WHAT IS CLAIMED IS:

1. A computer-implemented method for detecting collusive transaction fraud, comprising:

generating, with at least one processor, a merchant baseline based on a merchant category code associated with a first merchant system operating in an electronic payment processing network, the merchant baseline comprising: (i) a transaction data baseline comprising transaction data baseline data associated with a plurality of merchant systems having the merchant category code; and (ii) a time series baseline comprising time series baseline data associated with a plurality of merchant systems having the merchant category code;

extracting, with the at least one processor, time series data associated with the first merchant system;

generating, with the at least one processor, a first score based on comparing transaction data associated with the first merchant system to the transaction data baseline with a deep learning model;

generating, with the at least one processor, a second score based on comparing the time series data associated with the first merchant system to the time series baseline with the deep learning model;

generating, with the at least one processor, a first merchant risk score associated with the first merchant system based on the first score and the second score;

determining, with the at least one processor, that the first merchant risk score satisfies a threshold;

in response to determining that the first merchant risk score satisfies the threshold, determining, with the at least one processor, a plurality of related entities related to the first merchant system; and

classifying, with the at least one processor, the first merchant system and at least one related entity of the plurality of related entities in a first group risk class based on at least one risk score associated with the at least one related entity.

2. The computer-implemented method of claim 1, wherein the plurality of related entities comprise at least one of the following: an acquirer system associated with the first merchant system, a second merchant system associated with

the acquirer system associated with the first merchant system, and a payment device which initiated a payment transaction with the first merchant system.

3. The computer-implemented method of claim 1, further comprising:

in response to classifying the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class, placing, with the at least one processor, a hold on transaction activity conducted by at least one of the first merchant system and the at least one related entity of the plurality of related entities.

4. The computer-implemented method of claim 1, further comprising:

in response to classifying the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class, automatically initiating, with the at least one processor, an investigation protocol.

5. The computer-implemented method of claim 1, further comprising:

determining, with the at least one processor, that the merchant category code associated with the first merchant system is miscoded;

determining, with the at least one processor, a corrected merchant category code associated with the first merchant system; and

modifying, with the at least one processor, the merchant category code associated with the first merchant system to the corrected merchant category code.

6. The computer-implemented method of claim 5, further comprising:

determining, with the at least one processor, a region code associated with the first merchant system; and

detecting illicit transaction activity of the first merchant system based on the corrected merchant category code and the region code.

7. The computer-implemented method of claim 1, further comprising:

identifying, with the at least one processor, at least one payment transaction conducted between the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class;

determining, with the at least one processor, that the at least one payment transaction is a cross-border payment transaction associated with a first region and a second region;

generating, with at least one processor, a transaction risk score associated with the at least one payment transaction based on at least one of the following: a status of the at least one payment transaction as a cross-border payment transaction, the first region, the second region, and the merchant category code;

determining, with the at least one processor, that the transaction risk score satisfies a threshold; and

classifying, with the at least one processor, the at least one payment transaction in a first transaction risk class in response to determining that the transaction risk score satisfies the threshold.

8. A system for detecting collusive transaction fraud, comprising at least one processor programmed or configured to:

generate a merchant baseline based on a merchant category code associated with a first merchant system operating in an electronic payment processing network, the merchant baseline comprising: (i) a transaction data baseline comprising transaction data baseline data associated with a plurality of merchant systems having the merchant category code; and (ii) a time series baseline comprising time series baseline data associated with a plurality of merchant systems having the merchant category code;

extract time series data associated with the first merchant system;

generate a first score based on comparing transaction data associated with the first merchant system to the transaction data baseline with a deep learning model;

generate a second score based on comparing the time series data associated with the first merchant system to the time series baseline with the deep learning model;

generate a first merchant risk score associated with the first merchant system based on the first score and the second score;

determine that the first merchant risk score satisfies a threshold;

in response to determining that the first merchant risk score satisfies the threshold, determine a plurality of related entities related to the first merchant system; and

classify the first merchant system and at least one related entity of the plurality of related entities in a first group risk class based on at least one risk score associated with the at least one related entity.

