The correct forum for customers to redress their grievances arising out of E Banking frauds is the system of "Adjudication" under Section 46 of ITA 2000 where disputes for recovery of amount uptoRs 5 crore would be dealt with under an exclusive jurisdiction. The appeal for this lies with TDSAT (Telecom Disputes Settlement appellate Tribunal) which acts as the "Cyber Appellate Tribunal" under ITA 2000/8. Further appeals go back to the High Court and thereafter to the Supreme Court.
The Adjudication is handled by the Adjudicating officers who are the IT Secretaries of each State or Union Territory through an enquiry process. (Details of Adjudication process is out of scope of this module) and is expected to be customer friendly.

In an adjudication process, the complainant has to file a complaint when there is a contravention of ITA 2000/8 and a consequent wrongful loss that has occurred to him. The person who has made the wrongful gain and or the person who caused the wrongful loss will be liable to pay compensation to the victim.

The adjudicator has the powers of a civil court to conduct the adjudication but he is not bound by the Civil Procedure Code. He is expected to adopt his own process under the principle of natural justice and settle the disputes within 4 to 6 months.
A detailed procedure for Adjudication is available through the notification dated 17th March 2003[xxxv]
In the historic case of S.UmashankarVs ICICI Bank, where the customer had lost a sum of Rs 646,000/-, the adjudicator of Tamil Nadu granted compensation to be paid by the bank to the customer for the reason that the Bank was grossly negligent in following security norms.[xxxvi] The

judgement had been appealed by ICICI Bank in TDSAT and on 3rd April 2019, TDSAT upheld the Adjudication order [xxxvii].

This would be a model case of how "Negligence" by the Bank could constitute a reason for them to be held liable to repay the customer. This does not however preclude the Bank from proceeding further on the end fraudster who might have committed the fraud.

Several such cases have since been disposed off at other Adjudication offices particularly in Mumbai. Some of them have even been appealed in TDSAT. Students need to research these cases to understand how the judiciary may approach cases of E Banking frauds.

As regards Inter Bank frauds or Intra Bank frauds, the RBI may try to resolve it through a settlement. Where necessary, the cases may be referred to CBI or other forums and taken up by the Courts directly. If the amount involved is less than Rs 5 crores and one of the affected banks is a customer of the other bank, then it may be possible to treat such frauds as arising out of contravention of ITA 2000 and the adjudication system may be invoked as in the case of individual customers. In other cases the resolution has to be outside the Adjudication system.

## Limited Liability Circular

In a bid to protect the customers from the hassles of a long drawn litigation arising out of losses suffered due to E Banking frauds, RBI has introduced a system of "Limited Liability"[xxxviii] according to which the process of recovery of money lost through Cyber Crimes in Banking has been simplified.

The essence of the circular is that Bankers should have a linked mobile of the customer and should not fail to issue an SMS alert for every debit to the account. In case of any unauthorized transaction, if the customer informs the Banker within 3 days, he shall have zero liability. If the information is given after 3 days but before 7 days, the liability shall be limited to Rs 5000 for BSBD (Basic Savings bank Deposit) accounts.

In case of other SB Accounts, Pre-paid Payment Instruments and Gift Cards, Current/ Cash Credit/ Overdraft Accounts of MSMEs, Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh and Credit cards with limit up to Rs.5 lakh, the liability will be limited to Rs 10,000/-

In other cases (All other Current/ Cash Credit/ Overdraft Accounts and Credit cards with limit above Rs.5 lakh) the liability will be limited to Rs 25000/- .

If the Bank is informed beyond 7 days, the Bank will still be liable but the extent of liability would be as per the Bank's.

These limits will be applicable where the customer has no "Contributory Negligence" where he has parted with information on his account to phishing calls.

Most importantly, the burden of proving customer liability in case of unauthorised electronic banking transactions will lie on the bank.

The circular goes on to also mandate that the systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, banks must put in place:

i) appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;

ii) robust and dynamic fraud detection and prevention mechanism;

iii) mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorised transactions and measure the liabilities arising out of such events;

iv) appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom; and

v) a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

More details of the scheme is available at naavi.org[xxxix]

The Limited Liability circular if properly implemented will reduce the incidence of reference to the legal system including adjudication. Banks may however claim in most cases that there was "Negligence" of the customer but they need to also deduce the necessary proof.

If Banks are expected to follow the guidelines under this circular, the reversal of fraudulent transaction has to be completed within 30 days by a value dated credit. Bank can pursue its legal remedies against the fraudsters and also avail of Cyber Insurance to protect their interests.

## Secure Electronic Transactions

Secure Electronic Transaction is a term used to describe a protocol that is often referred to by its short form SET used in handling online payments.

SET is cryptography based protocol for secure payment processing via non secure networks. It was introduced in 1996 and was backed by VISA, MasterCard and other payment processing industry leaders and used for online authentication of Credit Card transactions for enabling use of credit cards in E Commerce transactions. In 2003, the protocol was published as RFC 3538 (RFC=Request For Comments) as an open source document. However, presently SET has been replaced by more advanced systems such as VISA's 3-D Secure.

In an E Commerce transaction which involves a customer buying goods and services online and making payment online there are multiple parties involved in completing the transaction such as

1. The Customer and the Buyer.
2. The person who makes the payment who may be the buyer himself in most cases.
3. The Payer is the owner of the Credit Card (or other online payment instrument) which is used for the payment.
4. The Credit card is issued by a "Card issuing Bank"
5. The Merchant presents the payment request to his Bank which is the "Acquiring Bank" which makes the payment to the merchant and later collects it from the card issuing Bank.
6. Acquiring bank uses the services of card networks like VISA/Masters/American Express/Diners to authenticate the card payment

A Secure Electronic Transaction protocol has to ensure efficient completion of the transaction along with preservation of security in the process.

SET is one such protocol which defines the process by which the transaction must be handled by all the parties concerned.

Let's now look at the transaction in greater detail and how it moves through the system.
In the E Commerce transaction, the customer places an order in an online establishment for a certain description of goods at a certain price and specifications. This is an information that is relevant between the buyer and the seller.

The merchant-customer transaction generates a demand for payment from the supplier/seller which the buyer wants to pay using an online system such as the Credit Card. The customer for this purpose uses a credit card which he has already applied for and obtained from a Card issuing bank and obtained an approved limit.

The Merchant has a Banking relationship with his own Bank which is the "Acquiring bank" and whenever a customer presents payment through a credit card, the merchant presents it to his Acquiring Bank for approval and payment.
The entire details of the card such as name, card number, the date of expiry etc are shared by the customer with the Merchant. If it is a card present transaction, the merchant collects the Card and is also able to view the Card Verification Number (CVV) which is on the back of the card.

In the past, the cards were swiped in a hardware to capture the details on the magnetic stripe on the back and also an impression was generated of the front of the card. The customer was asked to sign the charge slip and the merchant was responsible for signature verification in comparison with the signature on the back of the card before accepting the charge slip. The charge slip was then physically collected by the acquiring Bank and presented to the card issuing bank like a cheque instrument.

At the time of collecting the card details at the merchant establishment, the CVV number which was on the back was not captured by the merchant and hence was kept away from him in the records. In the "Card Not Present" transaction, the CVV input was considered like a code only known to the card holder and hence considered like a password for authentication. In the current "Chip Based" credit cards, the POS (Point of Sale) equipment electronically reads the information on the Chip and a secret PIN is input by the customer to authenticate the transaction. This information is shared with the acquiring bank on real time for authentication purpose.

The Acquiring bank makes verification of the card by sending the information collected through the umbrella card network such as VISA or Masters (or American Express/Diners) and approves the card both for its authenticity and availability of credit. The network verifies the authenticity and credit availability and approves the transaction on behalf of the card issuing Bank which is received by the acquiring bank and passed in real time to the merchant as "Approval" of the transaction.

After this confirmation, the merchant accounts the money as received and releases the goods.
The Acquiring Bank then collects its money from the card issuing Bank who bills it to the card owner and collects the payment.

In this entire process, information which is confidential in nature has to pass through the internet or telephone network from the merchant to the acquiring bank to the network (VISA/Masters) and back.

In this process of electronic communication being passed through different systems, there is a possibility that the data may be stolen or modified. Stolen data may be used for committing frauds or even creating clones of the cards.

Hence Security of Electronic Transactions depend on the security of the electronic communications between the different users of the payment protocol.
It is for this purpose that "Cryptography" becomes a key aspect of security. Strong encryption ensures that data collected is encrypted at the earliest and is stored or transmitted only in an encrypted state so that it cannot be easily stolen while it is under storage or under transmission.

In the early version of SET, the objective of SET was to ensure that trade related information lies between the merchant and the customer and credit card information is not collected by the merchant. After the invoice is raised, the customer would be connected to the network of the acquiring bank so that the card information goes directly from the customer to the acquiring Bank. The Bank may not need the trading information but may receive only the card information. Thus by segregating the e-commerce invoice information from payment information, the security was increased as compared to providing all details to the merchant first who in turn sends it to the acquiring Bank.

## 3-D Secure

As of now most of the card processing companies use 3-D Secure system to secure the online electronic transactions related to e-Commerce. Hence SET has been replaced by 3-D Secure.

This protocol was first adopted by VISA as "Visa Secure" and later by Mastercard as "MastercardSecureCode". Other operators like JCB international (used widely in Japan and China) adopted it as J/Secure, and Americal Express as "American Express Safekey".

The protocol more clearly defined as EMV 3-D Protocol is a three domain secure messaging protocol developed by EMVCo and is meant for authentication in a "Card Not Present" (CNP) transaction. The additional security layer helps prevent unauthorized CNP tranasactions and protects the merchant from CNP exposure to fraud.

The basic concept of the protocol is to tie the financial authorization process with an online authentication. This additional security authentication is based on a three-domain model (hence the 3-D in the name itself).

The three domains are:

1. Acquirer domain (the bank and the merchant to which the money is being paid).
2. Issuer domain (the bank which issued the card being used).
3. Interoperability domain (the infrastructure provided by the card scheme, credit, debit, prepaid or other types of payment card, to support the 3-D Secure protocol). It includes the Internet, merchant plug-in, access control server and other software providers

The protocol uses XML messages sent over SSL connections with client authentication (this ensures the authenticity of both peers, the server and the client, using digital certificates).

A transaction using Verified-by-Visa or SecureCode will initiate a redirection to the website of the card issuing bank to authorize the transaction. Each issuer could use any kind of authentication method (the protocol does not cover this) but typically, a password-based method is used, so to effectively buy on the Internet means using a password tied to the card. The Verified-by-Visa protocol recommends the bank's verification page to load in an inline frame session. In this way, the bank's systems can be held responsible for most security breaches. Today it is easy to send a one-time password as part of an SMS text message to users' mobile phones and emails for authentication, at least during enrollment and for forgotten passwords.

The main difference between Visa and Mastercard implementations lies in the method to generate the UCAF (Universal Cardholder Authentication Field): Mastercard uses AAV (Accountholder Authentication Value) and Visa uses CAVV (Cardholder Authentication Verification Value).
Despite all the efforts to improve the security of online payment systems, it must be recognized that online frauds are a reality and some times it is caused by the lack of security awareness of the customers as well as the inherent security vulnerabilities in the software, hardware as well as the protocols used.

The users of the system are required to adopt best industry practices regarding information security and obtain necessary Cyber Insurance. The PCI-DSS (Payment Card Industry Data Security System) is a standard that all users of Credit Card systems are expected to follow to be compliant with the requirements of CISA/Master network operators. The merchants are periodically audited for compliance of such security standards. With the advent of data protection regulations, the merchants are also exposed to the compliance requirements of data protection regulations and PCI-DSS[xl] or ISO27001[xli] or PDPSI[xlii] or other standards

In India the Aadhaar Authenticated payment System (AEPS) was also being considered as a payment mechanism where the UIDAI network could be used for authenticating an individual

who by further linking the transaction to the UPI network operated by NPCI could trigger online payments. Due to certain reservations expressed by the Supreme Court on Privacy issues in the use of Aadhaar by private parties, the system has gone into the background and alternatives such as "Virtual Aadhaar ID" and "Offline Aadhaar Authentication" is being considered to make the system compliant with the privacy regulations.

However, these changes may gain traction only after the Personal Data Protection Act is passed in India and the Government of the day takes up the issue of presenting a "Protocol" for the use of UIDAI and UPI jointly with "Rupay" cards.

## Concluding Remarks:

E Banking has today taken many dimensions including the Mobile Banking, the Prepaid Cards and other modes. Despite the efforts of the RBI, frauds have been increasing and becoming more and more sophisticated. As a measure of addressing the menace, RBI has increased the due diligence expectations of the Banks and adopted a stringent Cyber Security Framework for the industry. However the cost of information security has prevented small Banks from adopting the required levels of security and fraudsters are exploiting the lower levels of security in Cooperative Banks and attacking the Banks directly through the inter banking systems. The Banks as well as the customers are therefore looking forward to the development of Cyber Insurance to protect their financial interests in the digital banking era.

**References**


1. https://www.naavi.org/wp/index-of-articles-on-bitcoin-the-currency-of-the-criminals-by-the-criminals-for-the-criminals/
2. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0
3. https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=243
4. http://www.naavi.org/cl_editorial_11/ggwg_rbi_circular.pdf
5. http://www.naavi.org/archives/archive_2011/comments_ggwg.htm
6. http://www.naavi.org/cl_editorial_11/ggwg_rbi_circular.pdf
7. https://www.naavi.org/wp/umashankar-judgement-upheld-by-tdsat/
8. https://www.naavi.org/wp/a-note-for-the-attention-of-smes-on-cheque-disincentivisation/
9. https://m.rbi.org.in/Scripts/FAQView.aspx?Id=24
10. http://www.naavi.org/importantlaws/it_rules_compendium/adj_off_notification_goi.pdf
11. http://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf
12. https://www.naavi.org/wp/umashankar-judgement-upheld-by-tdsat/
13. http://naavi.org/uploads_wp/new/juy_72017_limited_liability.PDF
14. https://www.naavi.org/wp/zero-liability-is-there-a-fine-print-that-depositors-should-be-

wary-of/

15. https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
16. https://www.iso.org/isoiec-27001-information-security.html
17. https://www.naavi.org/wp/india-to-be-the-hub-of-international-personal-data-processing-objective-of-pdpsi/

*P.S: Since the entire content has been drawn from dynamic resources in the Internet and most of the published books may not contain updated information, no reference to books have been provided. In the changing world of technology, the value of judicial precedence is also low. Every judicial decision has to be seen with the law and technology as applicable to a case on hand and hence excessive reliance on case laws in areas of E Commerce is better avoided. Hence it is recommended that students develop an insight into the legal interpretation from out of the current developments they may observe on the resources available on the Internet after due filtration for the credibility of the information.*

# Chapter IV: Taxation Issues in Cyber Space

**Syllabus:**

Foundations of Taxation : Theoretical underpinnings, Canons of Taxation, Constitutional Basis of Tax

Direct Tax Regime: Residential status of assesse (company), Source v. residence based taxation, Scope of total income, Source based taxation (sec.9), Existing framework for taxation of e-commerce (business income),Online market, online subscription service, online advertisingCharacterization of income-royalty or fees for technical services, Equalisation levy

Indirect Tax Regime: Basics of GST,GST on Online Information Data Access and Retrieval (OIDAR),GST on non-OIDAR

**Learning Objectives:**

In this Chapter, the student would learn the basic tenets of taxation, the direct and indirect tax system prevalent in India, the concept of GST and an overview of the E Commerce taxation in India.

