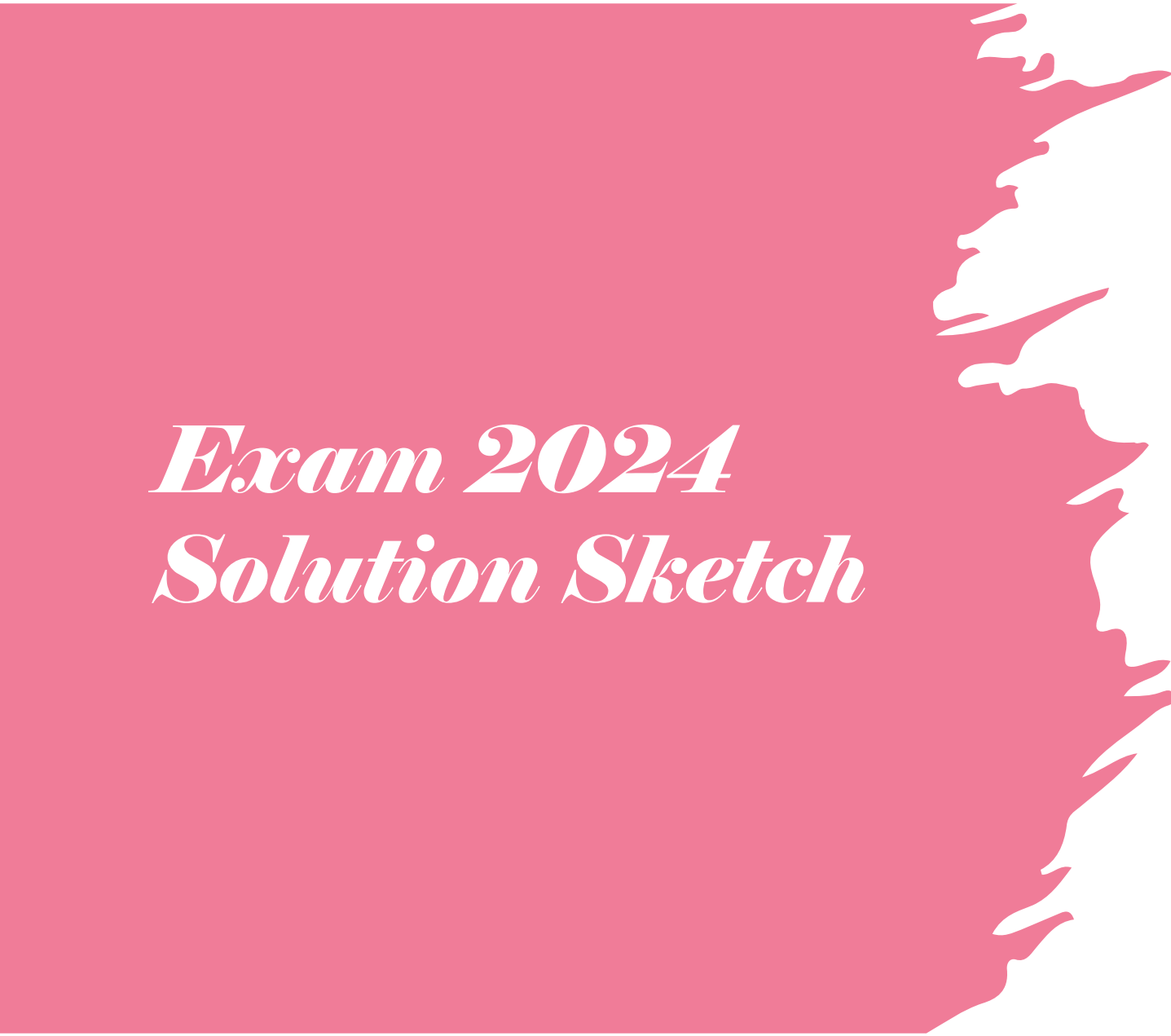
