BCS-062

E-COMMERCE

December 2015

1.

(a) Explain E-Commerce Trade Cycle. Explain the role of intermediary in addition of value by online marketplaces. 10

Ans: A trade cycle is a sequence of interactions that is involved in an online transaction between a supplier and a customer. A general trade cycle consists of the following phases:

Pre-sales : Customers browse online stores or platforms to find the products or services they need. This stage may involve negotiating terms like pricing, delivery schedules, payment methods and agreeing the terms.

Execution: In this stage, customers add items to their online shopping cart and proceed to checkout. The e-commerce business processes the order, prepares the items for shipment and arranges for delivery. The product is delivered to the customer.

Settlement: Customers make payment for the goods or services, often through various online payment methods. An invoice is generated for the transaction.

After-sales: E-commerce businesses provide support to address any customer queries, complaints or returns. This stage also includes warranty services or maintenance for the purchased items.

For business-to-business transactions, the trade cycle typically involves the provision of credit with execution preceding settlement whereas in C2B transactions, these two steps are typically coincident. The nature of the trade cycle can indicate the e-commerce technology most suited to the exchange.

EDI (Electronic Data Interchange) is the e-commerce technology appropriate to these exchanges. The trade cycle includes the following operations: search, negotiate, order, deliver, invoice, payment and after-sales.

Consumer transactions tend to be once-off (or at least vary each time) and payment is made at the time of the order. The trade cycle in the case of retail exchanges is different and includes the following operations: search, order, payment, deliver and after-sales.

Intermediaries:

Without using an intermediary, a merchant could provide his goods and services to a customer directly. New kinds of intermediaries were created as e-commerce technology advanced in development. New value-added services were being provided by these new intermediaries. With new services that facilitate their trade, new intermediaries draw many new customers and sellers.

An intermediary can provide the following four important mechanisms that cause marketplaces to add value:

* Matching buyers and sellers to negotiate prices on a dynamic and real-time basis,

* Ensuring trust among participants by maintaining a neutral position,

* Facilitating market operations by supporting certain transaction phases, and

* Aggregating many buyers and sellers together. Intermediaries bring together buyers and sellers, making it easier to find suitable trading partners

An intermediary provides different services to buyers and suppliers on the e-marketplace. Auctions, payments, logistics, legal, consultancy, and inter-company interactions via third-party inter-organizational systems and associated systems are just a few of the many activities that intermediary services can serve. Intermediaries help businesses cut costs by managing payment processing, transportation, and other transactional aspects. Intermediaries can combine services like logistics, pre-sales assistance, and customer support, making the overall experience more convenient for buyers.

Online marketplaces use intermediaries to add value by facilitating transactions, reducing search costs for both buyers and sellers, and fostering trust.
Online marketplaces make it simpler for customers to find what they need by serving as a single point of contact for information collecting and market transactions.

By assisting sellers in locating eligible purchasers, intermediaries lower their marketing and advertising expenses. Intermediaries can monitor transactions and prevent opportunistic behavior, protecting both buyers and sellers.

(b) What is an e-paper ? List the advantages and disadvantages of e-papers. 10

Ans: Electronic newspaper is normally called e-paper. Online newspapers are becoming more and more popular to news readers who are Internet savvy. Electronic newspaper is the newspaper which exists on the Internet either separately or as online version of a printed periodical. Examples of popular e-papers are: http://www.timesofindia.com and http://www.thehindu.com.

Features of e-newspaper are:

Search: Readers can easily search for specific news or articles. This makes it convenient to find relevant news.

Interactive content : Most online newspapers include videos, podcasts,hyperlinks and interactive infographics that enhance the reading experience.

Customize: Users can customize their news feed based on interests, helping them to focus on topics they are interested in.

Archives are easily available. The Hindu e-paper offers access to archived editions, enabling users to easily find and revisit past articles.