## Introduction

Cyber Space evolved as a space created by a communication system that included electronic documents which were instruments created in a language called "Binary", understood and interpreted for human consumption by devices called "Computer". It originated as a "Borderless" transaction space where documents could fly across physical boundaries as zeros and ones streamed through wireless and satellite transmissions. The identity of senders and receivers were also determined by the technology of connectivity and depended on the "network identification of the connected devices" such as the IP address.

As long as Internet was used only for communication, there was no issue that bothered regulators. But as the Internet became a medium for commercial communications and the laws like the

UNCITRAL Model Law on E Commerce and its derivatives like the Information Technology Act evolved, the electronic documents acquired a legal meaning. Any commercial transaction that occurred in this network therefore became accountable for legal purpose.
In this scenario the E Commerce took birth. Initially the share of E Commerce in global commerce was too small for tax authorities to bother about loss of income. Initially therefore there was a move to encourage E Commerce and hence there was "Exemption" of e-commerce from taxation. There was only talk of incentives for the use of E Commerce.

But as the volume of transactions increased, it became necessary for tax authorities in every country to review their approach to taxing of E Commerce. Since E Commerce also involved transnational trading across borders where physical goods were also involved besides the digital goods, the issues of International taxation also became relevant.

Hence E Commerce taxation regime today has to take into account both local taxation as well as international taxation issues.

We shall try to address some of these aspects in the following paragraphs.

## Taxation in India

Taxes form the main revenue of the Government. Both the Central Government and the State Government levy taxes based on their constitutional responsibilities of Governance. Some minor taxes may be also levied by local administration like the Corporations and Municipalities.
The authority to impose tax is conferred under Article 265 of the Constitution of India. The article states

> **Art 265: Taxes not to be imposed save by authority of law:**
>
> No Tax shall be levied or collected except by authority of law

"Law" means an act of legislature and it should be within the legislative competence of the legislature.
Article 246 of the Constitution has divided the responsibility of Governance and the power to levy taxes follow the same principle.
Accordingly, the Seventh schedule of the constitution[xliii] lists the powers of the Union/Central Government and the State Government into three lists namely

a) Union List where only the Parliament can make law
b) State List where only the State legislatures can make laws
c) Concurrent list where both Central and State Governments have powers to make laws.

The Union List consists of about 97 items

- Taxes on income other than agricultural income
- Duties on customs including export duties
- Duties of excise on tobacco and other goods manufactured or produced in India except
    - (a) alcoholic liquors for human consumption
    - (b) opium, Indian hemp and other narcotic drugs and narcotics;
    - but including medicinal and toilet preparations containing alcohol or any substance included in sub-paragraph (b) of this entry.
- Corporation Tax
- Taxes on services….etc

The State List consists of 66 items including the following:

- Taxes on agricultural income.
- Duties in respect of succession to agricultural land.
- Taxes on lands and buildings.
- Taxes on mineral rights subject to any limitations imposed by Parliament by law relating to mineral development.
- Duties of excise on the following goods manufactured or produced in the State and countervailing duties at the same or lower rates on similar goods manufactured or produced elsewhere in India-
    - (a) alcoholic liquors for human consumption
    - (b) opium, Indian hemp and other narcotic drugs and narcotics
        - but not including medicinal and toilet preparations containing alcohol or any substance included in sub-paragraph (b) of this entry.
- Taxes on the entry of goods into a local area for consumption, use or sale therein.
- Taxes on the consumption or sale of electricity. etc

The Concurrent list of taxation consists of 47 items including the following:

- Stamp duties other than duties or fees collected by means of judicial stamps, but not including rates of stamp duty.

## Principles of Taxation

Major principles of taxation by which a Government is meant to be guided in designing an equitable taxation regime are

- **Adequacy**: taxes should be just-enough to generate revenue required for provision of essential public services.

- **Broad Basing:**taxes should be spread over as wide as possible section of the population, or sectors of economy, to minimize the individual tax burden.
- **Compatibility:**taxes should be coordinated to ensure overall objectives of good governance.
- **Convenience:**taxes should be enforced in a manner that facilitates voluntary compliance to the maximum extent possible.
- **Earmarking:** tax revenue from a specific source should be dedicated to a specific purpose only when there is a direct cost-and-benefit link between the tax source and the expenditure, such as use of motor fuel tax for road maintenance
- **Efficiency:** tax collection efforts should not cost an inordinately high percentage of tax revenues.
- **Equity:** taxes should equally burden all individuals or entities in similar economic circumstances.
- **Neutrality:** taxes should not favor any one group or sector over another, and should not be designed to interfere-with or influence individual decisions-making.
- **Predictability:** collection of taxes should reinforce their inevitability and regularity.
- **Restricted exemptions:** tax exemptions must only be for specific purposes (such as to encourage investment) and for a limited period.
- **Simplicity:** tax assessment and determination should be easy to understand by an average taxpayer.

## Source Vs. Residence based taxation

In taxation of transactions that cut across two different tax authorities, taxation may adopt either the source based system or Residence based system

In a Source based taxation system tax is levied where the income arises. In the Residence based system, the tax is levied on the basis of residence of an assesse.

Indian taxation system adopts a combination of both systems.

Internationally there is also a concept of “Withholding Tax” where the country of the buyer deducts some amount as with holding tax before remitting the payment to an outsider. The ultimate taxability may be determined on the basis of tax treaties.

## Types of Taxes

Taxes can be fundamentally categorized into two types namely Direct Tax and Indirect Tax.
Direct Tax is the tax which is paid directly by an individual or organization. It is levied taking into consideration the ability-to-pay principle, which means that if you earn more, your rate of tax is also more. The purpose of Direct Tax is to redistribute the wealth of a nation.

Indirect Tax on the other hand is a taxlevied on goods or services, paid by the end consumer, by way of a higher retail price. Indirect taxes are passed on, to the consumer as the price of the commodity is compensated for by simply increasing the overall price of the good or service. Indirect taxes are levied equally upon all taxpayers irrespective of their income. The Rich and the Poor both pay the same tax for the same goods.

**Income Tax** is the principle direct tax that is payable by the assesses in India. It is the tax payable on the income earned during an assessment period. Advance Tax, Tax Deduction at Source are taxes on income collected in advance and deductible from the final tax payable and are not separate taxes.

**Capital Gains tax** is a form of tax payable on income earned by sale of Capital Assets based on the period of holding.

**Service Tax** is a the tax payable for supply of services as different from sale of "Goods".

**GST** is the tax payable on the transactions related to sale of goods and services.

**Securities Transaction Tax** is tax levied on securities transactions.

**Customs Duty** is the levy imposed on the import of goods.

**Dividend Tax** is the tax payable on dividend distributed by a Company.

**Minimum Alternate Tax (MAT)** is the tax payable by a Company on a flat basis when the assessed tax liability is otherwise Zero.

**Alternate Minimum Tax (AMT)** is a tax applicable to individuals for certain classes of assesses who have claimed certain deductions.

**Composite Tax** is the alternate tax payable by an assesse on a flat basis without going into detailed assessment, normally applied to small assesses as a part of simplification of the process of tax calculation. It may be applied to GST or Firms and LLP.

In reality, the division of taxes as Direct and Indirect may be unclear and may overlap.

For example, Income tax is treated as direct tax to be directly paid by the income earner. But taxes are deducted at source (TDS) and paid directly by the person responsible to pay leaving only the net amount becomes income of the earner.

Similarly, Service Tax is an indirect tax because it is collected by the service provider and passed on to the service receiver. However, in many services like works contract, manpower supply; it is the service recipient, who not only bear the tax burden, but also deposit the same to the government exchequer.

Income of a service provider results in payment of service tax on the turnover and income tax on the income after deduction of expenditure resulting in double taxation.

In practice, the legislation decides whether a tax is called a direct tax or an indirect tax. When service tax was introduced in India in 1994, there was a dispute for several years, whether it should be administered as Direct Tax by CBDT or Indirect Tax by CBEC. Finally, it was decided that it should be administered by CBEC and hence it became an Indirect tax. Had it been administered by CBDT, it would have been known today as Direct Tax.

A more realistic differentiation between the two taxes may be as following.

- Direct Taxes are the taxes that are levied on the income of individuals or organisations. And include Income tax, corporate tax,
- Indirect taxes are those paid by consumers when they buy goods and services. .

## Direct Tax Regime

Incidence of Taxes depend on the status of the assesse such as whether he is an Individual, HUF, Firm, Company etc, Corporate and also on the "Residential Status" of the assesse.

The "Residential Status" could be

a) Resident (and ordinarily Resident)

b) Resident but not ordinarily Resident (RNOR)

c) Non Resident (NR)

A person is a Non Resident if he is not a Resident as per the Income Tax Act. (Sec 6)[xliv] (IT Act)
An individual person is said to be resident in India in any previous year to which the tax assessment relates to if

a) He is in India in that year for a period or periods amounting in all to 182 days or more or
b) Has been in India for a period of 365 days or more within the four preceding years and 60 days in the previous year

If a person is an Indian Citizen working abroad or is a member of a crew of an Indian ship, or he is a person of Indian origin who is on a visit to India, the second condition is not applicable.

A Company is said to be a resident in India in any previous year if

a) It is an Indian Company or
b) Its place of effective management in that year is in India

A person is said to be "not ordinarily resident" in India in any previous year if such person is an individual who has been a non-resident in India in nine out of the ten previous years preceding that year, or has during the seven previous years preceding that year been in India for a period of, or periods amounting in all to, seven hundred and twenty-nine days or less;

## Tax Incidence

A Resident of India is taxed under Income Tax Act for his Total global income that is income arising from India and elsewhere, subject to any double tax avoidance treaties that may be applicable.
In the case of Residents but not ordinarily residents, Income arising out of India is taxable and Income arising out of business controlled in India is also taxable. Income whose source of origin is not India is not taxed.

In the Case of Non Residents, income accruing outside India would not be taxable in India. However, income which accrues to them or arises in India as well as deemed to accrue or arise in India is taxable. Also income received in India and deemed to be received in India is taxable.
In case of Companies incorporated in India, (like the individuals who are non residents of Indian origin), income accruing outside India from a business controlled from India or from a profession set up in India is not taxed in India.

Non Residents holding Indian Citzenship and/or Indian Origin may be eligible for certain exemptions in the computation of Income for tax purposes as compared to others.

A Company which is owned and controlled by Non Residents of Indian Citizenship or Origin (NRI) to the extent of more than 60% may be entitled to the privileges available to NRIs

If a Company is incorporated outside India, then the taxability would be different.
In the case of E Commerce taxation, income arising out of the E Commerce activity is income from business and will be taxed as per the terms of the Income Tax act along with whatever exceptions are provided therein.

## Tax on Royalty Income

Royalty received is income for the recipient. Royalty paid is the expenditure for the paying entity. Royalty may be payable on Books to the Authors or on Patents and Copyrights.

**Tax consideration on Royalty Payment**

Income Tax Act provides specific deductions for Royalty paid to "Authors" in respect of Books under Section 80QQB.
As regards Software, it is often not sold but licensed. Sale of software can be on a media like the CD when it can be identified as "Goods" and also allowed for download without a media, in which case it will be treated as an online information service.

When the software is licensed, the property is not transferred to the buyer and only a permission to use is granted. The payment made in consideration of such license has to be accounted as "License Fee" similar to the royalty.

Similarly, in products that are "Patented" or "Trade marked", the use may be subject to royalty or out right sale as the contract may determine. Where there is no transfer of property, the payments are similar to "Royalty".

Some times during the development of a software or in other projects, there may be payments involved for transfer of technical knowhow which is also in the nature of either an absolute sale or a transfer of right and hence the income may have the nature of royalty.

In case of payments going out of India, if the payment is characterised as royalty, it is subject to withholding tax at 20% on gross basis (this rate may be reduced by the provisions of a Double

Taxation Avoidance Agreements ("DTAA") between India and the country of residence of the foreign company). The payer would thus be required to withhold tax at such applicable rate on gross basis while making the payment or crediting the amount in its books to the foreign company.

If the fees paid by an Indian company to a foreign company for availing of services in relation to computer software are regarded as "fees for technical / included services", they could be subject to withholding tax in India at the rate of 20% on gross basis (this rate may be reduced by the provisions of a DTAA between India and the country of residence of the foreign company).

A payment characterised as business income is subject to taxation in India only if the foreign company has a business connection (permanent establishment in case there exists a DTAA between India and the country of residence of the concerned foreign company) in India. In such a scenario, only that portion of income that is attributable to a business connection or the permanent establishment ("PE"), as the case may be, in India, will be subject to tax in India.

In case of transactions which are classified as "Sales", the payment may be characterised as capital gains and taxed accordingly.

**Tax Consideration for Royalty Received**

Under section 9(1)(vi) of the Income Tax Act, in Explanation 2, royalty is defined as

> -the consideration (including lump sum payment) for the transfer of all or any rights (including the granting of a license) in respect of a patent, invention, model, design, secret formula, process, trademark, copyright, literary, artistic or scientific work.

It further includes consideration for the use of any patent, invention, model, design, secret formula, process, trademark or similar property.

Where the consideration paid is for the purchase of a product, and not for the transfer of the intellectual property per se, it may not be regarded as royalty. For example, the purchase of a book by a customer does not tantamount to the purchase of the copyright in the book, even though the publisher publishes the book by purchasing the copyright. Drawing a parallel from this example, purchase of a shrink-wrap product by an Indian company from a foreign company should not be regarded as purchase of a copyright but only a purchase of a copyrighted article and thus the payment therefor should not be regarded as royalty.

An important aspect that has been emphasised by the Indian courts is that while characterising the income, one should look at the predominant purpose for which the consideration is paid in a transaction.

## E Commerce Taxation for a Foreign Company

If the E Commerce activity is owned by an entity which is not a company registered in India (nor an individual who is a resident in India), then the rules applicable to foreign companies would be applicable. In such a scenario the concept of "Permanent Establishment" (PE) would come into reckoning.

In 2001, the CBDT had constituted a High Powered Committee (HPC) to contemplate the need for a separate tax regime for e-commerce transactions. The report submitted by the HPC took into consideration the principles laid down by the Organisation for Economic Co-operation and Development (OECD) for taxation of e-commerce transactions. It maintained that the existing laws are sufficient to tax e-commerce transactions and that no separate regime is required.