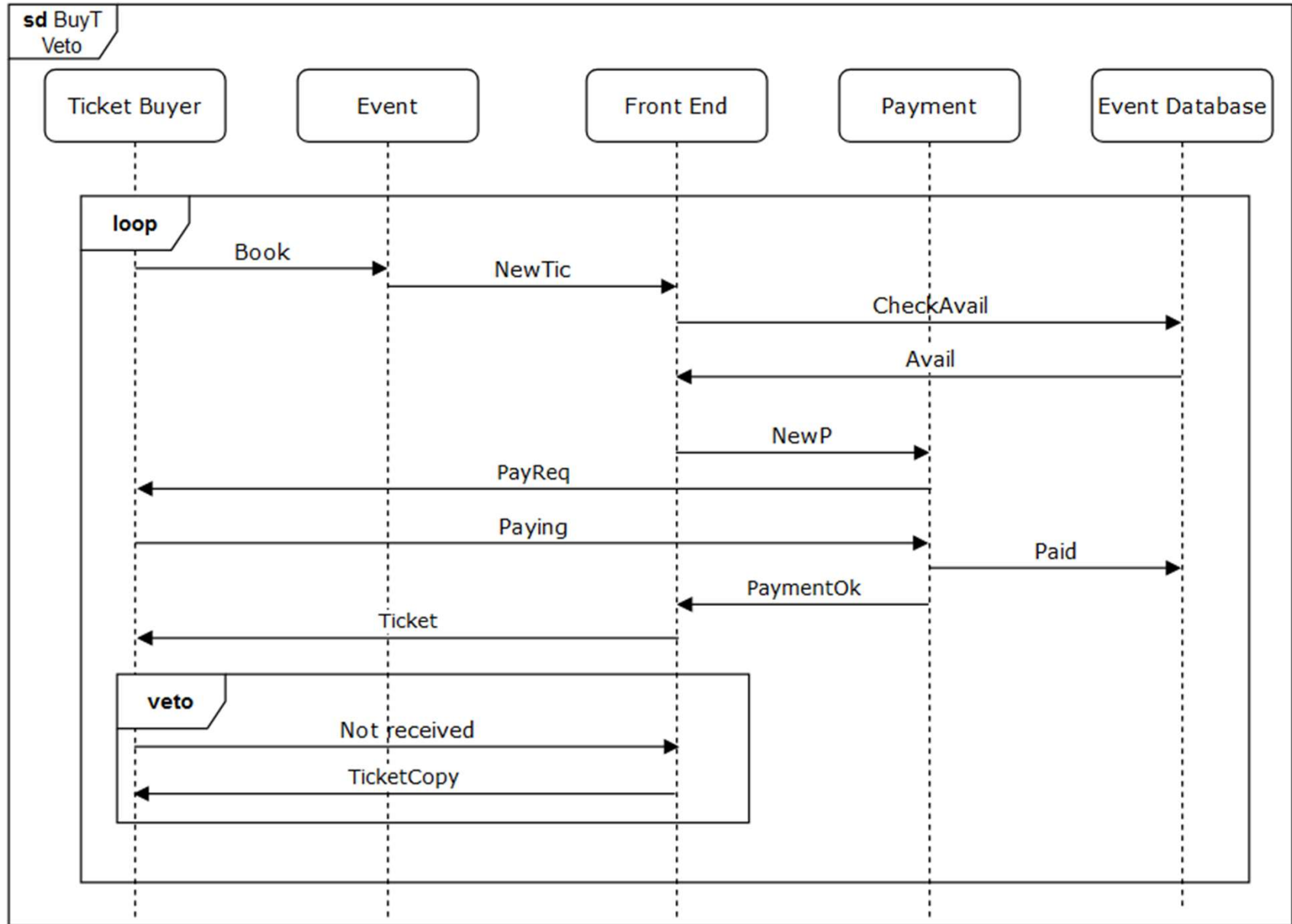


