

What is Claimed is:

1. A method of detecting abnormal transaction performed by an abnormal transaction detection server, comprising:

5 collecting a plurality of pieces of transaction data on transfer transactions;

 determining at least one piece of valid transaction data out of the plurality of pieces of transaction data;

 generating a valid transaction pattern based on the at least one piece of
10 determined valid transaction data; and

 determining whether a fraud occurs based on the valid transaction pattern,

 wherein generating the valid transaction pattern includes identifying an additional valid transactor for at least one valid transactor identified in the step
15 of determining the at least one piece of valid transaction data, and

 the valid transaction pattern is a pattern derived from the identified at least one valid transactor.

2. The method of claim 1, wherein the plurality of pieces of
20 transaction data comprises first transaction data including first personal name data and first transaction amount data associated with the first personal name data, and

 the step of determining the at least one piece of valid transaction data comprises:

generating a first transaction score based on the first transaction amount data, and

determining the first transaction data as first valid transaction data if the first transaction score is greater than or equal to a predetermined reference value.

3. The method of claim 2, wherein the generating a first transaction score comprises:

determining largest amount data out of transaction amount data associated with the first personal name data as first maximum transaction amount data, and

generating the first transaction score by using the first maximum transaction amount data and the first transaction amount data.

4. The method of claim 3, wherein the first transaction score is derived by the following <Equation 1>:

<Equation 1>

$$Ts1 = \frac{T1}{Tmax}$$

where Ts1 is the first transaction score, T1 is the first transaction amount data, and Tmax is the first maximum transaction amount data.

5. The method of claim 3, wherein the first transaction score is derived by the following <Equation 2>:

<Equation 2>

$$Ts1 = \frac{\log (T1)}{\log (Tmax)}$$

where Ts1 is the first transaction score, T1 is the first transaction amount
5 data, and Tmax is the first maximum transaction amount data.

6. The method of claim 2, wherein the first personal name data
comprises data on a first sender and a first recipient of the first transaction data,
and
10 the first transaction amount data corresponds to a cumulative total of
amounts transferred by the first sender to the first recipient.

7. The method of claim 1, wherein the step of generating the valid
transaction pattern comprises:
15 determining a first transactor,
determining at least one transaction that satisfies a predetermined
criterion out of first transaction data associated with the first transactor as first
valid transaction data, and
determining a second transactor that is associated with the first valid
20 transaction data and that is different from the first transactor.

8. The method of claim 7, wherein the step of generating the valid
transaction pattern further comprises:
determining at least one that satisfies the predetermined criterion out of

second transaction data associated with the second transactor as second valid transaction data, and

determining a third transactor that is associated with the second valid transaction data and that is different from the second transactor as the additional
5 valid transactor.

9. The method of claim 8, wherein the valid transaction pattern comprises a pattern schematized using the first and second valid transaction data.
10

10. The method of claim 1, wherein the step of determining whether a fraud occurs comprises:

determining whether a fraud occurs by comparing the valid transaction pattern with a predetermined fraud pattern, and

15 The method further comprises a step of providing a notification to a preset manager terminal if the fraud occurs.

11. The method of claim 1, wherein the step of determining whether a fraud occurs comprises:

20 deriving a fraud probability indicating a probability that a fraud will occur with respect to the valid transaction pattern by using a pre-trained deep learning module, based on the valid transaction pattern, and

The method further comprises a step of providing a notification to a preset manager terminal if the fraud probability is higher than a predetermined

reference value.

12. The method of claim 11, wherein the deep learning module comprises:

5 an input layer using data related to the valid transaction pattern as an input node;

an output layer using the fraud probability as an output node; and

one or more hidden layers arranged between the input layer and the output layer,

10 wherein weights of nodes and edges between the input node and the output node are updated by a training process of the deep learning module.

13. The method of claim 11, wherein the deep learning module derives modeling data most similar to the inputted valid transaction pattern by
15 using graphic neural networks, and outputs the fraud probability based on this.

14. A fraud detection server comprising:

a data collector configured to collect a plurality of pieces of transaction data on transfer transactions;

20 a data processor configured to determine at least one piece of valid transaction data out of the plurality of pieces of transaction data and to generate a valid transaction pattern by using the valid transaction data determined; and

a fraud determinator configured to determine whether a fraud occurs based on the valid transaction pattern,

wherein the data processor generates the valid transaction pattern by identifying an additional valid transactor for at least one valid transactor identified in the step of determining the at least one piece of valid transaction data, and

- 5 the valid transaction pattern is a pattern derived from the identified at least one valid transactor.