

What is claimed is:

1. A computer-implemented method comprising:
in response to a test transaction initiated through a virtual card provided to a merchant, receiving, with at least one processor, test transaction data from an acquirer bank of the merchant, wherein the acquirer bank receives the test transaction data from a remote terminal of the merchant;
detecting, in real-time and with at least one processor, a record of the test transaction in a transaction database associated with a card processing server using one or more attributes of the virtual card stored in the card processing server;
in response to detecting the record of the test transaction, retrieving, with at least one processor, signature data from the test transaction data stored in the transaction database; and
determining, with at least one processor, transaction source data of the merchant based on the signature data, wherein the transaction source data comprises location of the merchant at which the test transaction was initiated and a registered name of the merchant.
2. The computer-implemented method of claim 1, wherein the test transaction data is received by the card processing server when the acquirer bank authorizes the test transaction initiated through the virtual card.
3. The computer-implemented method of claim 1, wherein the test transaction data and the signature data comprise at least one of the following: virtual card data, a Bank Identification Number (BIN), a Card Acceptor Identifier (CAID) of the merchant, a merchant name, a Merchant Category Code (MCC), a Primary Account Number (PAN) used in the test transaction, a partial geolocation of the merchant, a merchant ID, a store ID of the merchant, transaction amount, date of transaction, an authentication code, or any combination thereof.
4. The computer-implemented method of claim 3, wherein the virtual card data comprises one or more attributes of the virtual card, wherein the one or more attributes comprise at least one of the following: a virtual card number, a name of a

cardholder, a virtual card verification value, an expiration date of the virtual card, a purpose of the virtual card, or any combination thereof.

5. The computer-implemented method of claim 1, wherein the test transaction is initiated when the virtual card is communicatively interfaced with the remote terminal.

6. The computer-implemented method of claim 1, wherein determining the transaction source data and the registered name of the merchant comprises:

comparing, with at least one processor, at least one of a merchant name of the signature data, a CAID of the merchant of the signature data, and a partial geolocation of the merchant of the signature data with transaction data stored in the transaction database;

extracting, with at least one processor, records of one or more transactions from the transaction data based on the comparison, wherein the extracted records of the one or more transactions are a complete match or a partial match to at least one of the merchant name of the signature data, the CAID of the merchant of the signature data, and the partial geolocation of the merchant of the signature data, used for the comparison; and

correlating, with at least one processor, each of the extracted records of the one or more transactions and the signature data of the merchant to determine the transaction source data.

7. The computer-implemented method of claim 6, wherein the transaction data comprises the records of one or more transactions performed at one or more merchant locations of a plurality of merchants.

8. A card processing server comprising:
at least one processor; and
a memory communicatively coupled to the at least one processor, wherein the memory stores processor-executable instructions, which, on execution, causes the at least one processor to:

in response to a test transaction initiated through a virtual card provided to a merchant, receive test transaction data from an acquirer bank of the merchant, wherein the acquirer bank receives the test transaction data from a remote terminal of the merchant;

detect, in real-time, a record of the test transaction in a transaction database associated with a card processing server using one or more attributes of the virtual card stored in the card processing server;

in response to detecting the record of the test transaction, retrieve signature data from the test transaction data stored in the transaction database; and

determine transaction source data of the merchant based on the signature data, wherein the transaction source data comprises location of the merchant at which the test transaction was initiated and a registered name of the merchant.

9. The card processing server of claim 8, wherein the test transaction data is received by the card processing server when the acquirer bank authorizes the test transaction initiated through the virtual card.

10. The card processing server of claim 8, wherein the test transaction data and the signature data comprise at least one of the following: virtual card data, a Bank Identification Number (BIN), a Card Acceptor Identifier (CAID) of the merchant, a merchant name, a Merchant Category Code (MCC), a Primary Account Number (PAN) used in the test transaction, a partial geolocation of the merchant, a merchant ID, a store ID of the merchant, transaction amount, date of transaction, an authentication code, or any combination thereof.