9. The system of claim 8, wherein the plurality of related entities comprise at least one of the following: an acquirer system associated with the first merchant system, a second merchant system associated with the acquirer system associated with the first merchant system, and a payment device which initiated a payment transaction with the first merchant system.

10. The system of claim 8, wherein the at least one processor is further programmed or configured to:

in response to classifying the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class, place a hold on transaction activity conducted by at least one of the first merchant system and the at least one related entity of the plurality of related entities.

11. The system of claim 8, wherein the at least one processor is further programmed or configured to:

in response to classifying the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class, automatically initiate an investigation protocol.

12. The system of claim 8, wherein the at least one processor is further programmed or configured to:

determine that the merchant category code associated with the first merchant system is miscoded;

determine a corrected merchant category code associated with the first merchant system; and

modify the merchant category code associated with the first merchant system to the corrected merchant category code.

13. The system of claim 12, wherein the at least one processor is further programmed or configured to:

determine a region code associated with the first merchant system; and

detect illicit transaction activity of the first merchant system based on the corrected merchant category code and the region code.

14. The system of claim 8, wherein the at least one processor is further programmed or configured to:

identify at least one payment transaction conducted between the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class;

determine that the at least one payment transaction is a cross-border payment transaction associated with a first region and a second region;

generate a transaction risk score associated with the at least one payment transaction based on at least one of the following: a status of the at least one payment transaction as a cross-border payment transaction, the first region, the second region, and the merchant category code;

determine that the transaction risk score satisfies a threshold; and

classify the at least one payment transaction in a first transaction risk class in response to determining that the transaction risk score satisfies the threshold.

15. A computer program product for detecting collusive transaction fraud, the 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:

generate a merchant baseline based on a merchant category code associated with a first merchant system operating in an electronic payment processing network, the merchant baseline comprising: (i) a transaction data baseline comprising transaction data baseline data associated with a plurality of merchant systems having

the merchant category code; and (ii) a time series baseline comprising time series baseline data associated with a plurality of merchant systems having the merchant category code;

extract time series data associated with the first merchant system;

generate a first score based on comparing transaction data associated with the first merchant system to the transaction data baseline with a deep learning model;

generate a second score based on comparing the time series data associated with the first merchant system to the time series baseline with the deep learning model;

generate a first merchant risk score associated with the first merchant system based on the first score and the second score;

determine that the first merchant risk score satisfies a threshold;

in response to determining that the first merchant risk score satisfies the threshold, determine a plurality of related entities related to the first merchant system; and

classify the first merchant system and at least one related entity of the plurality of related entities in a first group risk class based on at least one risk score associated with the at least one related entity.

16. The computer program product of claim 15, wherein the plurality of related entities comprise at least one of the following: an acquirer system associated with the first merchant system, a second merchant system associated with the acquirer system associated with the first merchant system, and a payment device which initiated a payment transaction with the first merchant system.

17. The computer program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

in response to classifying the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class, place a hold on transaction activity conducted by at least one of the first merchant system and the at least one related entity of the plurality of related entities.

18. The computer program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

in response to classifying the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class, automatically initiate an investigation protocol.

19. The computer program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

determine that the merchant category code associated with the first merchant system is miscoded;

determine a corrected merchant category code associated with the first merchant system; and

modify the merchant category code associated with the first merchant system to the corrected merchant category code.

20. The computer program product of claim 19, wherein the one or more instructions further cause the at least one processor to:

determine a region code associated with the first merchant system; and

detect illicit transaction activity of the first merchant system based on the corrected merchant category code and the region code.

21. The computer program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

identify at least one payment transaction conducted between the first merchant system and the at least one related entity of the plurality of related entities in the first group risk class;

determine that the at least one payment transaction is a cross-border payment transaction associated with a first region and a second region;

generate a transaction risk score associated with the at least one payment transaction based on at least one of the following: a status of the at least one payment transaction as a cross-border payment transaction, the first region, the second region, and the merchant category code;

determine that the transaction risk score satisfies a threshold; and

classify the at least one payment transaction in a first transaction risk class in response to determining that the transaction risk score satisfies the threshold.