An Indian Company is always treated as a resident and taxed accordingly. Any other company would be resident if its "Place of Effective Management" is in India.

Usually, foreign companies get tax concession under Double Taxation Avoidance Treaties and they pay taxes in their home countries. But if they have Permanent Establishments (PE) in India, they should pay taxes for the income they have created in India. Thus PE makes a Indian income of a foreign company taxable in India.

Issues around the taxability of income and the corresponding litigation are primarily on account of the reasons such as Characterization of income in the hands of the non-resident.
Certain types of income such as royalty and fees for technical services deemed to accrue or arise in India are taxable in India, but business profits in the absence of a permanent establishment (PE) are not.

On the PE front, there have been issues around whether a website in India constitutes a PE for a non-resident and whether certain activities performed by an agent in India constitute a dependent agent PE.

## Permanent Establishment

A Permanent Establishment in India is a fixed place of business, wholly or partly carried out by a foreign enterprise operating in India. Such fixed place of business can be a branch office, a place of management, a factory, a warehouse, a workshop etc.

The place of effective management (POEM) in case of a company engaged in active business outside India shall be presumed to be outside India if the majority meetings of the board of directors of the company are held outside India.

A company shall be said to be engaged in "active business outside India" if –

a. the passive income is not more than 50 per cent of its total income;

b. less than 50 per cent of its total assets are situated in India;

c. less than 50 per cent of total number of employees are situated in India or are resident in India;

and

d. the payroll expenses incurred on such employees is less than 50 per cent of its total payroll expenditure.

Passive income - "Passive income" of a company shall be aggregate of, —

a. income from the transactions where both the purchase and sale of goods is from/to its associated enterprises; and

b. income by way of royalty, dividend, capital gains, interest or rental income;

However, any income by way of interest shall not be considered to be passive income in case of a company which is engaged in the business of banking or is a public financial institution, and its activities are regulated as such under the applicable laws of the country of incorporation.

If on the basis of facts and circumstances it is established that the Board of directors of the company are standing aside and not exercising their powers of management and such powers are being exercised by either the holding company or any other person(s) resident in India, then the place of effective management shall be considered to be in India. For this purpose, merely because the Board of Directors follows general and objective principles of global policy of the group laid down by the parent entity which may be in the field of Pay roll functions, Accounting, Human resource (HR) functions, IT infrastructure and network platforms, Supply chain functions, Routine banking operational procedures, and not being specific to any entity or group of entities per se; would not constitute a case of Board of Directors of companies standing aside.

In most cases, the determination of POEM would be a two stage process, namely, identification or ascertaining the person or persons who actually make the key management and commercial decision for conduct of the company's business as a whole and determination of place where these decisions are in fact being made.

The place where these management decisions are taken would be more important than the place where such decisions are implemented. For the purpose of determination of POEM it is the substance which would be conclusive rather than the form.

It may be noted that the definition of permanent establishment may differ in each tax treaty.
The PE concept marks the dividing line for businesses between merely trading with a country and trading in that country. If an enterprise has a PE, its presence in a country is sufficiently substantial than when it is trading in a country.

In the Finance Bill 2018 the following Clarification was made:
Significant Economic Presence shall mean:

(i) Any transaction in respect of any goods, services or property carried out by a non-resident in India including provision of download of data or software in India

- if the aggregate of payments arising from such transaction or transactions during the previous year exceeds the amount as may be prescribed; or

(ii) Systematic and continuous soliciting of its business activities or engaging in interaction with such number of users as may be prescribed, in India through digital means.

It is further proposed that the transactions or activities shall constitute significant economic presence in India, whether or not the non-resident has a residence or place of business in India or renders services in India.

## Equalization Levy

Equalisation Levy is a direct tax imposed on Non-Resident service providers – Who earn revenue from India in excess of the Threshold. Its very purpose is to protect Indian Residents.

Equalisation Levy is charged only for services and only on non-residents of India. Hence Indian E-commerce companies are not liable to Equalisation Levy.

If a company is non-resident today and it opens a subsidiary or a PE in India to provide E-commerce services in India, the Indian subsidiary / PE will be liable to normal Indian Income-tax and it will escape Equalisation Levy.

Also, all Indian residents are already liable to Indian Income tax on their global incomes.
Only Non Residents who earn revenue from India; and escape Indian Income tax are sought to be covered by EL.

For EL, there is no need to determine Permanent Establishment or any other nexus to India because the liability for EL is when the non-resident earns revenue from India.
Revenue is the source of determining the EL liability. When it is in excess of the threshold, the nexus is adequate for India's tax jurisdiction.

Chapter VIII of Finance Act under which EL is introduced does not become part of the Income-tax law. Like STT, it will remain a separate tax. Hence Double Tax Avoidance Agreements are not applicable to EL.

Millions of home consumers and small business consumers utilise internet services like Google, Face Book, WhatsApp, Twitter etc. Only persons carrying on business or profession and making payment for specified services to non-resident E-commerce companies are liable for deducting EL at source and paying to Government of India.

Tax is payable on gross amount if it exceeds Rs 1 lakh . Hence there is no computation of taxable income and no deduction of expenses.
If the non-resident service provider receives less than Rs. 1 lakh from one Resident Payee, he is not liable to EL . If the resident payer is paying less than Rs. 1 lakh, to each NR service provider, he is not liable to deduct EL at source

Equalisation levy is aimed at levelling the play field between e-commerce players of domestic and foreign origin and e-commerce companies are expected to benefit from it.

## GST Impact on E Commerce

GST is a system of taxation relevant to all business and services in India. E Commerce being business done on the Internet is also within the purview of GST either as a stand alone activity or as a part of the sales channel of an organization. However, when GST itself is a concept which is

new, understanding of the challenges of E Commerce is even tougher for the tax authorities as well as the assesses.

The CGST Act defines Electronic Commerce as the supplyof goods or services or both, including digital products over digital or electronic network. [Sec 2(44)]
As per Section 2(105) of the CGST Act, 2017, Section 2(105) "supplier" in relation to any goods or services or both, shall mean the person supplying the said goods or services or both and shall include an agent acting as such on behalf of such supplier in relation to the goods or services or both supplied;
Further, as per Section 2(45), of the CGST Act, "electronic commerce operator" is defined as any person who owns, operates or manages digital or electronic facility or platform for electronic commerce.

The Act defines "goods" as every kind of movable property other than money and securities but includes actionable claim, growing crops, grass and things attached to or forming part of the land which are agreed to be severed before supply or under a contract of supply;
Services is defined as anything other than goods, money and securities but includes activities relating to the use of money or its conversion by cash or by any other mode, from one form, currency or denomination, to another form, currency or denomination for which a separate consideration is charged;

As a result of the above different components of E Commerce such as the market place operation, the logistic services, the payment services etc become taxable under GST and each subsequent activity is eligible for input tax credit.

The Goods and Service Tax Act was passed in the Parliament on 29th March 2017. The Act came into effect on 1st July 2017.
Goods & Services Tax Law in India is a comprehensive, multi-stage, destination-based tax that is levied on every value addition. Under the GST regime, the tax is levied at every point of sale. In the case of intra-state sales, Central GST and State GST are charged. Inter-state sales are chargeable to Integrated GST.

The GST proposition started in 2000 under the Vajapayee Government and culminated in 2017 under the Modi Government. The most difficult aspect of the law was to bring the States on board since there was an apprehension about loss of revenue of the States which needed to be addressed. Additionally, in a federal system of Governance the political differences between the Central and State Governments also delayed the implementation.

The constitution defines “Goods and Services Tax” as any tax on supply of goods, or services or both,

The Central and State governments will have simultaneous powers to levy the GST on Intra-State supply. However, the Parliament alone shall have exclusive power to make laws with respect to levy of Goods and Services Tax on Inter-State supply

There are different categories for rates of taxation 0%, 0.25%, 5%, 12%, 18% and 28%. An attempt is being made to reduce the tax slabs and rationalize the items in different tax slabs.

There are essentially three types of GST namely :

**CGST** : Central share of the tax on Goods and Services

**SGST/UGST**: Share of the State or Union Territory when the sales is within the State

**Integrated GST:** Where there is inter state movement of Goods and tax is collected by the Central Government from the buying State and later distributed to States

Under GST mechanism, every trader will have a unique registration. (Certain categories are exempted) based on commodities, Turnover and Type of activity.

Every invoice is entered into the system by the seller of the goods in the returns monthly and quarterly

Every supply is entered into the system by the seller and every receipt is entered into the system by the receiver of goods in the respective returns which are matched and reconciled.

Tax is collected in the invoice and directly distributed to the State or the Center

GST is mainly technologically driven. All activities like registration, return filing, application for refund and response to notice needs to be done online on the GST Portal. As a result the process of tax collection is automatic and quick..Tax is collected in the invoice and directly distributed to the State or the Center.

It however requires some computer literacy by the trader and possible incidence of computer frauds which need to be addressed.

For small establishments, Composition Scheme is available where GST may be paid at a consolidated fixed rate based on the turnover. (Presently this is optionally applicable for tax payers with turnover of less than Rs 1 crore).

Generally, the supplier of goods or services is liable to pay GST. However, in specified cases like imports and other notified supplies, the liability may be cast on the recipient under the reverse

charge mechanism. Reverse charge means the liability to pay tax is on the recipient of supply of goods or services instead of the supplier of such goods or services in respect of notified categories of supply.

There are two type of reverse charge scenarios provided in law

- Supply from an Unregistered Supplier
- Supply of specific goods or services

Reverse Charge is required in certain cases where the recipient of the goods or services is required to pay GST instead of the supplier.Government may, specify categories of supply of goods or services or both, the tax on which shall be paid on reverse

- Legal Services by advocate
- Goods Transport Agency Services
- Services supplied by an arbitral tribunal to a business entity
- Supply of services by an author, music composer, photographer, artist ..etc
- Services supplied by a recovery agent to a banking company or a financial institution or a non-banking financial company
- Cashew nuts, not shelled or peeled
- Bidi wrapper leaves (tendu)
- Tobacco leaves

GST subsumed many of the existing taxes and simplified the system of indirect taxes in India.

At the Central level, GST subsumed the following taxes:

a. Central Excise duty
b. . Duties of Excise (Medicinal and Toilet Preparations)
c. Additional Duties of Excise (Goods of Special Importance)
d. Additional Duties of Excise (Textiles and Textile Products)
e. Additional Duties of Customs (commonly known as CVD)
f. Special Additional Duty of Customs (SAD)
g. Service Tax
h. Central Surcharges and Cesses so far as they relate to supply of goods and services

At the state level, it subsumed the following taxes:

ii) State taxes that would be subsumed under the GST are:

a. State VAT
b. Central Sales Tax
c. Luxury Tax
d. Entry Tax (all forms)

e. Entertainment and Amusement Tax (except when levied by the local bodies)

f. Taxes on advertisements g. Purchase Tax

h. Taxes on lotteries, betting and gambling

i. State Surcharges and Cesses so far as they relate to supply of goods and services.

As a result, one of the advantages of GST is that it has removed the Cascading effect on the sale of goods and services where by from manufacturing to the point of sale, taxes on cost of goods at one point included the tax in the previous stage and therefore further VAT included tax on tax.

Under GST, Registered Suppliers must charge GST on supplies at the prevailing rate. This GST that is charged and collected is known as output tax .

The GST that incurred on business purchases and expenses (including import of goods) is known as input tax .Since the GST regime eliminates the tax on tax, the cost of goods decreases if the "Input Tax Credit" is accounted.

Input tax credit may not be available in cases such as:

- If goods and services are acquired for personal use.
- If one has paid tax in GST composition scheme for goods and services received.
- In case an immovable property is built apart from plant and machinery using the goods and services and this immovable property is not transferred.
- In the case where employees have used the goods and services for personal purposes.
- When the cost of capital goods depreciation is claimed, then Input Tax Credit cannot be claimed.

There are some teething problems in this regard which needs to be sorted out and in some cases the benefit of the input tax credits may not passed on to the consumers. Hopefully this will be ironed out over a period of time.

Law provides for "Anti Profiteering levy for those who try to cheat the consumers by not passing on the input tax credit. The crux of the anti-profiteering rules is that if there is reduction in rate of tax on the supply of goods or services or Benefit of input tax credit is now available under GST then a registered person must pass on the benefit by reduction in prices. In case where contract of supplies is inclusive of taxes, this provision will cast responsibility on the supplier to reduce the price due to reduction in rate of taxes.

## Scope of "Supply" under GST

The meaning and scope of supply under GST can be understood in terms of following six parameters, which can be adopted to characterize a transaction as supply:

1. Supply of goods or services. Supply of anything other than goods or services does not attract GST
2. Supply should be made for a consideration
3. Supply should be made in the course or furtherance of business
4. Supply should be made by a taxable person
5. Supply should be a taxable supply
6. Supply should be made within the taxable territory

Any transaction involving supply of goods or services without consideration is not a supply, barring few exceptions, as follows in which a transaction is deemed to be a supply even without consideration.

- an individual who is carrying on business and registered under normal tax provisions, transfers a car used for its business to another individual, permanently as a gift than it would constitute a taxable supply under GST.
- goods held or used for the purposes of the business, but are put to any private use
- Donation of business assets or scrapping or disposal in any other manner like giving the laptops to employee after period of use (other than as a sale – i.e., for a consideration) would also qualify as 'supply', where input tax credit has been claimed.

Activities as mentioned below shall be treated as supply even if made without consideration:

- Permanent transfer or disposal of business assets where input tax credit has been availed on such assets.
- Supply of goods or services or both between related persons or between distinct persons as specified, when made in the course or furtherance of business:
  Provided that gifts not exceeding fifty thousand rupees in value in a financial year by an employer to an employee shall not be treated as supply of goods or services or both.
- Supply of goods—
  (a) by a principal to his agent where the agent undertakes to supply such goods on behalf of the principal; or
  (b) by an agent to his principal where the agent undertakes to receive such goods on behalf of the principal.

Import of services for a consideration, whether or not in the course or furtherance of business is treated as supply.

Eg: Overseas entity send its officers to overlook its India operation and remuneration of these officers are paid by parent and these cost is not charged to its India unit. India entity would have to pay tax on transaction on open market value on reverse charge mechanism. where the Indian parent establishes overseas subsidiaries or liaison offices, to sell its services, services imported from the overseas subsidiaries, would be treated as taxable supply

Some of the activities which shall be treated as neither supply of goods nor supply of services and are outside the scope of GST are

- Services by an employee to the employer in the course of or in relation to his employment.
- Services of funeral, burial, crematorium or mortuary including transportation of the deceased.
- Sale of land and sale of building where the entire consideration has been received after completion certificate is issued or after its first occupation.
- Actionable claims are included in the definition of goods, however, that actionable claims other than lottery, betting and gambling shall be neither goods nor services.

