

Registration Number:

Date & session:

Registration Number:

Date & session:

**ST JOSEPH’S UNIVERSITY, BENGALURU -27**

**B.Com – 4th SEMESTER**

**SEMESTER EXAMINATION: APRIL 2024**

**(Examination conducted in May / June 2024)**

**BPS 4222: Banking for Business Processing Services**

**(For current batch students only)**

**Time: 2 Hours Max Marks: 60**

**This paper contains two printed pages and four parts**

**Section A**

**I.** Answer ***any five*** of the following (**3 x 5 = 15 marks)**

1. Name the presidency banks established in India.
2. Give any three examples of criminal conducts in money laundering.
3. List any three presumptions of negotiable instruments.
4. What is meant by advance payment in international trade? State its features.
5. Mention any three benefits of ATM.
6. Give the meaning of special crossing of cheques.

**Section B**

**II.** Answer ***any two*** of the following (**5 x 2 = 10 marks)**

1. Outline the importance of NEFT and RTGS.
2. Brief out the features of savings and current deposits.
3. Write a short note on wealth management.

**Section C**

**III.** Answer ***any two*** of the following (**10 x 2 = 20 marks)**

1. Discuss in detail the types of mortgages.
2. Describe the role of banks in international trade.
3. Explain in detail the types of bank customers.

**Section D**

**IV. Answer the following (15marks)**

1. In the bustling city, where digital transactions are part of our livelihood, there was a renowned online bank named MaxTrust. With its sleek interface and state-of-the-art security, MaxTrust had earned the trust of millions. One day, a skilled hacker known as Alpha, set their sights on exploiting the fortress of MaxTrust. Armed with advanced coding skills and an intricate knowledge of social engineering, Alpha has a great master plan. He crafted convincing phishing emails, resembling official MaxTrust communications. These emails lured unsuspecting customers into a trap, prompting them to click on seemingly harmless links that led to a fraudulent website mirroring the bank's login page. Falling victim to this digital bait, customers unknowingly revealed their sensitive login credentials. In addition, with the stolen credentials, Alpha gained unauthorized access to several accounts. To avoid detection, they subtly manipulated account details, making small transactions that wouldn't immediately raise suspicion. The hacker ensured no traces of evidence were found. Customers began noticing peculiar transactions on their statements. Panic spread as MaxTrust's customer support lines buzzed with worried inquiries. The bank, alerted to the unusual activity, launched an investigation. MaxTrust, led by their cyber security team, embarked on a digital chase to trace the source of the fraudulent transactions. As the bank raced against time, Alpha continued to exploit the compromised accounts, always staying one step ahead.
2. Identify the type of frauds highlighted in the case. **(5 marks)**
3. Explain the problems and provide suggestive measures to prevent such online frauds. **(10 marks)**

**\*\*\*\*\*\*\*\*\*\*\*\*\*End of the paper\*\*\*\*\*\*\*\*\*\*\*\*\*\***