WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

receiving, with at least one processor, transaction data associated with a plurality of transactions of at least one payment account;

detecting, with the at least one processor, at least one attempted attack based on the transaction data;

generating, with the at least one processor, using a deep learning model and a survival model, a fraud risk score for each subperiod of a plurality of subperiods in a time period following the at least one attempted attack based on the transaction data, the fraud risk score for each respective subperiod being associated with a probability that a fraudulent transaction will not occur by the respective subperiod, wherein generating the fraud risk score comprises:

generating, with the at least one processor, at least one embedding for each payment account of the at least one payment account based on inputting the transaction data for the payment account to the deep learning model to provide at least one hidden layer vector, wherein each embedding of the at least one embedding comprises a hidden layer vector of the at least one hidden layer vector; and

generating, with the at least one processor, the fraud risk score for each subperiod based on inputting the at least one embedding to the survival model;

generating, with the at least one processor, a survival curve based on the fraud risk score for each subperiod;

determining, with the at least one processor, an area bounded by the survival curve;

comparing, with the at least one processor, the area to a threshold to determine whether the at least one payment account is in a high risk category; and

sending, with the at least one processor, a notification indicating that the payment account is in a high risk category based on determining the at least one payment account is in the high risk category.

2. The method of claim 1, wherein the transaction data includes all transactions associated with the at least one payment account during a preceding time period.

3. The method of claim 1, wherein the deep learning model comprises at least one of a deep neural network, a recurrent neural network (RNN), a long short term memory (LSTM) network, or any combination thereof.

4. The method of claim 1, wherein the survival model comprises a Cox regression model.

5. The method of claim 1, wherein each subperiod comprises a day and the time period comprises a month.

6. The method of claim 1, further comprising:

rejecting, with the at least one processor, a subsequent transaction based on the fraud risk score.

7. A system, comprising:

at least one processor; and

at least one non-transitory computer-readable medium including one or more instructions that, when executed by the at least one processor, direct the at least one processor to:

receive transaction data associated with a plurality of transactions of at least one payment account;

detect at least one attempted attack based on the transaction data;

generate, using a deep learning model and a survival model, a fraud risk score for each subperiod of a plurality of subperiods in a time period following the at least one attempted attack based on the transaction data, the fraud risk score for each respective subperiod being associated with a probability that a fraudulent transaction will not occur by the respective subperiod, wherein, when

generating the fraud risk score, the at least one processor is programmed or configured to:

generate at least one embedding for each payment account of the at least one payment account based on inputting the transaction data for the payment account to the deep learning model to provide at least one hidden layer vector, wherein each embedding of the at least one embedding comprises a hidden layer vector of the at least one hidden layer vector; and

generate the fraud risk score for each subperiod based on inputting the at least one embedding to the survival model;

generate a survival curve based on the fraud risk score for each subperiod;

determine an area bounded by the survival curve;

compare the area to a threshold to determine whether the at least one payment account is in a high risk category; and

send a notification indicating that the payment account is in a high risk category based on determining the at least one payment account is in the high risk category.

8. The system of claim 7, wherein the deep learning model comprises at least one of a deep neural network, a recurrent neural network (RNN), a long short term memory (LSTM) network, or any combination thereof; and

wherein the survival model comprises a Cox regression model.

9. A computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

receive transaction data associated with a plurality of transactions of at least one payment account;

detect at least one attempted attack based on the transaction data;

generate, using a deep learning model and a survival model, a fraud risk score for each subperiod of a plurality of subperiods in a time period following the at least

one attempted attack based on the transaction data, the fraud risk score for each respective subperiod being associated with a probability that a fraudulent transaction will not occur by the respective subperiod, wherein, when generating the fraud risk score, the one or more instructions cause the at least one processor to:

generate at least one embedding for each payment account of the at least one payment account based on inputting the transaction data for the payment account to the deep learning model to provide at least one hidden layer vector, wherein each embedding of the at least one embedding comprises a hidden layer vector of the at least one hidden layer vector; and

generate the fraud risk score for each subperiod based on inputting the at least one embedding to the survival model;

generate a survival curve based on the fraud risk score for each subperiod;

determine an area bounded by the survival curve;

compare the area to a threshold to determine whether the at least one payment account is in a high risk category; and

send a notification indicating that the payment account is in a high risk category based on determining the at least one payment account is in the high risk category.

10. The computer program product of claim 9, wherein the deep learning model comprises at least one of a deep neural network, a recurrent neural network (RNN), a long short term memory (LSTM) network, or any combination thereof; and

wherein the survival model comprises a Cox regression model.