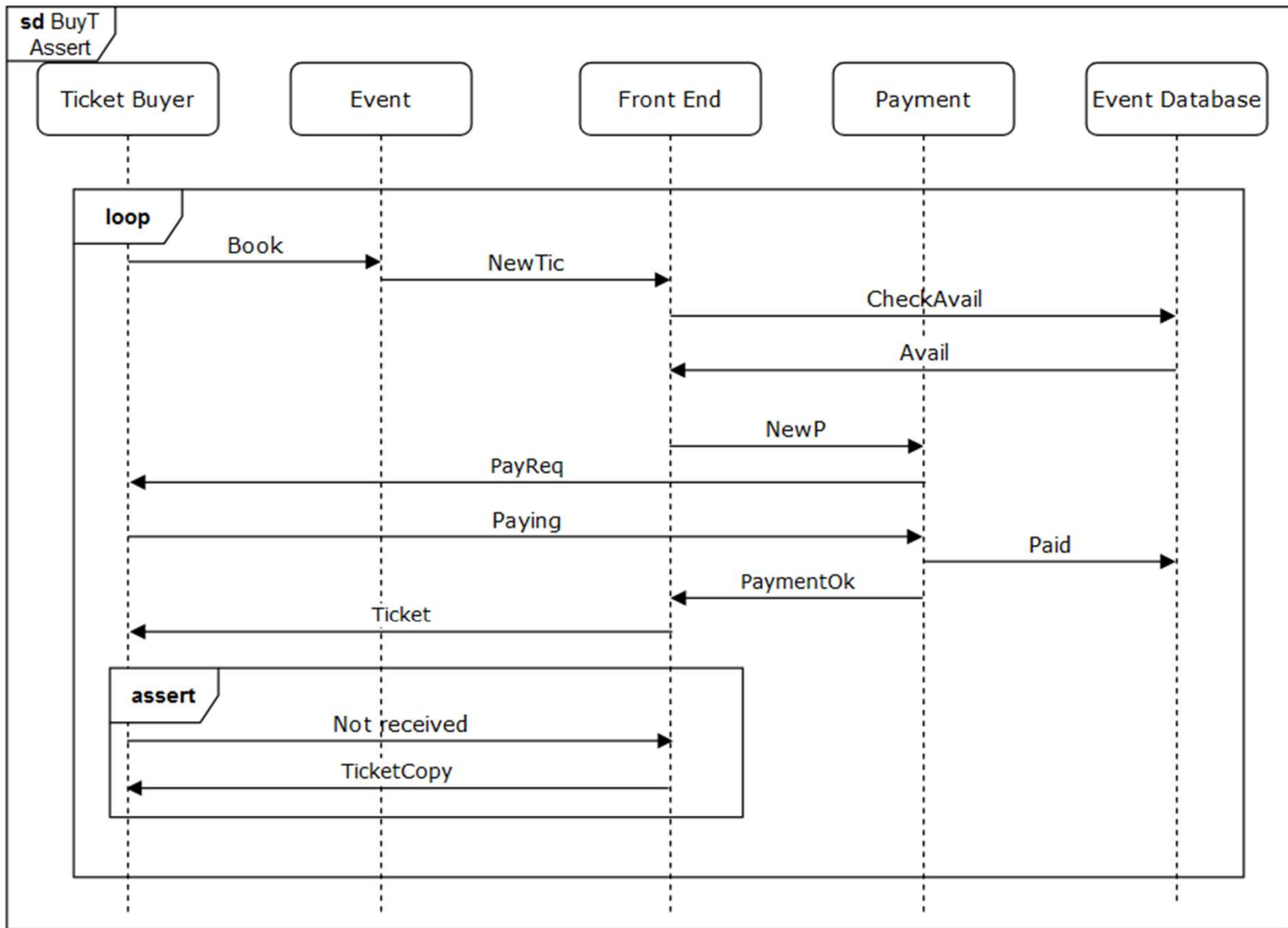
A large, solid pink shape that occupies the left half of the slide. It has a jagged, torn-paper-like right edge that separates it from the white background.

