CLAIMS

1. A computer implemented method for real-time determination of a merchant risk level, the method comprising:

calculating a transaction risk score for each transaction that occurs at a merchant during an hour *h,* wherein *h* is from 1 to 24;

aggregating the transaction risk scores for each transaction the occurred at the merchant during hour *h* to obtain a merchant risk score m_h for the merchant during each hour *h*;

repeating the calculating step and the aggregating step for each hour *h*;

compiling the merchant risk scores m_h to calculate a daily merchant risk score s_i; and,

providing the daily merchant risk score s_i to the merchant.

2. The method of claim 1, wherein the step of aggregating the transaction risk score for each transaction that occurred at the merchant during hour *h*, further comprises calculating a mean of the transaction risk scores for all the transactions that occurred during hour *h*.

3. The method of claim 1, further comprising:

determining a peer group for the merchant, wherein the peer group comprises one or more peer merchants that provide similar goods or services as the merchant;

calculating a transaction risk score for each transaction that occurs at the peer group during an hour *h,* wherein *h* is from 1 to 24;

aggregating the transaction risk score for each transaction that occurs at the peer group during hour *h* to obtain a peer group risk score p_h for the peer group;

repeating the calculating step and the aggregating step for each hour *h*;

compiling the peer group scores p_h to calculate a daily peer group risk score p_i; and,

comparing the daily peer group risk score p_i to the daily merchant risk score s_i.

4. The method of claim 1 further comprising:

using an anomaly detection algorithm to determine if an anomaly exists in the daily merchant risk score s_i; and,

if an anomaly is detected, adding the merchant to a list.

5. The method of claim 4, wherein the anomaly detection algorithm comprises:

determining a first merchant risk level at a time t_n, wherein the first merchant risk level y_n is a running average of the merchant daily risk scores s_i, wherein the first merchant risk level y_n is calculated as,

$$y_n = \sum_{i=1}^{n} e^{-(t_n - t_i)/T} s_i \Big/ \sum_{i=1}^{n} e^{-(t_n - t_i)/T}$$

wherein T is a decay parameter and i is from 1 to n.

determining a second merchant risk level at a time t_{n+1}, wherein the second merchant risk level y_{n+1} is calculated as,

$$y_{n+1} = \sum_{i=1}^{n+1} e^{-(t_{n+1} - t_i)/T} s_i / \sum_{i=1}^{n+1} e^{-(t_{n+1} - t_i)/T}$$

comparing the first merchant risk level y_n to the second merchant risk level y_{n+1},

if the difference between the first merchant risk level y_n and the second merchant risk level y_{n+1} is above a threshold, then an anomaly is identified.

6. The method of claim 1, further comprising:

creating a first entity profile using a first dataset

creating a second entity profile using a second dataset, wherein the second entity profile is created

using the first entity profile and the second entity profile to train a third dataset containing transaction data to determine a probability that a transaction is fraudulent;

converting the probability that the transaction is fraudulent into a transaction risk score.

7. The method of claims 6, wherein the transaction risk score is any of 1 to 100.

8. The method of claim 7, wherein a high transaction risk score indicates a high-risk transaction and a low transaction risk score indicates a low risk transaction.

9. The method of claim 6, wherein the first entity profile comprises one or more of a historical fraud rate, a transaction decline rate, and an average dollar amount.

10. The method of claim 6, wherein the second entity profile comprises user and merchant embeddings.

11. A computer system comprising an input output circuit, a memory for storing computer executable instructions and a processor physically configured according to computer executable instructions, the computer executable instructions implementing a method for real-time determination of a merchant risk level, the method comprising computer executable blocks for:

calculating a transaction risk score for each transaction that occurs at a merchant during an hour *h,* wherein *h* is from 1 to 24;

aggregating the transaction risk scores for each transaction that occurrs at the merchant during hour *h* to obtain a merchant risk score m_h for the merchant during each hour *h*;

repeating the calculating step and the aggregating step for each hour *h*;

compiling the merchant risk scores m_h to calculate a daily merchant risk score s_i; and,

providing the daily merchant risk score s_i to the merchant.

12. The computer system of claim 11, wherein the step of aggregating the transaction risk score for each transaction that occurred at the merchant during hour *h*, further comprises calculating a mean of the transaction risk scores for all the transactions that occurred during hour *h*.

13. The computer system of claim 11, further comprising computer executable instructions for:

determining a peer group for the merchant, wherein the peer group comprises one or more peer merchants that provide similar goods or services as the merchant;

calculating a transaction risk score for each transaction that occurs at the peer group during an hour *h,* wherein *h* is from 1 to 24;

aggregating the transaction risk score for each transaction the occurred at the peer group during hour *h* to obtain a peer group risk score p_h for the peer group;

repeating the calculating step and the aggregating step for each hour *h*;

compiling the peer group scores p_h to calculate a daily peer group risk score p_i; and,

comparing the daily peer group risk score p_i to the daily merchant risk score s_i.

14. The computer system of claim 11, further comprising computer executable instructions for:

using an anomaly detection algorithm to determine if an anomaly exists in the daily merchant risk score s_i; and,

if an anomaly is detected, adding the merchant to a list.

15. The computer system of claim 14, wherein the anomaly detection algorithm comprises computer executable steps for:

determining a first merchant risk level at a time t_n, wherein the first merchant risk level y_n is a running average of the merchant daily risk scores s_i, wherein the first merchant risk level y_n is calculated as,

$$y_n = \sum_{i=1}^{n} e^{-(t_n - t_i)/T} s_i \Big/ \sum_{i=1}^{n} e^{-(t_n - t_i)/T}$$

wherein *T* is a decay parameter and *i* is from 1 to *n*.

determining a second merchant risk level at a time t_{n+1}, wherein the second merchant risk level y_{n+1} is calculated as,

$$y_{n+1} = \sum_{i=1}^{n+1} e^{-(t_{n+1}-t_i)/T} s_i / \sum_{i=1}^{n+1} e^{-(t_{n+1}-t_i)/T}$$

comparing the first merchant risk level y_n to the second merchant risk level y_{n+1},

if the difference between the first merchant risk level y_n and the second merchant risk level y_{n+1} is above a threshold, then an anomaly is identified.

16. The computer system of claim 11, further comprising computer executable instructions for:

creating a first entity profile using a first dataset;

creating a second entity profile using a second dataset, wherein the second entity profile is created;

using the first entity profile and the second entity profile to train a third dataset containing transaction data to determine a probability that a transaction is fraudulent;

converting the probability that the transaction is fraudulent into a transaction risk score.

17. The computer system of claim 16, wherein the transaction risk score is any of 1 to 100.

18. The computer system of claim 17, wherein a high transaction risk score indicates a high-risk transaction and a low transaction risk score indicates a low risk transaction.

19. The computer system of claim 16, wherein the first entity profile comprises one or more of a historical fraud rate, a transaction decline rate, and an average dollar amount.

20. The computer system of claim 16, wherein the second entity profile comprises user and merchant embeddings.