The securities are excluded from the definition of goods as well as that of services. Money is also excluded from the definition of goods as well as services,. However, activities relating to the use of money or its conversion by cash or by any other mode, from one form, currency or denomination, to another form, currency or denomination for which a separate consideration is charged are included in services.

Consideration can be in money or in kind. A deposit given in respect of the supply of goods or services or both shall not be considered as payment made for such supply unless the supplier applies such deposit as consideration for the said supply. Further, when there is barter of goods of services, the same activity constitutes supply as well as a consideration.

A supply to attract GST should be made by a taxable person. Hence, a supply between two non-taxable persons does not constitute supply under GST. A “taxable person” is a person who is registered or liable to be registered under section 22 or section 24. Hence, even an unregistered

person who is liable to be registered is a taxable person. Similarly, a person not liable to be registered but has taken voluntary registration and got himself registered is also a taxable person.

**Composition Scheme**

A taxpayer whose turnover is below Rs 1.5 crores lakhs can opt in for Composition Scheme. GST in such cases would be a flat 2% on turn over for manufacturing, 5% for restaurant services, 1% for traders. No Input Tax Credit can be claimed by a dealer opting for composition scheme. The taxpayer can only make intra-state supply (sell in the same state) i.e. no inter-state supply of goods

It may be noted that businesses which supply goods through an e-commerce operator cannot opt for Composition Scheme

**Tax Collection At Source**

Marketplace operators are mandatorily required to deduct a percentage amount as the GST liability of seller and deposit it with government. (1%+1% of the net value of taxable supplies). This mechanism is being termed as "Tax Collection at Source (TCS)" under the GST law.

Eventually the marketplace seller will have to file monthly return under GST to claim the credit of TCS collected by the marketplace operator. This will also impact the liquidity and cash flow of these sellers.

**Supplies from Multiple States**

It should be noted that GST in India is State-centric. Hence, a person making supplies from different States needs to take separate registration in each State.

Further, the person may take more than one registration within a State if the person has multiple business verticals. A person who has obtained or is required to obtain more than one registration, whether in one State or Union territory or more than one State or Union territory shall, in respect of each such registration, be treated as distinct persons for the purposes of GST. Hence, a supply between these entities constitutes supply under GST.

**Inter/Intra State Supply**

The location of the supplier and the place of supply determines whether a supply is treated as an Intra State supply or an Inter State supply. Determination of the nature of supply is essential to ascertain whether integrated tax is to be paid or Central plus State tax are to be paid.

Inter- State supply of goods means a supply of goods where the location of the supplier and place of supply are in different States or Union territories. Intra State supply of goods means supply of

goods where the location of the supplier and the place of supply are in the same State or Union territory. Imports, Supplies from and to SEZs are treated as deemed Inter-State supplies.

**Exports and Imports**

Exports is considered as Zero rated supply and hence not taxable. Traders who export can export under bond/letter of undertaking without payment of tax and claim refund of input tax credit or pay IGST after setting off the input tax credit and claim the refund of tax paid. In E Commerce transactions therefore, delivery of products outside the geography of India particularly in respect of soft products need to be accounted as "Exports".

Under GST, the import of service is taxable if the supplier of service is located outside India, the recipient of service is located in India,.

However, there is no drastic change with respect to levy of Custom duty, Education cess, Anti-dumping duty, safeguard duty and the like. GST replaces Counterveiling duty and special additional duty of customs with Integrated GST. All imports shall be deemed as inter-State supplies and accordingly Integrated tax shall be levied in addition to the applicable Custom duties.

The IGST Act, 2017 provides that the integrated tax on goods imported into India shall be levied and collected in accordance with the provisions of the Customs Tariff Act, 1975 on the value as determined under the said Act at the point when duties of customs are levied on the said goods under the Customs Act, 1962. The integrated tax on goods shall be in addition to the applicable Basic Customs Duty (BCD) which is levied as per the Customs Tariff Act. In addition, GST compensation cess, may also be leviable on certain luxury and demerit goods under the Goods and Services Tax (Compensation to States) Cess Act, 2017.

The Customs Tariff Act, 1975 has accordingly been amended to provide for levy of integrated tax and the compensation cess on imported goods. Accordingly, goods which are imported into India shall, in addition to the Basic Customs duty, be liable to integrated tax at such rate as is leviable under the IGST Act, 2017 on a similar article on its supply in India. Further, the value of the goods for the purpose of levying integrated tax shall be, assessable value plus Customs Duty levied under the Act, and any other duty chargeable on the said goods under any law for the time being in force as an addition to, and in the same manner as, a duty of customs.

The value of the imported article for the purpose of levying cess shall be, assessable value plus Basic Customs Duty levied under the Act, and any sum chargeable on the goods under any law

for the time being, in force as an addition to, and in the same manner as, a duty of customs. The integrated tax paid shall not be added to the value for the purpose of calculating cess.
GST entities in India importing goods through an E Commerce website need to factor in the impact of GST if any.

## Online Information Services

IGST under Section 2(17) defines "online information and database access or retrieval services" (OIDAR)[xlv] as a category of service. It means a service provided through the medium of internet and received by the recipient online without having any physical interface with the supplier of such services. E.g. downloading of an e-book online for a payment would amount to receipt of OIDAR services by the consumer downloading the e-book and making payment.
These are services include

- (i) advertising on the internet;
- (ii) providing cloud services;
- (iii) provision of e-books, movie, music, software and other intangibles through telecommunication networks or internet;
- (iv) providing data or information, retrievable or otherwise, to any person in electronic form through a computer network;
- (v) online supplies of digital content (movies, television shows, music and the like);
- (vi) digital data storage; and
- (vii) online gaming;

The need for this taxation arises because the nature of OIDAR services are such that it can be provided online from a remote location outside the taxable territory. A similar service provided by an Indian Service Provider, from within the taxable territory, to recipients in India would be taxable.
Further, such services received by a registered entity in India would also be taxable under reverse charge. The overseas suppliers of such services would have an unfair tax advantage should the services provided by them be left out of the tax net.

At the same time, since the service provider is located overseas and may not be having a presence in India, the compliance verification mechanism become difficult.
The government has introduced a simplified scheme of registration for such service providers under GST.

The place of supply of online information and database access or retrieval services shall be the location of the recipient of services.

- Explanation.—For the purposes of this sub-section, person receiving such services shall be deemed to be located in the taxable territory, if any two of the following non-contradictory conditions are satisfied, namely:—

  (a) the location of address presented by the recipient of services through internet is in the taxable territory;

  (b) the credit card or debit card or store value card or charge card or smart card or any other card by which the recipient of services settles payment has been issued in the taxable territory;

  (c) the billing address of the recipient of services is in the taxable territory;

  (d) the internet protocol address of the device used by the recipient of services is in the taxable territory;

  (e) the bank of the recipient of services in which the account used for payment is maintained is in the taxable territory;

  (f) the country code of the subscriber identity module card used by the recipient of services is of taxable territory;

  (g) the location of the fixed land line through which the service is received by the recipient is in the taxable territory.

On supply of online information and database access or retrieval services by any person located in a non-taxable territory and received by a non-taxable online recipient, the supplier of services located in a non-taxable territory shall be the person liable for paying integrated tax on such supply of services:

- Provided that in the case of supply of online information and database access or retrieval services by any person located in a non-taxable territory and received by a nontaxable online recipient,
- an intermediary located in the non-taxable territory, who arranges or facilitates the supply of such services, shall be deemed to be the recipient of such services from the supplier of services in non-taxable territory and supplying such services to the non-taxable online recipient except when such intermediary satisfies the following conditions, namely:—
- (a) the invoice or customer's bill or receipt issued or made available by such intermediary taking part in the supply clearly identifies the service in question and its supplier in non-taxable territory;
- (b) the intermediary involved in the supply does not authorise the charge to the customer or take part in its charge which is that the intermediary neither collects

or processes payment in any manner nor is responsible for the payment between the non-taxable online recipient and the supplier of such services;

- (c) the intermediary involved in the supply does not authorise delivery; and
- (d) the general terms and conditions of the supply are not set by the intermediary involved in the supply but by the supplier of services.

A "non-taxable online recipient" means any Government, local authority, governmental authority, an individual or any other person not registered and receiving online information and database access or retrieval services in relation to any purpose other than commerce, industry or any other business or profession, located in taxable territory.

**Examples**

The inclusive part of the definition of OIDAR services are only indicative and not exhaustive. To determine if a particular service is an OIDAR service, the following test can be applied.

| **Service** | **Mediation of IT** | **Impossible to avoid IT** | **OIDAR Service** |
|---|---|---|---|
| Pdfdocument manually emailedby provider | Yes | No | No |
| Pdfdocument automatically emailedby provider's system | Yes | Yes | Yes |
| Pdfdocument automatically downloaded fromsite | Yes | Yes | Yes |
| Stock photographs availablefor automatic download | Yes | Yes | Yes |
| Onlinecourse consistingof pre-recorded videosand downloadable pdfs | Yes | Yes | Yes |
| Onlinecourse consistingof pre-recorded videosand downloadable pdfsplus | Yes | No | No |
| Individually commissioned contentsentin digitalform e.g., photographs, reports, | Yes | No | No |

**Indicative List of OIDAR Services**

1. Websitesupply,web-hosting,distance maintenance ofprogrammesandequipment;

(a) Websitehostingandwebpagehosting;

(b)automated, online and distancemaintenance of programmes;

(c) remote systems administration;

(d) online data warehousing where specific data is stored and retrieved electronically;

(e) online supply of on-demand disc space.

2. Supply of software and updating thereof;

(a) Accessing or downloading software (including procurement/accountancy programmes and anti- virus software) plus updates;

(b) software to block banner adverts showing, otherwise known as Banner blockers;

(c) download drivers, such as software that interfaces computers with peripheral equipment (such as printers);

(d) online automated installation of filters on websites; (e) online automated installation of firewalls.

3. Supply of images, text and information and making available of databases;

(a) Accessing or downloading desktop themes;

(b) accessing or downloading photographic or pictorial images or screensavers;

(c) the digitised content of books and other electronic publications;

(d) subscription to online newspapers and journals;

(e) weblogs and website statistics;

(f ) online news, traffic information and weather reports;

(g) online information generated automatically by software from specific data input by the customer, such as legal and financial data, (in particular such data as continually updated stock market data, in real time);

(h) the provision of advertising space including banner ads on a website/web page;

(i) use of search engines and Internet directories.

4. Supply of music, films and games, including games of chance and gambling games, and of political, cultural, artistic, sporting, scientific and entertainment broadcasts and events;

(a) Accessing or downloading of music on to computers and mobile phones;

(b) accessing or downloading of jingles, excerpts, ringtones, or other sounds;

(c) accessing or downloading of films;

(d) downloading of games on to computers and mobile phones;

(e) accessing automated online games which are dependent on the Internet,or other similar electronic networks, where players are geographically remote from one another.

(5) Supply of distance teaching.

(a) Automated distance teaching dependent on the Internet or similar electronic network to function and the supply of which requires limited or no human intervention, including virtual classrooms, except where the Internet or similar electronic network is used as a tool simply for communication between the teacher and student;

(b) workbooks completed by pupils online and marked automatically, without human intervention,

## Emerging E Commerce Policy

In February 2019, Government of India came up with a draft E Commerce policy[xlvi] which is expected to have a strong impact on the industry. The policy was released for public comments and may be taken up for implementation in the later part of the year. However, this indicates the direction in which the policy makers are looking at and students need to study this document and how it evolves.

Some of the strategies suggested in the policy include the following:

1. Legal and Technological framework to be created for restricting cross border flow of data from IoT devices and E-Commerce platforms, social media, search engines etc. The policy states that even with "Consent" of the data subject, the data shall not be shared with foreign business entities or Governments. (This will have to be resolved with the data protection act under consideration, namely the Personal Data Protection Act 2018 or PDPA 2018).
2. Policy also states that suitable framework will be developed for sharing of community data that serves larger public interest. This means that "Big Data" generated in the e-commerce activity will be made available to indigenous data research agencies. A mild suggestion for a "Data Authority" is also made in this regard though how this will work with the Data Protection Authority as envisaged under PDPA 2018.
3. Policy envisages that steps will be taken to develop capacity for data storage in India. This includes domestic alternatives to foreign based clouds and e-mail facilities. Hopefully incentives would be available for a health development of data storage business. This policy goes with the "Digi Locker Scheme" alreadyin operation and the proposed Data Fiduciaries under PDPA 2018. If a synergy is brought between these three aspects, there would be an entirely new business opportunity that would spring forth in India.
4. In addition to the FDI regulation of market places already in place, it is proposed that product shipments from other countries to India should be channelized through customs route. In this process an integrated system to connect Customs, RBI and India Post is to be developed.

5. The policy also sets an ambitious plan to require all E Commerce sites and apps available for download in India, must have a registered business entity in India as "Importer on record" or as an entity through which all imports are routed.
6. The policy expects several measures aimed at anti piracy/anti-counterfeiting as well as measures to protect the misuse of trademarks. It is proposed that a body of industry stakeholders will be created that shall identify "Rogue websites" which shall be listed as "Infringing websites list". The ISPs including search engines will be required to block access to such sites.
7. The policy reiterates some of the measures like the provision of details of the "Grievance Redressal officer" of the E Commerce entity on the website and a system of grievance redressal.
8. The E Commerce platform will also be required to ensure that prohibited items shall not be sold on their platform.
9. Policy also envisages an Inter-Ministerial Group of Secretaries to ensure that multiple regulatory authorities work in collaboration, consider appropriate changes for Expoert Promotion through e-Commerce adoption of better international taxation systems etc.

Thus the new policy may usher in a new era of E Commerce in the country and we may await its finalization and how it is implemented.

**Concluding Remarks**

Taxation issues in Cyber Space is an extension of the taxation principles applicable to physical society. The fact that a person is either a resident or a non resident, determines most of the aspects of taxation. In terms of the taxation related to trade, apart from the residential status, the mode in which the taxable revenue was generated could also affect whether a person has to pay a tax and if so on what income etc. There are many conceptual issues on which conflicting interpretation may arise in respect of digital products. The Indian system tries to address these through the NRI taxation scheme, GST scheme and further through E Commerce guidelines on FDI and other related issues. This is a developing and students need to watch for further information over the resources available on the Internet.

**References:**


1. https://www.mea.gov.in/Images/pdf1/S7.pdf
2. https://www.incometaxindia.gov.in/Pages/i-am/non-resident.aspx?k=Introduction[1]
3. http://www.cbic.gov.in/resources//htdocs-cbec/gst/51_GST_Flyer_Chapter42.pdf;jsessionid=1ED151DA92373BD69A16E314BC731BED
4. https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

*P.S: Since the entire content has been drawn from dynamic resources in the Internet and most of the published books may not contain updated information, no reference to books have been provided. In the changing world of technology, the value of judicial precedence is also low. Every judicial decision has to be seen with the law and technology as applicable to a case on hand and hence excessive reliance on case laws in areas of E Commerce is better avoided. Hence it is recommended that students develop an insight into the legal interpretation from out of the current developments they may observe on the resources available on the Internet after due filtration for the credibility of the information.*

# Chapter V: International Taxation in E-Commerce

**Syllabus:** Existing framework- permanent establishment-virtual PE, Base Erosion and Profit Shifting (OECD) Action Plan- Tax Challenges Arising from Digitalisation, Public Consultation Document- User Participation proposal, marketing intangibles proposal, significant economic presence, Double Taxation, Role of ISPs, OECD initiatives in International Taxation.