Sharing articles: The e-paper enables easy sharing of articles with others through social media or email.
Advantages:

- It is accessible 24* 7. The e-paper can be easily accessed on smartphones, tablets, or laptops, allowing for convenient reading while commuting or traveling.
- It can be read anywhere, anytime.
- The reader can select the news of interest and avoid the rest.
- It is environmentally friendly than getting a printed newspaper.
- It is a reliable source of news as it is updated at regular intervals.
- E-newspapers do not require physical storage and can avoid cluttering in the home.

Disadvantages:

- Prolonged screen time can lead to eye strain and digital distractions, potentially detracting from the immersive reading experience.
- Not everyone has access to the internet which can limit readership.
- Misinformation**:** The online sphere can be less regulated, potentially leading to the spread of misinformation, which readers need to be aware of and filter out.
- A newspaper company should be prepared for reduced revenues if it provides e-paper free of cost.

2.

(a) List any five cyber offences and related penalties under IT Act, 2000. 5

Ans: Cyber crimes can be classified on the following basis:

- Against Person

- Against Property
- Against Government/Corporate Entities
- Against Society at Large

Against Person

• Harassment via e-mails: Repeatedly sending abusive messages via email.

• Cyber stalking: Use of Internet to stalk someone like online harassment and online abuse.

• Email spoofing: Emailing messages with a forged sender address.

• Publishing/transmitting of obscene material.

• Cyber defamation: causing injury to the reputation of a person with the help of Internet by floating/publicizing negative messages.

• Cheating and fraud: Any deliberate deception for unfair or unlawful gain online is fraud. Examples are no delivery of paid products purchased online, misrepresentation of a product advertised for sale, and fraudulent promises for investment in securities.

Against Property :

• Unauthorized control/access of Computer system.

• Intellectual property crimes: Patent violations, copyright infringement, trademark violations, etc.

• Transmitting virus.

Against Government/Corporate Entities

• Possession of information in an unauthorized manner.

• Cyber terrorism: Use of Internet for terror activities.

• Distribution of pirated software.

Against Society at Large:

• Pornography.

• Polluting the youth through indecent exposure

• Financial crimes.

• Forgery- Manipulations in mark sheets, currency notes etc with the use of information technology.

• Sale of illegal articles like narcotics, weapons, etc.

• Online gambling

Cyber crime	Penalties
Sending offensive or false messages through communication service, etc. lt is also known as cyber stalking.	Imprisonment up to three years and with fine.
Cyber terrorism: Whoever uses cyber space with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the society or any section of the people.	Imprisonment which may extend to life imprisonment.
Violation of privacy: Intentionally or knowingly captures, publishes or transmits the image of any person without his or her consent, under circumstances of violating the privacy of that person.	Imprisonment up to three years or fine up to two lakh rupees or both.
Breach of confidentiality and privacy: Securing access to any Computer, system or network.	Imprisonment up to two years or fine up to one lakh rupees or both.
Identity theft: Fraudulently or dishonestly make use of the .electronic signature, password or any other unique identification feature of any other person.	Imprisonment up to three years or fine up to rupees one lakh.
Hacking the Computer system	Imprisonment up to three years or with fine which may extend up to 5 lakh rupees or both.
Publishing or transmitting obscene material in electronic form.	First conviction: Imprisonment up to three years and with fine up to five lakh rupees. Subsequent conviction: Imprisonment up to five years and with fine up to ten lakh rupees .

(b) What is SSL ? Explain its working with the help of a figure. 5

Ans: It is a web security protocol that is used to establish an encrypted link between a web server and a web browser. It was developed by Netscape. It operates between the application and transport layers. It is commonly used to manage the security of message transmission on the Internet. It secures the data during online transactions or when

transmitting confidential information. It is a solution to authentication, privacy and integrity problems and avoids attacks. SSL authenticates servers and users. It establishes encrypted link to hide the data transmitted thus leading to data integrity.

Characteristics of SSL:

• It operates at TCP/IP transport layer,

• It uses a dedicated TCPIIP socket,

• It encrypts the communications between the server and client when connection is established, and

• It requires a server certificate.

Working of SSL:

The following are various steps of SSL handshake:

1. Establishing a connection:

Client hello: SSL client attempts to connect to a SSL server (website secured with SSL) by sending a client hello message.

Server hello: Web server responds with a server hello.

