

WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:
receiving, with at least one processor, transaction data associated with a plurality of transactions;
determining, with at least one processor, based on the transaction data, that two or more consecutive transactions associated with a same account identifier include a value for a same at least one transaction parameter;
in response to determining that each of the two or more consecutive transactions associated with the same account identifier include the value for the same at least one transaction parameter, determining, with at least one processor, a difference between the value for the at least one transaction parameter associated with a first transaction of the two or more consecutive transactions and the value for the at least one transaction parameter associated with a second transaction of the two or more consecutive transactions; and
determining, with at least one processor, based on the difference, that the two or more consecutive transactions are fraudulent transactions.
2. The computer-implemented method of claim 1, wherein the transaction data includes in-network transaction data associated with at least one in-network transaction processed in a transaction processing network and out-of-network transaction data associated with at least one out-of-network transaction processed outside of the transaction processing network.
3. The computer-implemented method of claim 2, wherein the in-network transaction data is received from a transaction service provider system inside the transaction processing network, and wherein the out-of-network transaction data is received from at least one of a merchant system outside of the transaction processing network and an issuer system outside of the transaction processing network.
4. The computer-implemented method of claim 2, wherein the first transaction includes the at least one out-of-network transaction, and wherein the second transaction includes the at least one in-network transaction.

5. The computer-implemented method of claim 4, further comprising:
in response to determining that the out-of-network transaction and the in-network transaction are fraudulent transactions, denying, with at least one processor, authorization of the in-network transaction processed in the transaction processing network.

6. The computer-implemented method of claim 4, further comprising:
in response to determining that the out-of-network transaction and the in-network transaction are fraudulent transactions, providing, with at least one processor, a notification to an issuer system associated with the out-of-network transaction, wherein the notification includes an indication that the out-of-network transaction is a fraudulent transaction.

7. The computer-implemented method of claim 1, wherein the at least one transaction parameter includes at least one of the following: a geographic location, a merchant category code (MCC), a transaction time, a transaction amount, or any combination thereof.

8. A computing system comprising:
one or more processors programmed and/or configured to:
receive transaction data associated with a plurality of transactions;
determine based on the transaction data, that two or more consecutive transactions associated with a same account identifier include a value for a same at least one transaction parameter;
in response to determining that each of the two or more consecutive transactions associated with the same account identifier include the value for the same at least one transaction parameter, determine, a difference between the value for the at least one transaction parameter associated with a first transaction of the two or more consecutive transactions and the value for the at least one transaction parameter associated with a second transaction of the two or more consecutive transactions; and

determine, based on the difference, that the two or more consecutive transactions are fraudulent transactions.

9. The computing system of claim 8, wherein the transaction data includes in-network transaction data associated with at least one in-network transaction processed in a transaction processing network and out-of-network transaction data associated with at least one out-of-network transaction processed outside of the transaction processing network.

10. The computing system of claim 9, wherein the in-network transaction data is received from a transaction service provider system inside the transaction processing network, and wherein the out-of-network transaction data is received from at least one of a merchant system outside of the transaction processing network and an issuer system outside of the transaction processing network.

11. The computing system of claim 9, wherein the first transaction includes the at least one out-of-network transaction, and wherein the second transaction includes the at least one in-network transaction.

12. The computing system of claim 11, wherein the one or more processors are further programmed and/or configured to:

in response to determining that the out-of-network transaction and the in-network transaction are fraudulent transactions, deny authorization of the in-network transaction processed in the transaction processing network.

13. The computing system of claim 11, wherein the one or more processors are further programmed and/or configured to:

in response to determining that the out-of-network transaction and the in-network transaction are fraudulent transactions, provide a notification to an issuer system associated with the out-of-network transaction, wherein the notification includes an indication that the out-of-network transaction is a fraudulent transaction.

14. The computing system of claim 8, wherein the at least one transaction parameter includes at least one of the following: a geographic location, a

merchant category code (MCC), a transaction time, a transaction amount, or any combination thereof.

15. A computer program product comprising at least one non-transitory computer-readable medium including program 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;

determine based on the transaction data, that two or more consecutive transactions associated with a same account identifier include a value for a same at least one transaction parameter;

in response to determining that each of the two or more consecutive transactions associated with the same account identifier include the value for the same at least one transaction parameter, determine, a difference between the value for the at least one transaction parameter associated with a first transaction of the two or more consecutive transactions and the value for the at least one transaction parameter associated with a second transaction of the two or more consecutive transactions; and

determine, based on the difference, that the two or more consecutive transactions are fraudulent transactions.

16. The computer program product of claim 15, wherein the transaction data includes in-network transaction data associated with at least one in-network transaction processed in a transaction processing network and out-of-network transaction data associated with at least one out-of-network transaction processed outside of the transaction processing network.

17. The computer program product of claim 16, wherein the in-network transaction data is received from a transaction service provider system inside the transaction processing network, and wherein the out-of-network transaction data is received from at least one of a merchant system outside of the transaction processing network and an issuer system outside of the transaction processing network.

18. The computer program product of claim 16, wherein the first transaction includes the at least one out-of-network transaction, and wherein the second transaction includes the at least one in-network transaction.

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

in response to determining that the out-of-network transaction and the in-network transaction are fraudulent transactions, denying, with at least one processor, authorization of the in-network transaction processed in the transaction processing network.

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

in response to determining that the out-of-network transaction and the in-network transaction are fraudulent transactions, providing, with at least one processor, a notification to an issuer system associated with the out-of-network transaction, wherein the notification includes an indication that the out-of-network transaction is a fraudulent transaction.