**Learning Objectives:** In this chapter the students would be exposed to the international taxation systems in E Commerce and in particular the OECD guidelines, the Double Tax Avoidance treaties, the Base Erosion and Profit shifting Action Plan etc.

## Basics of International Taxation

In the previous chapter we have discussed several aspects of Taxation in India. In the process of discussion on E Commerce, we have also discussed some aspects of incidence of taxation in international transactions that arise out of E Commerce or by the reason of an assesse being a Non Resident.

In this chapter, we shall discuss the concept of International incidence of Tax, approach of the Double Tax Avoidance Treaties and the concept of Tax Havens as we go a little deeper into the topic of international taxation.

## Principles of International Taxation

International Taxation arises when either the entity which is the subject of taxation or the transaction itself has multi national spread. Since Taxation is considered as a territorial right of a Government to collect revenue, in cross border transactions or existence, multiple Governments may be interested in taxing the transactions at different levels. This may result in unfair taxation which needs to be corrected by the respective Governments so that international trade may not be impeded.

The basic principles of international taxation are not different from domestic transaction. They include “Simplicity”, “Neutrality”, “Stability” and “Flexibility”. The three broad methods of taxation namely Income, Wealth and Consumption also apply for International Taxation.
The difference between domestic and international transaction however lies in the fact that the interests of two different jurisdictions are involved and each would like to preserve their right to tax and have the freedom to implement them without hindrance from another country. In the process, laws are often made but are not implemented effectively. Countries try to resolve their differences with international agreements and try to protect their rights.

The issues that come for discussion in international taxation is whether a subject is liable for taxation in Country A or B or both? Whether a particular transaction is subject to taxation in Country A or B or both?

**Residence Consideration**

Some countries tax individuals and Corporations on the basis of their place of residence.
As we have already in some detail in the previous chapter, in India, the taxation status could be Resident, Non Resident or Resident but Not ordinarily resident. The distinction is on the basis of the period upto which a person is in India in a given year. In case of Corporates, the registration of the company in a particular country or establishment of a permanent management and operational structure in a country may determine its taxation status. Based on the taxable status, income would also be classified as “domestic income” or “Global Income” and the calculation of tax liability may accordingly be defined differently.

It may be noted that some countries may not have personal income tax and in some the rates may be different from the rates in India so that an arbitratge opportunity may be available to reduce the burden of taxation. If one of the countries presents a tax haven, then assesses may prefer to reduce the profit recorded in India and retain more of the profit in the tax haven itself. Hence where possible entities may resort to transfer pricing in such a manner that less income is shown in India.

In USA, taxes are levied on its citizens as residents, and provides lengthy, detailed rules for individual residency of foreigners, covering, periods establishing residency (including a formulary calculation involving three years), start and end date of residency and exceptions for transitory visits, medical conditions, etc.

The United Kingdom, prior to 2013, established three categories: non-resident, resident, and resident but not ordinarily resident. From 2013, the categories of resident are limited to non-

resident and resident. Residency is established by application of the tests in the Statutory Residency Test.
Switzerland residency may be established by having a permit to be employed in Switzerland for an individual who is so employed.
Territorial systems usually tax local income regardless of the residence of the taxpayer. The key problem argued for this type of system is the ability to avoid taxation on portable income by moving it outside of the country. This has led governments to enact hybrid systems to recover lost revenue.

**Citizenship**

In the vast majority of countries, citizenship is completely irrelevant for taxation. Very few countries tax the foreign income of non resident citizens in general.

United States taxes the worldwide income of its nonresident citizens using the same tax rates as for residents. To mitigate double taxation, nonresident citizens may exclude some of their foreign income from work from U.S. taxation, and take credit for income tax paid to other countries, but they must file a U.S. tax return to claim the exclusion or credit even if they result in no tax liability.
Some countries tax based on citizenship only in limited situations.

For example, France taxes its citizens who move to Monaco as residents of France, according to a treaty signed between the two countries in 1963. However, those who already lived in Monaco since 1957, as well as those who were born in Monaco and have always lived there, are not subject to taxation as residents of France.

Italy continues taxing its citizens who move from Italy to a tax haven as residents of Italy, unless they demonstrate that they no longer have any ties to Italy.

Sweden continues taxing its citizens (as well as foreigners who lived there for at least ten years) who move from Sweden to another country as residents of Sweden, for the first five years after moving there, unless they demonstrate that they no longer have essential connections to Sweden. After this period, they are no longer considered residents of Sweden for tax purposes.

Each country may for their own historical or ideological reasons adopt different taxation rules for their citizens and non citizens.

**Corporate Status**

As in India countries also distinguish their taxation practices based on whether the assesse is an individual or a Company.

Many countries allow for fiscal transparency of certain forms of enterprise. For example, most countries tax partners of a partnership, rather than the partnership itself, on income of the partnership.

A common feature of income taxation is imposition of a levy on certain enterprises in certain forms followed by an additional levy on owners of the enterprise upon distribution of such income.

For example, the U.S. imposes two levels of tax on foreign individuals or foreign corporations who own a U.S. corporation. First, the U.S. corporation is subject to the regular income tax on its profits, then subject to an additional 30% tax on the dividends paid to foreign shareholders (the branch profits tax). The foreign corporation will be subject to U.S. income tax on its effectively connected income, and will also be subject to the branch profits tax on any of its profits not reinvested in the U.S.

**Income Source**

Another important criteria in which countries may differ in taxation could be on the way the sources of income are treated for taxation purpose.

For example, Hong Kong does not tax residents on dividend income received from a non-Hong Kong corporation. Source of income is also important in countries that grant credits for taxes of other jurisdictions.

The manner of determining the source of income is generally dependent on the nature of income. For example, Income from the performance of services (e.g., wages) is generally treated as arising where the services are performed.[ Financing income (e.g., interest, dividends) is generally treated as arising where the user of the financing resides. Income related to use of tangible property (e.g., rents) is generally treated as arising where the property is situated. Income related to use of intangible property (e.g., royalties) is generally treated as arising where the property is used. Gains on sale of realty are generally treated as arising where the property is situated.

**Tax Havens**

Tax Haven is a term to describe a country or a territory within a country which provides some substantial tax incentives to registered companies and/or to attract settlement of such business

entities in their territory. In some cases such entities are provided complete exemption of tax on income.
In most cases there may be a very low incidence of tax sufficient to attract companies to set up businesses.

Tax haven status benefits the host country as well as the companies and individuals maintaining accounts in them. Tax haven countries benefit by drawing capital to their banks and financial institutions, which can form the foundation of a thriving financial sector. Individuals and corporations

**Withholding tax**

A withholding tax, or a retention tax, is an income tax to be paid to the government by the payer of the income rather than by the recipient of the income. The tax is thus withheld or deducted from the income due to the recipient. In most jurisdictions, withholding tax applies to employment income.
The TDS system in India as well as the Equalization levy for E Commerce are types of Withholding tax.

Withholding tax is applicable in case of payments done to non-resident individuals. So when a liability to carry out payment to a Non-Resident Indian arises the payer is liable to deduct the tax at source. As per the Income Tax Act under section 195, it is obligatory for the payee, who is the person responsible to make payment, to deduct the tax at the time of payment or at the time of crediting the payment in the account of the Non-Resident Individual.

Such payment is taxable only on the chargeable income i.e. the chargeable payment to be done to the non-resident individual. Only the person making payment for the services received by him from a non-resident individual can deduct withholding tax. And it is obligatory on the part of the payee to deposit the deducted withholding tax with the government. The withholding tax is to be deducted as per the prescribed rates stated in the act or at the rates mentioned in the Double Taxation Avoidance Agreement whichever is beneficial for the non-resident individual.

There are two major benefits related to the charging of withholding tax. They are

1. The first and most important beneficiary of charging withholding tax is the government. The primary benefit is that the government gets early generation of revenue.
2. The second benefit of charging withholding tax is that every transaction is under radar and scrutiny. Under withholding tax, it is the liability of the payee to deduct the tax and deposit the same with the government. So as the liability is on the payer it is imperative

on the part of the payer to ensure that the amount of tax charged is correct and that the same correct amount is being deposited with the government in their account.

## Permanent Establishment

We have already discussed the concept of Permanent Establishment (PE) in the previous chapter. In the case of a Citizen, he is liable for taxation in the country of his citizenship but is provided exemptions if he is an Non Resident. Similarly, PE concept incorporates the rules to determine under what circumstances a Company would be liable for taxation either in the country where it is registered or elsewhere.

The concept of PE is evolving to keep pace with the changing business environment.

In the OECD Model Tax Convention,[xlvii] essentially three types of PEs can be construed

a) A fixed place of business PE
b) A construction or project PE, which is a special subset of the fixed place of business PE, with different requirements and
c) An agency PE, through the actions of a dependent agent .

The UN Model Tax Convention, which gives greater consideration to developing countries, adds what is known as a service PE in article 5(3)b.

Some countries, such as Saudi Arabia, have been trying to extend the concept of service PE into a virtual service PE.

Under Article 5, a permanent establishment (PE) is defined a fixed place of business through which the business of an enterprise is wholly or partly carried on.

The term "Place of business" covers any premises, facilities or installations used for carrying on the business whether or not they are exclusively used for that purpose. A place f business may also eist where no premises are available and it simply has a certain amount of space at its disposal, whether owned or rented. A place of business my therefore be constituted by a pitch in a market place, or a certain permanently used area in a customs depot. It may also be contained within the business facilities of another enterprise.

Article 5(4) lists a number of business activities which are treated as exceptions to the general definition laid down in paragraph 1.

Article 5(5) addresses the issue of persons acting on behalf of an enterprise though the enterprise itself does not have a fixed place of business.
Article 5 (8), defines a "Closely related enterprise". It provides that a person or enterprise is closely related if based on the relevant facts, one has contrl of the other or both are under the control of the same persons or enterprises.

As regards Electronic Commerce, location where automated equipment is operated by an enterprise constitutes a permanent establishment in the country where it is situated. The Internet website itself does not constitute a permanent establishment On the other hand the server on which the website is stored or through which it is accessible is a piece of equipment having a physical location and may constitute a fixed place of business.

In the case of websites hosted on an ISP, the servers may owned by a person other than the establishment and may be moved from one location to another . In such a case no "Fixed Place of Business" may arise at the place where the ISP maintains the servers.

But if the servers are owned by the enterprise, then it becomes a fixed place of business.
In case of Cloud Services, an argument similar to the website may be made.

If in such services, the enterprise locates a person on its behalf for maintenance of the servers, a PE may be construed.
Services performed in the territory of a contracting state by an enterprise of the other contracting state are not taxable in the first state if they are not attributable to a permanent establishment situated there in.

**Virtual PE**

It is reported however that the Bengaluru bench of the Income-tax Appellate Tribunal ('the Tribunal') has held that a UAE company ('the taxpayer') had a Service PermanentEstablishment (PE) in India since the tax payer has been furnishing services to the Indian company even without any substantial physical presence of its employees in India (in this case the physical presence of employee was only 25 days in the previous year).

The Ruling carves out a new niche principle of 'Virtual PE' not very much accepted in the global context but very relevant in today's technology era.
This concept however raises some issues according to experts.

(a) If principles laid down by the Tribunal are to be rigorously applied, then, provision of services by a foreign entity in their home country through employees / personnel will be

included for Service PE purposes, so will virtually all income generating activities of the foreign entity which are rendered from outside India be taxable in the source country under concept of an implied service PE?

(b) In modern digital era, where services are furnished through digital modes, place of provision / furnishing of services should be the place where such aids of communication have been initiated (in present case home country of the taxpayer). If this interpretation of the Tribunal is carried forward, will all services rendered in the digital form should arise in the source country and be taxable therein?

Further, traditional PE rules may not be sufficient to address virtual presence. In absence of specific rules (like that in Saudi Arabia, Israel), it is not clear how digital services would be brought to tax in India except for "Equalisation levy" which presently covers advertising services.

This may require a judicial review in the future to provide some clarity.

## Base Erosion and Profit Shifting (BEPS) Action Plan[xlviii]

OECD (Organization of Economic Cooperation and Development, issued its Action Plans (APs) on "Base Erosion and Profit Shifting" (BEPS), in November 2015. This action plan, created in response to a request by the G20, identifies a set of domestic and international actions to address the problems of base erosion and profit sharing.

The AP recognized that in most cases, existing domestic law and treaty rules governing the taxation of cross border profits provide satisfactory resolution of differences between different countries. BEPS relates chiefly to instances where the interaction of different tax rules leads to double non taxation or less than single taxation.

BEPS is also relevant when arrangements that achieve no or low taxation shift profits away from the jurisdictions where the activities creating those profits take place.

The main concern that the BEPS recognized was that "Gaps in the interaction of different tax systems, and in some cases application of bilateral tax treaties result in income from cross-border activities go untaxed anywhere or be only unduly lowly taxed".

The growth of digital economy adds to the concerns of fair international taxation. BEPS recognized that the digital economy is charecterized by reliance on intangible assets, massive use of data, use of multi sided business models capturing value from externalities generated by free products and difficulty of determining the jurisdiction in which value creation occurs.

It is in this context that OECD concluded that if the AP fails to develop effective solutions in a timely manner, some countries may take unilateral action for protecting their tax base resulting in avoidable uncertainty and unrelieved double taxation. The AP was therefore focussed on restoring both source and residence taxation in case of cross border income which would otherwise go untaxed.

The G 20 finance ministers therefore called on the OECD to develop an action plan to address BEPS issues in a coordinated and comprehensive manner. Specifically, it was expected to provide countries with domestic and international instruments that will better align rights to tax with economic activity.

The document identified 15 Action Plans on different aspects of concern to BEPS. A quick list of the 15 Action plans are

1. Address the tax challenges of the digital economy
2. Neutralize the effects of hybrid mismatch arrangements
3. Strengthen CFC (Controlled Foreign Company) Rules
4. Limit Base erosion via interest deductions and other financial payments
5. Counter harmful tax practices more effectively, taking into account transparency and substance
6. Prevent Treaty Abuse
7. Prevent the artificial avoidance of PE Status
8. Assure that transfer pricing outcomes are in line with value creation.- Intangibles
9. Assure that transfer pricing outcomes are in line with value creation -Risks and capital
10. Assure that transfer pricing outcomes are in line with value creation -Other high risk transactions
11. Establish methodologies to collect and analyse data on BEPS and the actions to address it
12. Require taxpayers to disclose their aggressive tax planning arrangements
13. Re examine transfer pricing documentation
14. Make dispute resolution mechanisms more effective
15. Develop a multilateral instrument.