2. Client requests web server to prove its identity.

3. The server sends its SSL certificate to the client. The certificate contains the server's public key and is signed by a trusted Certificate Authority (CA).

4. The client verifies the server's certificate against its list of trusted CAs. Accordingly, it sends a message to the server. If the certificate is valid, the client trusts that it is communicating with the right server.

5. If the server requires client authentication, it asks for "client certificate request".

6. Then the client sends its certificate.

7. SSL server verifies the signature on the client certificate.

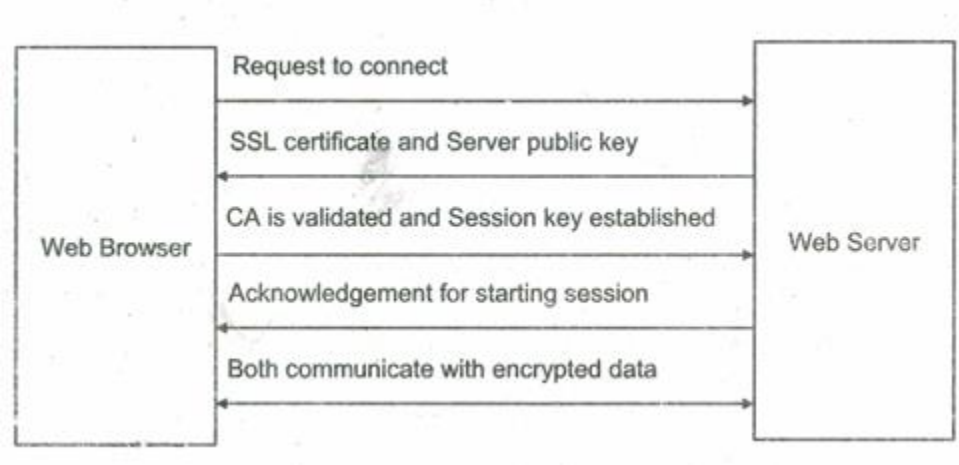
8. Client sends a digitally signed acknowledgement to start sharing.

9. Server sends a digitally signed acknowledgement to start sharing.

10. The data in encrypted form is shared between the server and browser and a secured session starts that protects message privacy, integrity and security. A secure session

starts between server and client enabling data to be transmitted in encrypted form, thus ensuring privacy, integrity and security.

11. When the session ends, both parties can send a message to close the connection securely.



Working of SSL

3.

(a) Explain any five challenges to the success of m-commerce. 5

Ans: Some of the prominent challenges to the success of m-commerce are given below:

* Screen size : Mobile devices smaller screens can make browsing and navigating more difficult, which could affect the user experience and make it harder to access product details or finish transactions.

* Security: This is one of the prime concerns which is further increased due to the transactions happening over wireless networks. Similarly, the security issues related to mobile payment systems is another limitation. Mobile devices are susceptible to various security threats like hacking, phishing, and malware attacks.

* Mobile experience: Due to the wide variety, of mobile devices, operating systems and device form factors, it requires a design that leads to robust user experience that caters to consumers of all these devices. Applications not conforming to standards pose challenges across various mobile platforms.

* Mobile network coverage and bandwidth: Wireless networks offering high bandwidths are not available in all areas posing challenges to commerce transactions.