Exam 2024

Solution Sketch

KETIL STØLEN



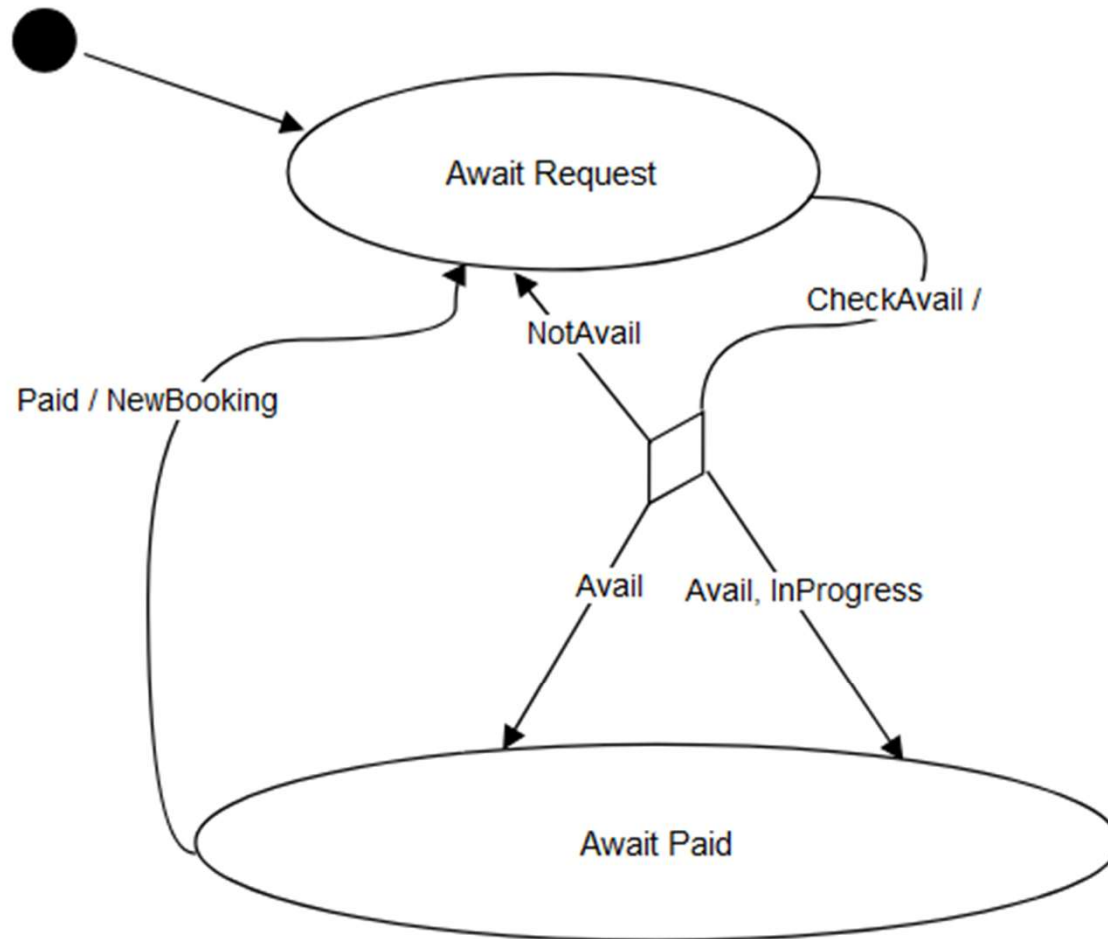


Question 1

- a. What is/are the possible second event/event(s) in a positive trace of sd BuyT Veto under the assumption that the loop iterates at least once? Explain your answer.
- b. What is/are the possible last event/event(s) in a negative trace of sd BuyT Veto under the assumption that the loop iterates at least once? Explain your answer.
- c. How many positive traces do we get under the assumption that sd BuyT Veto does not iterate more than once? Explain your answer.
- d. What is/are the possible last event/event(s) in a positive trace of sd BuyT Assert under the assumption that the loop iterates at least once? Explain your answer.
- e. What is the minimum length of a negative trace of sd BuyT Assert? Explain your answer.

Solution Outline Question 1

- a. ?Book
- b. ?TicketCopy and ?Paid
- c. 6
 - <> if loop 0
 - 5 depending on the interleaving of ?Paid
- d. ?TicketCopy and ?Paid
- e. 20 since <> is negative in the assert fragment