The benefit through tax savings resulting from rates ranging from zero to the low single digits versus higher taxes in their countries of citizenship or domicile.

The list of tax haven countries includes Andorra, the Bahamas, Belize, Bermuda, the British Virgin Islands, the Cayman Islands, the Channel Islands, the Cook Islands, Hong Kong, The Isle of Man, Mauritius, Lichtenstein, Monaco, Panama, and St. Kitts, and Nevis.

Some of the tax haven countries may attract investors by providing assurance on secrecy of their operations from other countries. As a result, they may attract not only genuine businessmen but also fugitives of law or hard core criminals.

Some of the tax havens may not require "Residency" in the territory and most entities may simply be "Book Entries".

It is therefore an eternal fight between sovereign countries and the tax haven administrations to ensure that the benefits are not misused by fraudsters and criminals trying to hide their criminal wealth or run away from their home countries after committing tax frauds.

Tax Havens should not be instruments of "Tax Avoidance". While some small island economies which may not have enough natural resources to develop a domestic manufacturing economy may require strategies to attract global business houses to use its territory for trading and finance activities so that the country benefits by the development of the ecosystem, there are many countries whose intention is just to profit from the provision of safe parking space for ill gotten wealth.

Singapore is one example of how the country can prosper through genuine trade activities but there are many other countries who provide easy citizenship for fugitives of law just to attract investment of any hue and colour.

E Commerce and Crypto Currencies have enabled such countries to also emerge as popular tax havens.

**Treaty Law Regime**

In order to avoid double taxation in cross border transactions, countries rely heavily on "Double Tax Avoidance Agreements " (DTAA) under bilateral or multi lateral treaties between countries. DTAA is a tax treaty signed between two or more countries to help taxpayers avoid paying double taxes on the same income. A DTAA becomes applicable in cases where an individual is a resident of one nation, but earns income in another.

DTAA is meant to remove the anomalies that may arise between the trade transactions of two countries due to the difference in the taxation methodologies used by them. It is normally meant to promote trade and economic relations between the two countries by providing some special privileges to such transactions.

India has DTAA with many countries. An indicative list of such countries is given below.

Below is a list of countries with which India has signed a Double Tax Avoidance Agreement:

Mauritius: Comprehensive Agreements

South Africa: Comprehensive Agreements

Afghanistan: Limited Agreements

USA: Intergovernmental agreement to Improve International Tax Compliance and to Implement FATCA

Australia: Comprehensive Agreements

Austria: Comprehensive Agreements

Bahamas: Tax Information Exchange Agreement (TIEA)

Bahrain: Tax Information Exchange Agreement (TIEA)

Bangladesh: Comprehensive Agreements

Belgium: Comprehensive Agreements

Canada: Comprehensive Agreements

Cayman Islands: Tax Information Exchange Agreement (TIEA)

China: Comprehensive Agreements

Denmark: Comprehensive Agreements

France: Comprehensive Agreements

Germany: Comprehensive Agreements

New Zealand: Comprehensive Agreements

Norway: Comprehensive Agreements

Russia: Comprehensive Agreements

Saint Kitts and Nevis: Tax Information Exchange Agreement (TIEA)

Saudi Arabia: Comprehensive Agreements

Singapore: Comprehensive Agreements

UAE: Comprehensive Agreements

UK: Comprehensive Agreements

USA: Comprehensive Agreements

The detailed provisions of each agreement and their impact on individuals may differ.

## Double Taxation – Models for Double Taxation Treaties

The issue of Double Taxation arises with the growth of commerce and the movement of goods, services and manpower across the national boundaries. Hence many instances arise where the income belongs to one national domain while the earner belongs to another. The conflicting claims to that income is what results in Double Taxation. If a country wants to improve it's economic standing in the international scene, then interstate commerce is what is to be encouraged, and this will occur only when the tax regimes are flexible enough to accommodate the problems of foreign incomes and evolve a system which is in the best interests of the taxpayer. Otherwise if interstate commerce proves to be burdensome to the taxpayer, then other undesirable repercussions may result in the form of tax-avoidance and evasion, which is but a loss to the exchequer.

Hence at the international level various efforts have been at work to evolve a tax structure, which is in the interest of interstate commerce and its just taxation.

Double Tax avoidance agreements are aimed at eliminating double taxation. They do not grant taxation jurisdiction to any Government nor take away any jurisdiction already existing.

The various models of double taxation agreements are but an expression of these efforts.

## The Evolution of Double Taxation Treaties

Avoidance can be achieved either unilaterally or bilaterally. Double Taxation can be avoided unilaterally if one of the states involved withdraws its tax claim. This practice is developed under Anglo-American Law whereby the state of residence if it is not the state of source allows

1) A tax credit for the tax levied in the state of source upto an amount equivalent to its own tax charge
2) Lumpsum to be deducted instead of exact equivalent of the foreign tax paid310.
3) Allowance of exemptions

Then bilateral treaties and agreements for avoidance of double taxation came into vogue by the end of 19th century. Though to start with only federally related or closely allied states were involved, following the World War 1 an extensive treaty network developed in Central Europe. The League of Nations contributed substantially to an assimilation of existing bilateral treaties and to the development of Uniform Model Treaties. The efforts of the OECD to develop a system of avoidance of Double Taxation picked up from where the League had left off. The OECD Committee on Fiscal Affairs (1956) drafted a complete model treaty and appended an official commentary to it in 1963. The OECD Council recommended member states to adopt the model

treaty format in Double Taxation Agreements signed by them. With the passage of time a number of changes were made to the OECD MC.

The opposing model shaped more according to the special interests of developing countries and was adopted in 1971 by the member states of the Andean Group, viz., Bolivia, Chile, Ecuador, Columbia, Peru and Venezuela.

The UN published another model treaty intended to serve the interests of the developing countries in 1980. This treaty was the culmination of the efforts of the ECOSOC over a period of 10 years. Its structure corresponds to the OECD MC but its content diverges in certain important aspects.

The US model is another model which is different from other models. U.S. Government has envisaged several kinds of tax planning and tried to curb the tax planning. It has also tried to protect its own interest qua the other Contracting State.

## The OECD Model of Double Taxation

The Organization for European Economic Cooperation (OEEC) worked right from the beginning for a convention for the avoidance of Double Taxation with respect to taxes on income and capital. The work of the OEEC lasted from 1948 to 1961 in this direction after which it was taken over by the Organization for Economic Cooperation and Development (OECD). The work of the organization consisted mainly of bringing out model drafts, which were followed by its members in signing double taxation agreements with each other and also third parties. The OECD's membership was characterized as one of the developed countries. The first of such model draft treaties prepared by the OECD was in 1963, which has been later revised from time to time.

The important features of the OECD Model can be summed up as, those benefiting the developed world rather than the developing. The Convention applies to all taxes on income and capital irrespective of the authority on behalf of which the taxes are imposed. It applies to residents of the contracting states. The kinds of taxes covered by the Convention are taxes on income, taxes on capital, taxes on gains from alienation of movable or immovable property, taxes on total amount of wages or salaries, taxes on capital appreciation. There are two methods of double taxation relief provided under the Convention, exemption method and credit method. The OECD Model gives primacy to the residence principle. The Convention while committing to the principle of double taxation avoidance ensures that the tax bases of the contracting parties are not substantially reduced, by commitments on an international plane.

## The UN Model for Double Taxation

As opposed to the OECD model the UN model on double taxation avoidance agreements developed. In 1968 the UN Secretary General set up an adhoc group of experts on the tax treaties between the developed and developing countries. The experts hailed mostly from the developing world, namely Latin America, Africa and Southeast Asia and the Far East, though they were experts from UK and US also. All these experts worked in their personal capacity and not as the representatives of their respective countries.

This group of experts drafted the UN Model Convention on Double Taxation Avoidance and Relief. This model convention was published in 1980. This model has so to say come to be used predominantly in the tax treaties between the developed and the developing countries. All the tax agreements that India has concluded in the recent past have been based on this model with suitable modifications made for the Indian conditions.

The following can be said to the main features of the UN model. This model represents a compromise between the source and the residence principle. It gives more weightage to the source principle than the OECD model. Its provisions are based on the recognition of the contribution of source countries in the process of income generation. The model recommends that the country of residence give a tax relief equivalent to the foreign tax paid. Taxation of income from foreign capital would have to take into account expenses allocable to the earning of the income so that such income would be taxed on net basis. The idea of the Convention is to provide an atmosphere conducive for investments, taxation should not be so high as to discourage investment. Income from a foreign source may be shared with the country providing the capital or technology. The methods of double taxation relief provided under the convention resemble the OECD model. In fact most of the provisions of both the Models are similar, except for certain provisions, like for example the permanent establishment concept where the UN model is more elaborate and comprehensive.

## Legal Framework for Double Taxation Treaties

The objective of Double Taxation Treaties is to give a general idea as to the form, content and basic framework for double taxation treaties. In the process various issues are discussed, which pertain to their conclusion, implementation, interpretation, comparison with rules of international law, both private and public etc.

## A. Conclusion of Double Taxation Treaties and their implementation in the domestic sphere.

Double Taxation Treaties are 'International agreements'. Their creation and consequences are determined according to the rules contained in the Vienna Convention on the Law of Treaties.

All treaties are preceded by negotiations. The Executive generally conducts the negotiations. During the negotiations a treaty draft is prepared initially only in one language. A 'final protocol' may also be separately prepared for negotiation results that are less important or have effects on only one of the parties involved. And it is distinguished from the main text. At the conclusion of the negotiations the leaders of both delegations authenticate two copies of the treaty by initialling at each page.

The negotiation phase is followed by the conclusion of the treaty. Mere initialling does not actually commit the contracting state to conclude the treaty. A commitment to that albeit a limited one does not come into operation until the text of the treaty is signed. By signing the treaties, the contracting parties commit themselves to initiate the procedures necessary under domestic law for the binding conclusion of the treaty. Thus the signing of the treaty does not constitute a binding commitment to conclude it.

In Parliamentary democracies the Executive must ordinarily obtain the consent of the Parliament to conclude important agreements. The absence of parliamentary consent where necessary, would constitute a clear and fundamental infraction and would pursuant to A. 46(2) of the Vienna Convention cause the treaty to be invalid in International Law.

As regards US, the Secretary of State formally submits the treaty to the President who in turn submits it to the Senate accompanied with a Presidential message. The senate Committee on Foreign Relations then considers it. The Senate is then asked to pass a resolution giving its advice and consent. The final vote on the resolution of ratification requires 2/3rd majority of the Senators present for approval. The Constitution does not prescribe a quorum. Then the treaty is returned through proper channels to the President for ratification.

In UK where parliamentary consent is not required for conclusion of a treaty, the treaty becomes applicable internally only when a special law is passed to this effect by the parliament after the treaty enters into force under International Law.

In Germany internal applicability of the treaty generally is achieved through enactment of implementing legislation, as provided under A.59, Abs. 2 Grundgesetz (Federal Constitution).

Under the Dutch Constitutional Law, the treaty becomes applicable domestically at the same time as it enters into force internationally, reflecting the monist theory of International Law321.

For the purposes of International Law a treaty comes into existence upon the declaration of consent by both contracting states. The method by which the contracting states declare their consent is left to them. Important treaties however shall be concluded and effected only through ratification. Ratification however is distinguished from parliamentary consent, one is the act of the Executive while the other is that of the Legislature.

**B. Double Taxation Treaty Rules and International Law of Treaties**

The point at which a treaty enters force internationally and the point at which it becomes applicable under the domestic law must be distinguished from the point at which material consequences of the treaty begin to take effect, or in other words, the taxable period or the date at which taxation shall be limited by the treaty. Usually the initiation of treaty effects is established by explicit treaty rules. In general the material effects of a treaty apply retrospectively. Through the mandate of the legislature treaties in most countries most states obtain the same authority as internal law.

**C. Structure and Application of Double Taxation treaties**

Generally treaty models are structured and organized into 7 chapters. Chapters 1 & 2 deal with requirements for application of the treaty, i.e. the scope of the Convention and definitions of the treaty terms etc. Chapter 3 is the most important of all, as contains the distributive rules regarding income taxes. Chapter 4 contains the distributive rules for capital taxes. Chapter 5 provides for additional legal consequences supplementing the rules of chapters 3 & 4. Chapter 6 contains additional provisions regarding non- discrimination. Chapter 7 contains provisions, which regulate the entry into force and the termination of the treaty. This broadly is the structure of the Double Taxation Treaty models.

Distributive rules in Chapter three and their content are of major interest at present. As regards their content different types can be distinguished.

1) Rules referring to income from the certain activities – there are four such activities.
   (i) business
   (ii) independent personal services
   iii) dependent personal services
   (iv) agriculture and forestry
2) Rules referring to income from certain assets.
   (i) dividends
   (ii) interest
   (iii) royalties
   (iv) immovable property

3) Rules referring to capital gains.

4) Residuary rule referring to income not dealt with in the foregoing three categories.

**D. Interpretation of Double Taxation Treaties**

International agreements like domestic law require interpretation. A need for interpretation arises from a difference of opinion between two countries. Either the countries may resolve this problem by interpreting it themselves or they may subject themselves to the jurisdiction of the ICJ. In most countries the courts are authorized to interpret treaties.

The interpretation of international agreements even by domestic courts of interpretation cannot be based on the domestic rules of interpretation. In interpreting an International agreement for domestic application, domestic courts must be particular that their interpretations do not conflict with the international obligations of the state in question. For the effective interpretation of international treaties therefore it is necessary to reconcile the various national methods of interpretation.

There are two rules of interpretation, which are applied in the interpretation of international agreements:

1) Lx cause:-the essence of this rule being that every legal rule takes its classification from the legal system to which it belongs. In other words the treaty countries would interpret the terms and expressions in the agreement in accordance with the laws in regard to income which accrues or arises in their respective countries called as source country qualification.

2) LexFori – this means that the each state qualifies the agreement terms according to the requirements of its own domestic law.

Various rules of interpretation have been formulated for the interpretation of International agreements. The text of the treaty is of prime importance, i.e. the ordinary meaning of the terms is to be taken first and interpreted within the framework of the treaty.

In United Kingdom the judge is bound strictly by the wording of the statute, especially so in case of tax law. In principle he is not allowed to consider the intention of the legislators or the equity of the matter. A teleological interpretation (i.e.relating to or involving the explanation of phenomena in terms of the purpose they serve rather than of the cause by which they arise) and even more so a development of the law would be considered as a usurpation of the rights of the legislators. To an extent however the above has to be viewed in the light of new approach of the British Courts in the limited instance of tax avoidance treaties.

In US however the interpretation of tax law became liberal only after the 1930s to be specific after the Supreme Court's decision in White vs. United States.