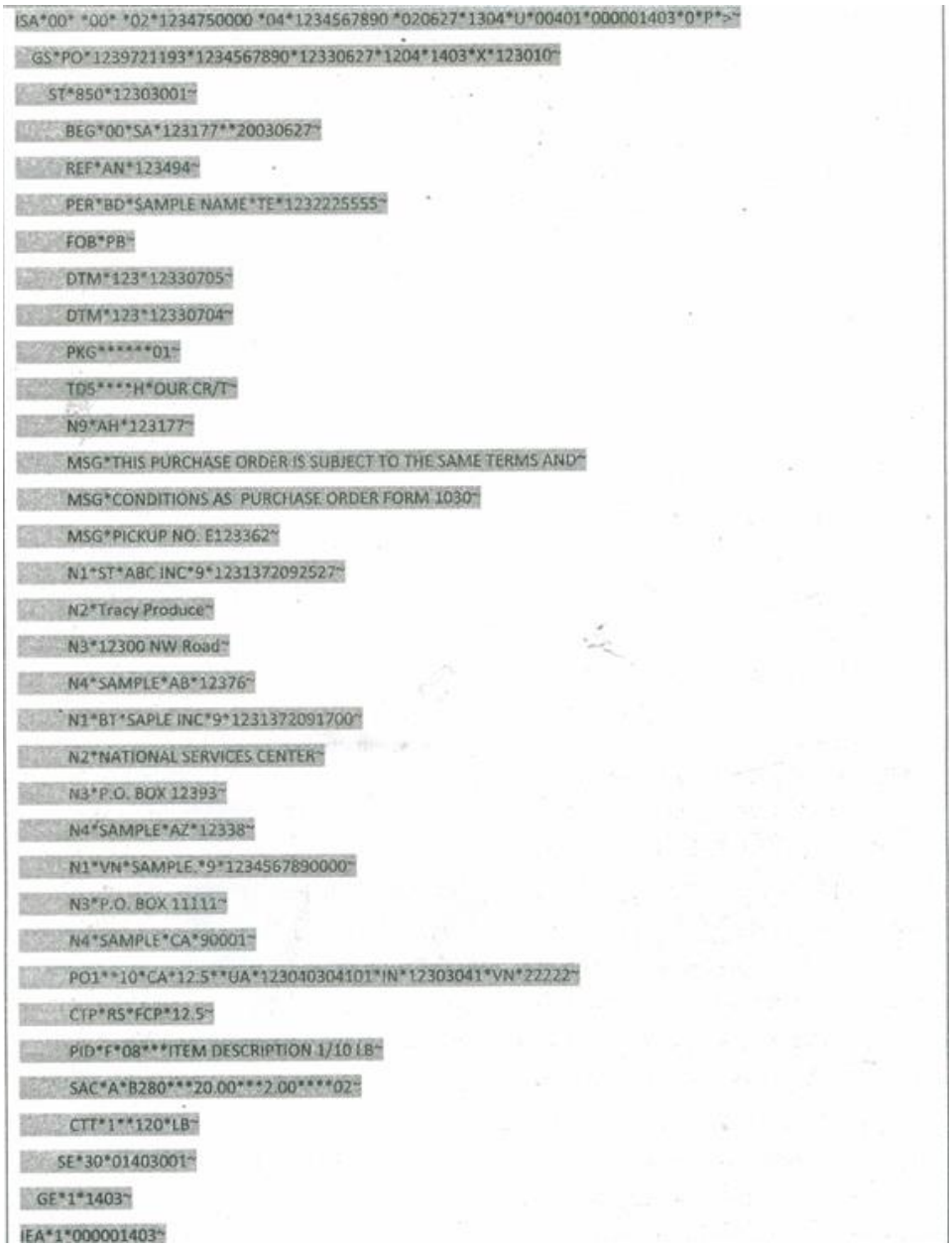
* Web page performance is not optimized for mobile devices resulting in slower page loads on mobile platforms.

* Internet connectivity: Stable internet access is crucial for m-commerce, and unreliable or slow connections can lead to frustrating user experiences, particularly during the checkout process. In areas with poor connectivity, m-commerce adoption may be limited.

(b) Explain any two EDI standards. 5

Ans: There are multiple EDI standards such as ANSI X12, EDIFACT, TRADACOMS (Trading Data Communications), ODE1TE (Organization for Data Exchange by Tele Transmission in Europe), VDA (Verband Der Automobilindustrie), SWIFT (Society for Worldwide Interbank Financial Telecommunication).

ANSI X12: ANSI X12 is most popular in North American region. It defines standards for various business transactions such as order processing, material handling, warehousing services, manufacturing services, etc. X12 standard uses transaction set to identify each business transaction and each transaction set is denoted by a numeric code.