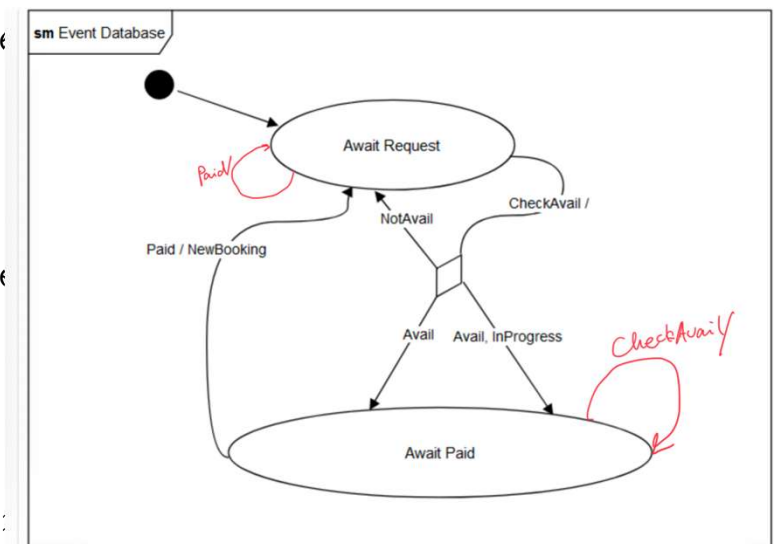


Question 2

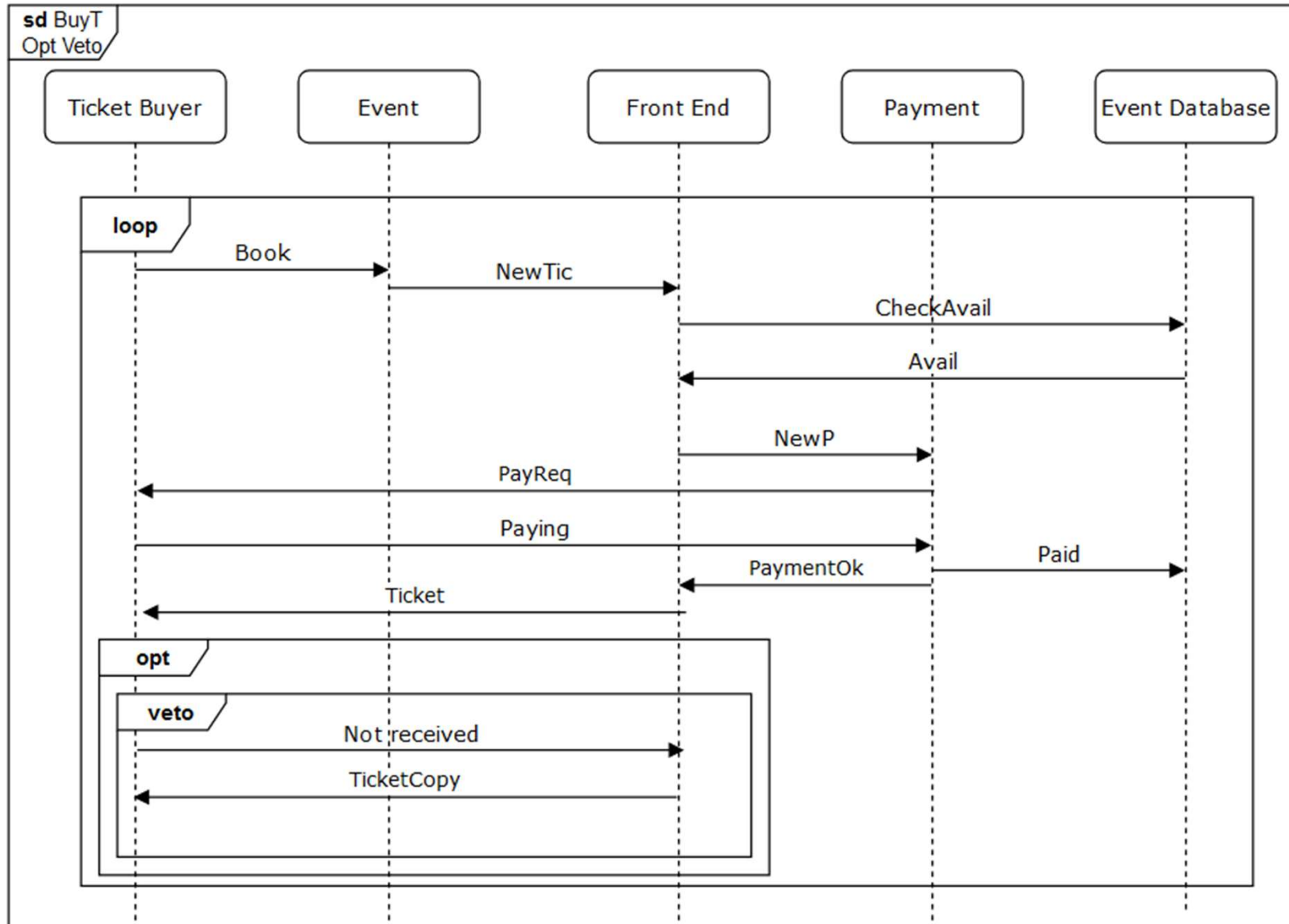
- a) What is the minimum length of a negative trace of sm Event Database? Explain your answer.
- b) How would you alter sm Event Database so that any positive trace of the lifeline Event Database in sd BuyT Veto is also a positive trace of sm Event Database? Explain your answer.
- c) What is/are the possible last event/events of a positive trace of sm Event Database under the assumption that the possible input messages are restricted to those that appear in the diagram (CheckAvail, Paid)? Explain your answer.
- d) What is/are the possible last event/events of a positive trace of sm Event Database in the general case? Explain your answer.
- e) How many traces of length four is a positive trace of sm Event Database under the assumption that the possible input messages are restricted to those that appear in the diagram (CheckAvail, Paid)? Explain your answer.