11. The card processing server of claim 10, wherein the virtual card data comprises one or more attributes of the virtual card, wherein the one or more attributes comprise at least one of the following: a virtual card number, a name of a cardholder, a virtual card verification value, an expiration date of the virtual card, a purpose of the virtual card, or any combination thereof.

12. The card processing server of claim 8, wherein the at least one processor initiates the test transaction when the virtual card is communicatively interfaced with the remote terminal.

13. The card processing server of claim 8, wherein the at least one processor determines the transaction source data and the registered name of the merchant by:

comparing, with at least one processor, at least one of a merchant name of the signature data, a CAID of the merchant of the signature data, and a partial geolocation of the merchant of the signature data with transaction data stored in the transaction database;

extracting, with at least one processor, records of one or more transactions from the transaction data based on the comparison, wherein the extracted records of the one or more transactions are a complete match or a partial match to at least one of the merchant name of the signature data, the CAID of the merchant of the signature data, and the partial geolocation of the merchant of the signature data, used for the comparison; and

correlating, with at least one processor, each of the extracted records of the one or more transactions and the signature data of the merchant to determine the transaction source data.

14. The card processing server of claim 13, wherein the transaction data comprises the records of one or more transactions performed at one or more merchant locations of a plurality of merchants.

15. A non-transitory computer readable medium including instructions stored thereon that when processed by at least one processor causes a card processing server to perform operations comprising:

in response to a test transaction initiated through a virtual card provided to a merchant, receiving, with at least one processor, test transaction data from an acquirer bank of the merchant, wherein the acquirer bank receives the test transaction data from a remote terminal of the merchant;

detecting, in real-time and with at least one processor, a record of the test transaction in a transaction database associated with a card processing server using one or more attributes of the virtual card stored in the card processing server;

in response to detecting the record of the test transaction, retrieving, with at least one processor, signature data from the test transaction data stored in the transaction database; and

determining, with at least one processor, transaction source data of the merchant based on the signature data, wherein the transaction source data comprises location of the merchant at which the test transaction was initiated and a registered name of the merchant.

16. The non-transitory computer readable medium of claim 15, wherein the test transaction data and the signature data comprise at least one of the following: virtual card data, a Bank Identification Number (BIN), a Card Acceptor Identifier (CAID) of the merchant, a merchant name, a Merchant Category Code (MCC), a Primary Account Number (PAN) used in the test transaction, a partial geolocation of the merchant, a merchant ID, a store ID of the merchant, transaction amount, date of transaction, an authentication code, or any combination thereof.

17. The non-transitory computer readable medium of claim 16, wherein the virtual card data comprises one or more attributes of the virtual card, wherein the one or more attributes comprise at least one of the following: a virtual card number, a name of a cardholder, a virtual card verification value, an expiration date of the virtual card, a purpose of the virtual card, or any combination thereof.

18. The non-transitory computer readable medium of claim 15, wherein the test transaction is initiated when the virtual card is communicatively interfaced with the remote terminal.

19. The non-transitory computer readable medium of claim 15, wherein, to determine the transaction source data and the registered name of the merchant, the instructions cause the at least one processor to:

compare at least one of a merchant name of the signature data, a CAID of the merchant of the signature data, and a partial geolocation of the merchant of the signature data with the test transaction data stored in the transaction database;

extract records of one or more transactions from the transaction data based on the comparison, wherein the extracted records of the one or more transactions are a complete match or a partial match to at least one of the merchant name of the signature data, the CAID of the merchant of the signature data, and the partial geolocation of the merchant of the signature data, used for the comparison; and

correlate each of the extracted records of the one or more transactions and the signature data of the merchant to determine the transaction source data.

20. The non-transitory computer readable medium of claim 19, wherein the transaction data comprises the records of one or more transactions performed at one or more merchant locations of a plurality of merchants.