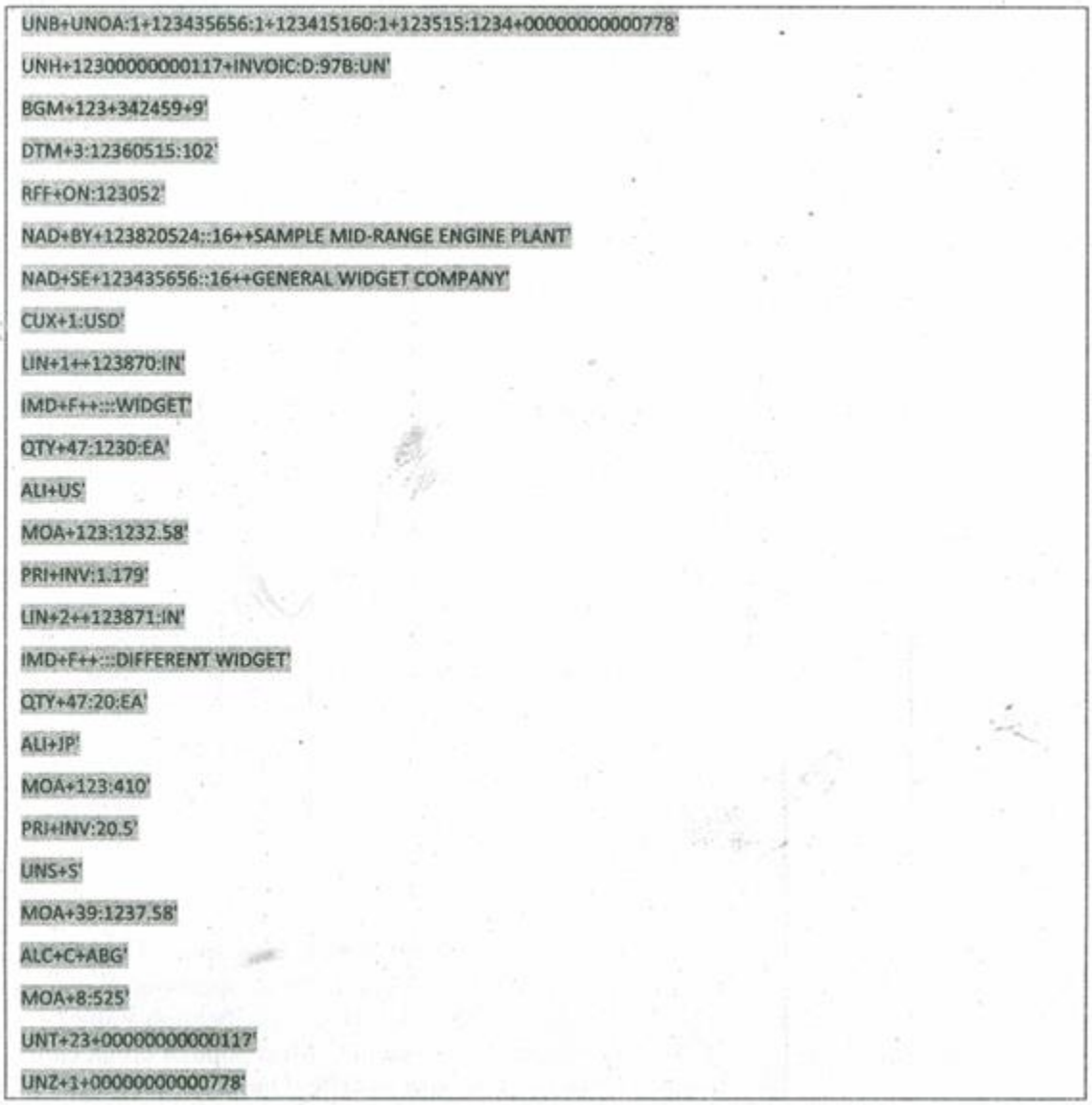
EDIFACT:

EDIFACT is an EDI standard format developed under UN (United Nations), Hence, EDIFACT is also denoted as UNIEDIFACT. This is the international standard which consists of the following four key elements:

- Syntax which defines the message structure
- Data elements within the document

• Segments which groups the date elements

• Messages which are an ordered group of segments and symbolize a business transaction.