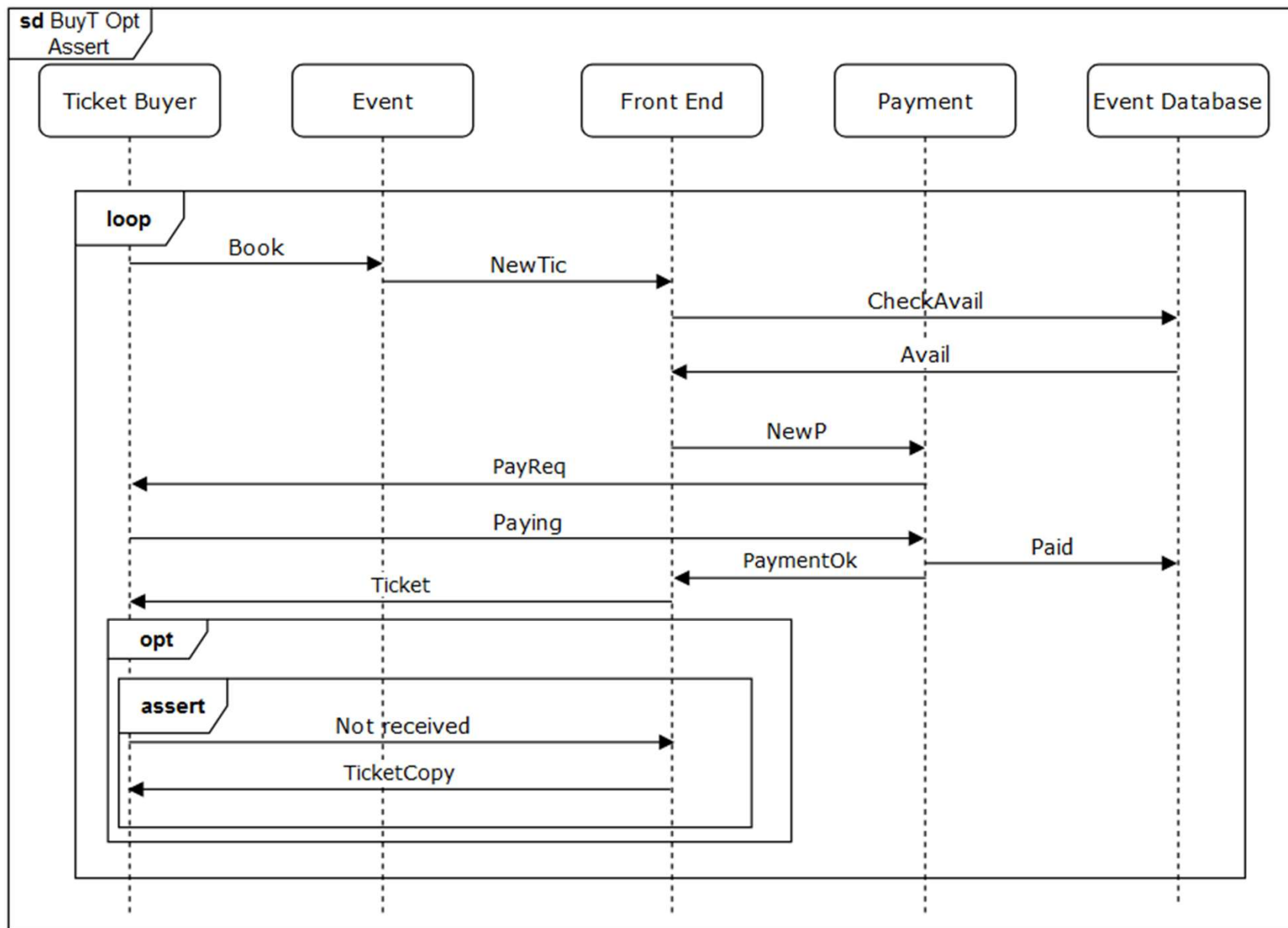
Solution Outline Question 2

- a. 1
 - note that receiving input not specified explicitly and doing nothing is allowed; but sending something without first receiving input is not
- b. Buy removing NewBooking as output
- c. 4 (if question is understood such that implicit transitions are ignored)
 - !Avail, !InProgress, !NotAvail, !NewBooking
 - 2 more (otherwise)
 - ?Paid, ?CheckAvail
- d. In addition to the four above, ?m for any message m
- e. 3 (if question is understood such that implicit transitions are ignored)
 - <?CheckAvail, !Avail, ?Paid, !NewBooking>,
 - <?CheckAvail, !NotAvail, ?CheckAvail, !NotAvail>,
 - <?CheckAvail, !NotAvail, ?CheckAvail, !Avail>
 - 6 more (otherwise)
 - <?Paid, ?Paid, ?Paid, ?Paid>, <?Paid, ?Paid, ?CheckAvail, !NotAvail>,
 - <?Paid, ?Paid, ?CheckAvail, !Avail>, <?Paid, ?CheckAvail, !NotAvail, ?Paid>
 - <?CheckAvail, !NotAvail, ?Paid, ?Paid>, <?CheckAvail, !Avail, <?CheckAvail, <?CheckAvail>