Canada again follows the British practice of strict interpretation of Tax treaties and avoidance and relief agreements.

According to the French and Belgian practices tax laws are to be interpreted against the fiscal authorities in case of doubt.

There are specific rules, which are applicable to the Interpretation of treaties. Interpretations of treaties should not give rise to obligations, which are not implied by the treaty document itself, as it would mean an additional burden on the country. Nor should it absolve the state from any obligations, as there would be difficulty placing the responsibility for the discharge of that obligation in the International sphere. There are certain factors, which govern and control interpretations:

(a) Statutory text or statutory purpose
(b) Case-law
(c) Authentic interpretation of the text (mostly followed by Germany)
(d) Ordinary meaning of the words of the text
(e) Accompanying materials in the treaty and Technical Explanations

The importance of the above rules of interpretation cannot be over- emphasized but they are essential to avoid disputes in the administration and application of the treaty. Common interpretations and consistent interpretations will solve half of the problems that are encountered in the application of DTAAs.

The two Model Conventions on Double Taxation Avoidance Agreements have many common aspects. Their overall structure is similar, their treatment of various concepts involved in computing tax and establishing tax liability is similar, their dispute resolution mechanisms are similar, their methods of double taxation avoidance are similar etc. Despite this problems of interpretation crop up, because even though the provisions are similar, the manner in which they are interpreted are different. This is probably because they cater to different kinds of contracting states.

The OECD model is more attuned to the interests of the Capital-exporting countries, who want to encompass all the activities of their nationals wherever they may operate and the same time not exempt any non-nationals within their jurisdiction from tax. The developing countries on the other

side need precious capital for the development of their economies, but in the process cannot afford to lose their tax base which is essential for their won revenues. In all these interpretations of provisions of the agreement can establish or remove the legitimate basis for taxation by the domestic taxing authorities.

## Internet Service Providers (ISPs)

The classic definition of ISPs was a technology provider who enabled hosting and transmission of digital information. The traditional ISP was an "Intermediary" and was not a stake holder in the content transmitted. However the increasing complexities in digital presentation of content where content can be stored in multiple devices and dynamically configured and served based on the consumer preferences using user profiles has increased the role ISPs from merely being a technology partner to a business partner.

For example, if the content of a book is available at one hosting site and the content owner is delivering the content based on the "Book Purchase Concept", the ISP can enable the book to be divided into multiple chapters and sold on chapter basis to different interest groups. The moot point here is whether the technology supplier here is merely an ISP like the traditional telecom carrier or is a partner in the process of adding value to the content.

This enhanced role of the ISP as a value adder through aggregation, division or selective collation of content in digital form adds a new dimension of taxation where the ISP's service charges has an element of "Copyright" and nature of a "Royalty" along with the cost of providing the storing and transmission service.

This is also evident in products such as music albums where the album can be divided into individual songs and sold either as a downloadable file or on streaming basis. The purchaser's rights in the information transferred could therefore vary depending on the contract between the parties.
The purchaser of a digitized image could obtain the right to use a single copy of the image, the right to reproduce ten copies of the image for use in a corporate report, the right to reproduce the image for use in an academic work that is expected to have a limited press run, or the right to reproduce the image in a mass-circulation magazine.

Depending on the facts and circumstances, some of these transactions may be viewed as the equivalent of the purchase of a physical copy or copies of the photograph, which would probably not subject the seller to domestic taxation, while other of these transactions would result in

royalty income because they involve payments for the use of or the privilege of using copyrights or similar property in the host-country, which could be taxable there.

Technological developments have necessitated a re-examination of existing income classification principles in light of the ease of perfectly reproducing and disseminating digitized information. Classifying transactions involving digitized information may require a more complex analysis that disregards the form of the transaction – without regard to whether tangible property is involved – in favor an analysis of the rights transferred. This is necessary to ensure neutrality between the taxation of transactions in digitized information and transactions in traditional forms of information, such as hard copy books and movies, so that decisions regarding the form in which information is distributed are not affected by tax considerations.

**Classification of income issues**

Information that can be digitized is generally protected by copyright law. Payments made for the use of or for the privilege of using copyrights are considered royalties. Similarly the Model Tax Conventions define "royalties" as "payments of any kind received as consideration for the use of, or the right to use, any copyright of literary, artistic or scientific work including cinematograph films.." It is not always clear how this definition applies to the sale of digitized information. Yet, it is clear that some of these transactions, such as the electronic purchase of computer programs, are merely substitutes for conventional transactions involving physical objects.

Digitized information also presents unique issues because it can be perfectly reproduced, often by the purchaser. Although someone desiring to purchase ten copies of a bound book will generally purchase ten copies from a publisher, someone wishing to purchase ten copies of an electronic book may simply purchase one copy and acquire the right to make nine additional copies. This transaction might literally be considered to create royalty income, at least in part, since the right to make reproductions is a right reserved to the copyright holder and by allowing a third party to make reproductions, the payment is, at least in part, in consideration for the use of the copyright. However, this transaction may also be viewed as merely a substitute for the purchase of ten copies from the publisher in which the purchaser has undertaken to make the copies, a process which would not be feasible were the information not digitized. Therefore, it is necessary to apply the definition of "royalties" in a manner that takes into account the unique characteristics of digitized information.

**Definition of services income.**

Digitized information may also further complicate existing difficulties in defining services income, as distinguished from sales of goods income or royalties. This distinction is important

for purposes of determining the source of income. Therefore, whether a transaction is deemed to result in sale of goods income, as distinguished from services income, may affect whether such income will be subject to current tax.

The distinction between services income and other types of income is a pervasive issue. For example, in many cases, the distinction between service contracts and other arrangements is unclear. Although many commercial transactions involve elements of both the provision of tangible property and the performance of services, these transactions are generally classified in accordance with their predominant characteristic. For example, a transaction involving the performance of professional services may result in the provision of a letter or other document. The aspect of the transaction consisting of the provision of the tangible property is treated as incidental to the performance of the services. In contrast, if a retail establishment sells a suit to a customer but agrees to make slight alterations as part of the purchase price, the performance of services would be viewed as an integral part of a transaction consisting of the sale of goods.

A further example of where new technologies will blur these distinctions involve transactions in digitized information over the Internet. For example, a reference work, such as an encyclopedia, would previously have been sold only as a set of bound volumes and the sale of the bound volumes would have resulted in sale of goods income, notwithstanding the fact that the cost of printing and binding represented only a fraction of the encyclopedia's value. Now, instead of purchasing a bound volume, a potential purchaser might be able to choose between a set of CD-ROMs and a computer on-line service through which the encyclopedia's content can be accessed. If the customer has a sufficiently fast modem connection, there may be little practical difference between accessing the on-line service and the CD-ROMs on the customer's personal computer. The sale of the CD-ROMs may result in sale of goods income while the classification of the income arising from the on-line service is not clear. The on-line service may result in services income although in some circumstances it could be characterized as a means of distributing copies of copyrighted works351. However, a distinction between sales of goods and services income may still be appropriate in this area taking into account the frequency at which the on-line service will be updated and the fact that the user of the online service must continue to make periodic payments, as contrasted with the fact that the purchaser of the CD-ROM may acquire the right to use the disk in perpetuity for a single payment. It will be necessary to consider the principles to be applied in these situations that will best implement the policy of taxing Cyber commerce.

**Source of Services Income**

Income derived from the performance of labor or personal services only constitutes source income if the person performing the services is physically present in the host country. This is also

a generally accepted international principle. This requirement is based on the view that there is generally an independent, substantial significance to the location where the person rendering the services is located with the result that it is reasonable for that country to tax such services. As travel and communications have become more efficient and less expensive, the relationship between the service provider's location and the service consumer's location has weakened. For example, it is now possible for physicians to remotely diagnose certain diseases through telecommunications links and videoconferencing has eliminated the need for many face-to-face meetings .

These technological developments are generally extensions of existing communications devices. For example, a video conference is likely to be a substitute for a conference telephone call. Although these communications developments may pose some base erosion potential since service providers will find it easier to relocate to low-tax jurisdictions, it may be the case that the base erosion potential is not so significant as to require review of the current general principles of residence- based taxation applicable to services353. In devising rules to source this type of income, it may also be necessary to consider the relationship between the service-provider's physical location and other potential indicia of source, such as the location of a computer server or communications link. Furthermore, to the extent the source of this income is becoming both less meaningful and increasingly difficult to determine, residence-based taxation should necessarily play a larger role.

**Global Services: Allocation of Income and Expenses**

The foregoing section discussed the problem of determining the source of income derived from the performance of services. A related issue arises from increases in global collaboration arising from modern telecommunications. One example is global dealing. As discussed above, global dealing refers to the capacity of financial intermediaries, mainly banks and securities firms, to execute customers' orders and to take propriety positions in financial products in markets around the world and around the clock. Global dealing could not take place without modern computers and communications, which permit a firm's trading position to be transferred around the world as markets open and close. Similarly, certain scientific and engineering projects are now being worked on twenty-four hours a day as laboratories in one region electronically hand-off the project at the end of the day to a laboratory where the day is beginning. This type of global collaboration is expected to increase.

Global collaboration is not a new concept. When goods are manufactured in one country and marketed and distributed in another, the overall transaction could be characterized as global collaboration in the sale of goods. Global collaboration requires transfer pricing and source of

income principles, to correctly allocate the resulting income between the countries involved. Current transfer pricing principles are focused on global collaboration in the manufacture and sale of goods and the creation and transfer of intangibles.

By contrast, global dealing income has been allocated through case- by- case negotiations between the competent authorities involved, although a guidance project on global dealing is currently developing rules of general application. As the ways in which companies collaborate globally to provide services continue to grow, it may be appropriate to consider the creation of general principles for the arm's length allocation of broader categories of services income based on each situation's particular facts. To the extent that capital is not a material income-producing factor in this situation, it would be expected that the place where the component services were performed would be of primary importance in allocating such income.

## OECD Initiatives in International Taxation

The Fiscal Committee of the Organization for European Economic Cooperation (OEEC) which later became OECD, published the first draft instalment of how a model treaty on international taxation may look. This was way back in the 1950s. By 1963 a full draft was ready though it was not until 1977 that the model Double Taxation Convention was published. The 1963 draft was essentially the consolidation of four earlier drafts, the first one of which was published in 1958. This is why we consider that the birth of the OECD model was 1 July 1958.

At the outset, there were fewer than 15 countries involved in drafting the first text; by 1963 the OECD had expanded to 20 countries. It was primarily OECD member countries that contributed to the model, but since 1996 we have opened up the process to non-OECD countries and to business and each year in September, the OECD hosts a global forum of government officials from around the world who work on tax treaties. Today there are more than 3,000 tax treaties in force around the world based on the OECD model. Some 30 non-OECD countries have set out their positions on the model.

The OECD model has established itself as the means of settling the most common problems that arise in the field of international taxation. By enabling a certain harmonisation of double tax treaties, it guides bilateral negotiations and helps settle disputes on a uniform basis. Consider the issue of double taxation.

Since 1991, the Committee on Fiscal Affairs has provided periodic and more timely updates and amendments, without waiting for a complete revision. To date, there have been updates in 1992,

1994, 1995, 1997, 2000, 2003, 2005, 2008,2010,2014 and 2017. The latest version, of July 2017, incorporates the approved Actions developed under the Base Erosion and Profit Shifting (BEPS) project initiated by the G20.

On the E Commerce front, one of the first of the Initiatives of the OECD was a ministerial conference held by member-states at Ottawa in 1998[xlix] on Electronic Commerce, the main focus of the conference being on defining new forms of governance for the Internet. The thrust was on harmonization of laws or co-ordination of enforcement. The specific issues for debate were privacy, consumer protection, governance of domain names and IP addresses. The Conference arrived at a 'Global Action Plan' on the issues of "Consumer Empowerment/ Marketing and Advertising Ethics".

The Global Action Plan says, "Governments should avoid mandating unnecessary standards that could be led by Business." On questions of Internet governance, governments should "continue to support the proposed transfer of administration of the Internet name and address system to the private sector," consistent with protection of "existing trademarks." Governments should "remove existing barriers for workers to share in the new and different employment generated by electronic commerce." On the issue of privacy, governments were encouraged to "recognize the validity and adequacy of effective self-regulation augmented by the use of privacy- enhancing technologies".

## OECD Public Consultation Document

The area of taxation is a dynamic field and changes occur almost every day. The status of International taxation therefore could change continuously. Hence students need to keep themselves abreast of the developments through the resources available on the web. The past developments are important to understand the historical development of the different concepts. However it is important to keep an eye on the future and how the wold of international taxation is shaping up.

Following a mandate by G20 Finance Ministers in March 2017, the Inclusive Framework on BEPS, working through its Task Force on the Digital Economy (TFDE), delivered an Interim Report in March 2018, Tax Challenges Arising from Digitalisation – Interim Report 2018. One of the important conclusions of this report is that members agreed to review the impact of digitalisation on nexus and profit allocation rules and committed to continue working together towards a final report in 2020 aimed at providing a consensusbased long-term solution, with an update in 2019. As a part of this process, a OECD published a public consultation document[l]

seeking public comments on possible solutions identified to address the tax challenges arising from the digitization of the economy.

The OECD notes that the proposals included in the consultation do not represent the consensus views of the BEPS IF, the OECD's Committee on Fiscal Affairs (CFA) or their subsidiary bodies. It is important in this regard to note that the current proposals may continue to be revised or added to. In that regard, they represent a current snapshot of what is being discussed by OECD member countries.

The consultation document is divided into three key sections:

Section 1: Introduction: provides detailed background, reviewing the OECD's work in this area to date

Section 2: Revised profit allocation and nexus rules: provides detailed examination of three key proposals under debate

Section 3: Global anti-base erosion proposal: sets out proposals to address the continued risk of profit shifting to entities subject to no or very low taxation

Some of the salient features of the consultation document are summarised below.

**Section 1: Introduction**

Section 1 discusses how, in March 2017, the G20 Finance Ministers mandated the BEPS IF working through the Task Force on the Digital Economy (TFDE), to deliver an interim report on the implications of digitalization for taxation by April 2018 and a final report in 2020. The interim report, Tax Challenges Arising from Digitalisation – Interim Report 20182 was delivered to the G20 in March 2018. Building on the BEPS Action 1 Report, the Interim Report reflected, among other things, the progress made since 2015 in considering the two previously identified direct tax issues, namely the exacerbated BEPS issues and the broader tax challenges.

The TFDE has continued evaluating various proposals and the result of this effort is presented in the consultation document, which sets out a number of proposals for consideration as part of a longer-term solution. The proposals are not legislative instruments or specific recommendations, and are at the policy design phase only, and therefore only high-level descriptions are provided. Importantly, and as noted throughout the consultation document, the proposed design elements of some of the proposals would mean that the impact of any changes adopted may not be limited to highly digitalized business models alone, and as such, may impact any multinational enterprise (MNE) utilizing intangible assets, including "marketing intangibles" (as defined in the OECD's Transfer Pricing Guidelines).