4.

(b) What is meant by Inter-organizational e-commerce ? How does it differ from Intra-organizational e-commerce ? 5

Ans: When e-commerce transaction involves multiple organizations, then it is termed as Inter- organizational e-commerce. It refers to the online transactions and interactions that occur between different organizations. Inter-organizational e-commerce involves

transactions between different companies, suppliers, partners, and customers. It focuses on the exchange of goods, services and information across organizational boundaries.

B2B is the most common form where businesses sell products or services to other businesses.

Inter-organizational e-commerce vs intra organizational e-commerce:

Inter-organizational e-commerce	intra organizational e-commerce
When e-commerce transaction involves multiple organizations, then it is termed as Inter- organizational e-commerce.	When e-commerce transaction does not involve multiple organizations, then it is termed as intra-organizational e-commerce.
Inter-organizational e-commerce is about "business to business" or "business to consumer" interactions.	Intra-organizational e-commerce is about "business to employee" interactions or internal business process automation.
Inter-organizational e-commerce spans multiple organizations.	intra-organizational e-commerce is limited to a single organization.
Inter-organizational e-commerce involves businesses selling to other businesses or collaborating on supply chains.	intra-organizational e-commerce involves internal processes and transactions within a company.
Inter-organizational e-commerce may utilize technologies like EDI, B2B marketplaces, and collaborative platforms.	intra-organizational e-commerce often relies on ERP systems, intranets, and internal management tools
Inter-organizational e-commerce aims to improve efficiency and collaboration across organizations.	intra-organizational e-commerce focuses on streamlining internal operations, improving communication, and enhancing employee experience
For example, A manufacturer using an online portal to order raw materials from its suppliers, or a retailer using a B2B marketplace to source products from various vendors.	An employee using an internal portal to submit expense reports, a company offering an online platform for employees to access benefits information, or an internal system for managing employee performance reviews.

5.

(a) List and explain any five emerging trends in m-commerce.

Ans: The following are some of the emerging trends in the space of m-commerce:

M-wallet: Using mobile devices for various ranges of financial transactions. M-wallets like Apple Pay, Google Pay are becoming more popular. It allows users to make quick and secure payments using their smartphones.

Near Field Communications (NFC) enable radio communication between smart phones and other similar devices which are in proximity (normally not more than a few inches) or when they touch each other.

Mobile coupons are expected to become popular at retail stores.

Social commerce enablement though mobile devices. Social media platforms are increasingly integrating shopping features.

Taking off of Mobile first strategy wherein the enterprises design their online strategy predominantly around mobile devices first making the user experience on mobile devices more friendlier.

In-store personalization based on mobile app which indicates the available sales and acts as a smart store guide.

Mobile shopping is going to play a major role in the shopping space.

In-store personalization based on mobile app which indicates the available sales and acts as a smart store guide.

Majority of purchase decisions may be done via mobile phones during shopping. It includes product research, product comparison etc.

(b Whenever you perform transactions online that involve online payment, what are the precautions you take before making payment? 5

Ans: Precautions to take before making payment :

- Use secure connections : Check for a padlock icon in the browser address bar and "https://" in the URL (the "s" denotes a secure connection).
- Avoid opening attachments or clicking links from senders you don't recognize because they could be phishing efforts.
- Hackers may take advantage of flaws in outdated software and browsers.
- Stay away from crucial transactions on public Wi-Fi: Since public Wi-Fi networks are frequently unprotected, hackers may be able to access your data.
- Don't use the same password for many accounts; instead, create complicated ones that combine capital and lowercase characters, numbers, and symbols.

- Before finalizing the payment, double-check the amount, merchant name, and other information.
- Install Antivirus software and keep it updated :Antivirus software can help detect and prevent malware infections that could compromise your information.
- Verify website's legitimacy: Research the website and company reputation through online reviews and independent sources.
- Scrutinize the domain name for misspellings or unusual characters that may indicate a phishing site.
- Look for clear contact information, including a physical address, phone number, and email address, and verify their authenticity.