26 with implicit transition



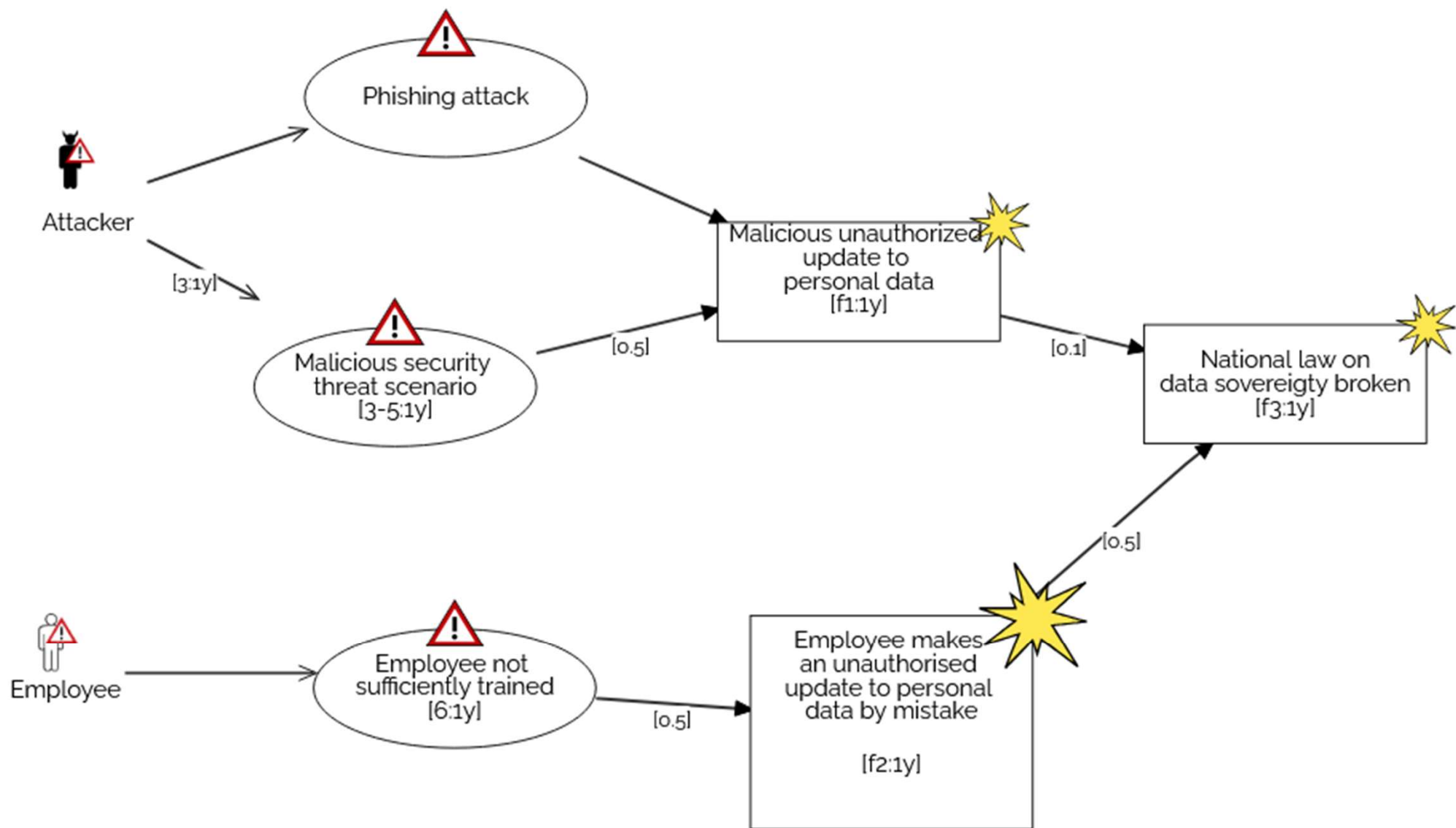


Question 3

- a. Is sd BuyT Opt Veto a refinement of sd BuyT Veto? Explain your answer.
- b. Is sd BuyT Assert a refinement of sd BuyT Veto? If so, what kind? Explain your answer.
- c. Is sd BuyT Veto a refinement of sd BuyT Assert? If so, what kind? Explain your answer.
- d. Is sd BuyT Opt Assert a refinement of sd BuyT Veto? If so, what kind? Explain your answer.
- e. How would you update sm Event Database so that the updated state machine is a pure narrowing of sm Event Database? Explain your answer.

Solution Outline Question 3

- a. Yes, because they are semantically identical
- b. No, because traces are not allowed to move from negative to positive
- c. No, because traces are not allowed to move from negative to positive
- d. No, because traces are not allowed to move from negative to positive
- e. Remove any of the outputs "NotAval", "Avail", "Avail, InProgress", but not all of them



Question 4

- a. Assume we do not know whether the threat diagram is complete. What can we then deduce about the value of f_2 ?
- b. Assume we do not know whether the threat diagram is complete. What can we then deduce about the frequency of the initiate relation starting in Employee?
- c. Assume the threat diagram is complete. What can we then deduce about the value of f_1 ?
- d. Two initiate relations, one threat scenario and one leads-to relation lack likelihoods. How would you update one or more of those so that the diagram is consistent if it is incomplete but inconsistent if it is complete?
- e. Assume the diagram is complete and that $f_1=6$ and $f_2=5$. What can we then deduce about the frequency of the unwanted incident “Malicious unauthorized update to personal data OR Employee makes an unauthorised update to personal data by mistake”?

Solution Outline Question 4

- a. It must be greater or equal to 3
- b. 6:1y is the maximum
- c. 1.5
- d. Assign 3:1y to the initiate relation starting from Employee
- e. 11, since the unwanted incidents are separate