**Section 2: Revised profit allocation and nexus rules**

The consultation document describes the current proposals related to the "broader tax challenges" to the existing profit allocation and nexus rules. Sections 2 and 3 broadly describe policy proposals made by some members of the BEPS IF that would modify those rules based on the concepts of

(i) user participation,
(ii) marketing intangibles, and
(iii) significant economic presence,

The consultation document notes that the Interim Report identified three key characteristics – scale without mass, a heavy reliance on intangible assets, and the role of data and user participation – which sometimes work together to enable highly digitalized businesses to create value by activities closely linked with a jurisdiction without needing to establish a physical presence. The consultation document notes that any solution that seeks to address nexus must also address the closely-related issue of profit allocation.

The consultation document highlights developments already taking place in response to the recommendations from the BEPS project, including BEPS Action 7 (relating to permanent establishments). By way of example, the consultation document notes that some MNE groups with highly-digitalized business models have been able to establish local affiliates in market jurisdictions, whereby the local affiliates are commonly structured to have no ownership interest in intangible assets, perform no DEMPE (development, enhancement, maintenance, protection, and exploitation) functions, and do not assume any risks. Accordingly, only a modest return may be allocated to these "limited risk distributors," (LRDs). Thus, without effective changes to profit allocation rules, the document notes that an MNE group may seek to sidestep the nexus issue by establishing local affiliates that are not entitled to an appropriate share of the group's profit.

Importantly, the consultation document asks whether the issues raised with respect to highly digitalized MNEs also are relevant to a broader set of businesses – for example, businesses that, due to digitalization and changes in the global economy, can build their brand, develop an engaged customer base and create value in the absence of local activities or in the absence of local activities that attract a significant share of taxable profits.

Section 2 describes the (i) user participation proposal, and (ii) marketing intangibles proposal that focus on value creation in the user/market jurisdiction that is not recognized in the current framework for allocating taxing rights and taxable profits.

The consultation document notes that three proposals for revising the profit allocation and nexus rules are currently being debated. It should be noted that these proposals are in no way final and continue to be debated among jurisdictions.

The "user participation" proposal focuses on the value created by certain highly-digitalized businesses through developing an active and engaged user base, and soliciting data and content contributions from them. The proposal is premised on the idea that soliciting the sustained engagement and active participation of users is a critical component of value creation for certain highly-digitalized businesses.

These include  Social media platforms, Search engines and Online marketplaces.

The proposal suggests revising profit allocation rules to accommodate the value creating activities of an active and engaged user base. In addition, nexus rules would also be revised, so that the user (i.e., market) jurisdictions would have the right to tax the additional profit allocable to them. However, the consultation document notes, this proposal would be limited in applicability to business models which benefit from this type of user base; thus for businesses that have more traditional relationships with customers, no change in the profit allocation or nexus rules would be proposed.

The consultation document notes that the mechanics of this proposal would act to modify current profit allocation rules to require that, for certain businesses, an amount of profit be allocated to jurisdictions in which those businesses' active and participatory user bases are located, irrespective of whether those businesses have a local physical presence. It further notes that there would be significant difficulties in using traditional transfer pricing methods for determining the amount of profit that should be allocated to a user jurisdiction. As an example, it dismisses the idea that the value created by user activities can somehow be determined through the application of the arm's-length principle. Instead, it proposes that the profit allocated to a user jurisdiction, in respect of the activities/participation of users, be calculated through a non-routine or residual profit split approach.

The "marketing intangibles" proposal is based on the concept of "marketing intangibles" as defined in the OECD Transfer Pricing Guidelines. Like the "user participation" proposal, it would change the profit allocation and nexus rules, but would also be broader in scope in an effort to respond to the impact of the digitalization on the economy.

The "marketing intangibles" proposal addresses a situation where an MNE group can essentially (in the OECD's words) "reach into" a jurisdiction, either remotely or through a limited local presence (such as an LRD), to develop a user/customer base and other marketing intangibles. It

sees an intrinsic functional link between marketing intangibles and the market jurisdiction. Taking this link into account, the proposal would modify current transfer pricing and treaty rules to require marketing intangibles and risks associated with such intangibles to be allocated to the market jurisdiction. The proposal considers that the market jurisdiction would be entitled to tax some or all of the non-routine income properly associated with such intangibles and their attendant risks, while all other income would be allocated among members of the group based on existing transfer pricing principles. The proposal does not look at trade intangibles which, according to the consultation document, are seen as not similarly possessing an intrinsic functional link with market jurisdictions.

The special allocation of some or all non-routine returns from marketing intangibles, and the related expansion of the market country's taxation rights, would apply regardless of which entity in the MNE group owns legal title to the marketing intangibles, regardless of which entities in the group factually perform or control DEMPE functions related to those intangibles, regardless of how risks related to the marketing intangibles would be allocated under existing transfer pricing rules, and regardless of how those rules would ordinarily allocate income related to the marketing intangibles and their associated risks.

The "significant economic presence" proposal is based on the concept of "significant economic presence" as originally described in Section 7.6 of the BEPS Action 1 Report.
Under this proposal, a taxable presence in a jurisdiction would arise when a nonresident enterprise has a significant economic presence on the basis of factors that evidence a purposeful and sustained interaction with the jurisdiction via digital technology and other automated means. Revenue generated on a sustained basis is the basic factor, but such revenue would not be sufficient in isolation to establish nexus. Only when combined with other factors (such as existence of a user base, the volume of digital content derived from the jurisdiction and sustained marketing and sales promotion activities) would revenue potentially be used to establish nexus in the form of a significant economic presence in the country concerned.

The proposal contemplates that the allocation of profit to a significant economic presence could be based on a fractional apportionment method, as discussed in Section 7.6.2.2 of the Action 1 Report. Other simplified methods for allocating profit will also be considered, such as the modified deemed profits methods described in section 7.6.2.3 of the Action 1 Report. The proposal also contemplates the possible imposition of a withholding tax as a collection mechanism and enforcement tool. In this context, consideration could be given to a gross-basis withholding tax at a low rate on payments to an enterprise with a significant economic presence,

with the enterprise having the right to file an income tax return and seek a refund if the withheld amount exceeded the enterprise's income tax liability.

**Section 3: Global anti-base erosion proposal**

Section 3 describes proposals related to the perceived risk of profit shifting and explores two sets of rules designed to give jurisdictions a remedy in cases where income is subject to no or only very low taxation: (i) an income inclusion rule, and (ii) a tax on base eroding payments. Importantly, the scope of the anti-base erosion proposal is not limited to highly digitalized businesses. Instead it focuses on the remaining BEPS challenges and looks to propose a systematic solution designed to ensure that all internationally operating businesses pay a minimum level of tax.

The income inclusion rule would operate as a minimum tax by requiring a shareholder in a corporation to bring into account a proportionate share of the income of that corporation if that income was not subject to tax at a minimum rate. The rule would apply to any shareholder with a significant (e.g., 25%) direct or indirect ownership interest in that company and would be applied on a per jurisdiction basis. The amount of income to be included would be calculated under domestic law rules and shareholders would be entitled to claim a credit for any underlying tax paid on the attributed income, with such credits also being calculated on a jurisdiction-by-jurisdiction basis. This rule would supplement rather than replace a jurisdiction's Controlled Foreign Corporation rules.

The consultation document explains that the income inclusion rule would build on the BEPS Action 3 recommendations and draw on aspects of the United States (US) regime for taxing Global Intangible Low-Taxed Income (GILTI). The rule would be designed in such a way that Member States of the European Union (EU) could apply it to both domestic and foreign subsidiaries and it could be adopted via an EU directive.

The second key element of the proposal is a tax on base eroding payments that complements the income inclusion rule by allowing a source jurisdiction to protect itself from the risk of base eroding payments. More specifically, this element of the proposal would include:

An undertaxed payments rule that would deny a deduction for a payment to a related party if that payment was not subject to tax at a minimum rate; and

A subject-to-tax rule in tax treaties that would only grant certain treaty benefits if the item of income is sufficiently taxed in the other state.

The consultation document highlights that because the various elements of the anti-base erosion proposal are intended to tackle the same structures, there is the possibility that these rules will overlap to a certain extent. Given the potential for overlap, an ordering rule would be necessary and there are at least two design options for such an ordering rule: a rule that could be applied on a payment by payment basis or a more systemic approach that would switch off the application of one rule if an MNE was based in a jurisdiction that had introduced the other rule. Further technical work would need to explore these overall approaches and then also establish the order in which they would be applied.

A public consultation meeting was held at the OECD Conference Centre in Paris on 13 March and the morning of 14 March 2019. Comments received are available on the OECD website.[li]
The outcome of the public consultation should be reflected in the next draft that may come out from OECD. Students need to keep track of the developments on the OECD's website.

**Concluding Remarks**

International Taxation is an extension of the domestic taxation principles to cross border transactions. E Commerce is a component of the International trade and the international taxation principles apply to E Commerce to the extent it involves cross border transactions. The digital products and the easy transmission across the borders make E Commerce issues slightly different from other international trade issues. Though most of the taxation issues in the cross border trade are resolved through bilateral treaties, organizations like OECD lay down the framework for multilateral agreements and also shape the practices adopted in the bilateral agreements. This is a dynamic field where developments should be watched over the resources available on the Internet.

**References:**

[1]https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en#page1

[1]https://read.oecd-ilibrary.org/taxation/action-plan-on-base-erosion-and-profit-shifting_9789264202719-en#page17

[1]http://www.oecd.org/tax/administration/20499630.pdf

[1]https://taxinsights.ey.com/archive/archive-news/oecd-opens-public-consultation-on-addressing-tax-challenges.aspx

[1] https://www.oecd.org/tax/beps/public-comments-received-on-the-possible-solutions-to-the-tax-challenges-of-digitalisation.htm

*P.S: Since the entire content has been drawn from dynamic resources in the Internet and most of the published books may not contain updated information, no reference to books have been provided. In the changing world of technology, the value of judicial precedence is also low. Every judicial decision has to be seen with the law and technology as applicable to a case on hand and hence excessive reliance on case laws in areas of E Commerce is better avoided. Hence it is recommended that students develop an insight into the legal interpretation from out of the current developments they may observe on the resources available on the Internet after due filtration for the credibility of the information.*

---

[i] https://en.wikipedia.org/wiki/Justice_K._S._Puttaswamy_(Retd.)_and_Anr._vs_Union_Of_India_And_Ors.
[ii] http://ceac.in/wp/ceac-edb/
[iii] Naavi is the trademark name by which the author is known and as a thought leader contributed to the development of Cyber Jurisprudence in India.
[iv] https://www.naavi.org/wp/ita-2008-already-has-a-provision-if-sophia-breaks-our-law/
[v] http://ita2008.in/ita_2008/ch4_2008.htm
[vi] https://www.naavi.org/wp/creating-protection-indian-companies-european-hegemony/
[vii] www.odrglobal.in
[viii] https://dipp.gov.in/sites/default/files/pn2_2018.pdf
[ix] https://patents.google.com/patent/US7996298B1/en
[x] https://www.naavi.org/wp/closure-of-bazee-com-case-sharat-digumati-gets-relief-amidst-intriguing-precedents-created/
[xi] https://www.naavi.org/wp/the-e-tendering-issues-in-maharashtra-uploading-is-not-the-same-as-submitting-the-tender/

[xii] https://www.naavi.org/wp/167-2/
[xiii] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
[xiv] http://www.naavi.org/naavi_comments_itaa/historical_perspective/ect_1998/index.htm
[xv] http://ceac.in/wp/ceac-edb/
[xvi] Naavi is the trademark name by which the author is known and as a thought leader contributed to the development of Cyber Jurisprudence in India.
[xvii] https://www.naavi.org/wp/ita-2008-already-has-a-provision-if-sophia-breaks-our-law/
[xviii] http://ita2008.in/ita_2008/ch4_2008.htm
[xix] https://www.naavi.org/wp/creating-protection-indian-companies-european-hegemony/
[xx] http://www.lookalikes.in/
[xxi] http://www.odrglobal.in/

[xxii] http://ceac.in/wp/ceac-edb/
[xxiii] http://ceac.in/wp/2017/04/25/basheer-case-judgement-and-section-65b-of-indian-evidence-actcyber-jurisprudence-develops/
[xxiv] http://ceac.in/wp/2018/04/19/the-tragedy-of-shafhi-mohammad/
[xxv] http://www.naavi.org/ebook2011/index.htm
[xxvi] https://www.naavi.org/wp/index-of-articles-on-bitcoin-the-currency-of-the-criminals-by-the-criminals-for-the-criminals/
[xxvii] https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0
[xxviii] https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=243
[xxix] http://www.naavi.org/cl_editorial_11/ggwg_rbi_circular.pdf
[xxx] http://www.naavi.org/archives/archive_2011/comments_ggwg.htm
[xxxi] http://www.naavi.org/cl_editorial_11/ggwg_rbi_circular.pdf
[xxxii] https://www.naavi.org/wp/umashankar-judgement-upheld-by-tdsat/

[xxxiii] https://www.naavi.org/wp/a-note-for-the-attention-of-smes-on-cheque-disincentivisation/
[xxxiv] https://m.rbi.org.in/Scripts/FAQView.aspx?Id=24
[xxxv] http://www.naavi.org/importantlaws/it_rules_compendium/adj_off_notification_goi.pdf
[xxxvi] http://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf
[xxxvii] https://www.naavi.org/wp/umashankar-judgement-upheld-by-tdsat/
[xxxviii] http://naavi.org/uploads_wp/new/juy_72017_limited_liability.PDF
[xxxix] https://www.naavi.org/wp/zero-liability-is-there-a-fine-print-that-depositors-should-be-wary-of/
[xl] https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
[xli] https://www.iso.org/isoiec-27001-information-security.html
[xlii] https://www.naavi.org/wp/india-to-be-the-hub-of-international-personal-data-processing-objective-of-pdpsi/
[xliii] https://www.mea.gov.in/Images/pdf1/S7.pdf
[xliv] https://www.incometaxindia.gov.in/Pages/i-am/non-resident.aspx?k=Introduction
[xlv] http://www.cbic.gov.in/resources//htdocs-cbec/gst/51_GST_Flyer_Chapter42.pdf;jsessionid=1ED151DA92373BD69A16E314BC731BED
[xlvi] https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf
[xlvii] https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en#page1
[xlviii] https://read.oecd-ilibrary.org/taxation/action-plan-on-base-erosion-and-profit-shifting_9789264202719-en#page17
[xlix] http://www.oecd.org/tax/administration/20499630.pdf
[l] https://taxinsights.ey.com/archive/archive-news/oecd-opens-public-consultation-on-addressing-tax-challenges.aspx
[li] https://www.oecd.org/tax/beps/public-comments-received-on-the-possible-solutions-to-the-tax-challenges-of-digitalisation.htm