Claims

1. An issuer server of an issuer for processing a card-not-present (CNP) transaction, the issuer server comprising:

a computer processor and a data storage device, the data storage device including executable instructions which, when executed by the computer processor, cause the issuer server to:

receive, from an acquirer associated with a merchant, via a payment network associated with a payment card issued to a consumer by the issuer, an authorization request for a card-not-present (CNP) transaction for one or more products, the authorization request including a credential for the payment card and a delivery address for the one or more products;

based on the credential, retrieve, from a database in communication with the issuer server, an address registered in association with the credential, the database including a plurality of addresses registered for a plurality of payment card credentials;

compare the delivery address with the registered address; and

in response to the delivery address not matching the registered address:

generate a verification request for at least one personal identifier associated with the credential for the payment card;

send the verification request to a communication device associated with the consumer, to thereby solicit the at least one personal identifier from the consumer;

receive, from the communication device, a verification response including at least one personal identifier input;

in response to the at least one personal identifier input matching the at least one personal identifier, generate a second-factor authorization response including an indication that the CNP transaction is to proceed; and

in response to the at least one personal identifier input not matching the at least one personal identifier, decline the CNP transaction.

2. The issuer server of claim 1, wherein the executable instructions, when executed by the computer processor, further cause the issuer server to compare the at least one personal identifier input with the at least one personal identifier.

3. The issuer server of claim 1, wherein the authorisation request further includes an amount for the CNP transaction; and

wherein the executable instructions, when executed by the computer processor, further cause the issuer server to:

determine whether the amount is greater than or equal to a transaction threshold, the transaction threshold associated with the credential for the payment card; and

in response to the amount being greater than or equal to the transaction threshold, include at least another personal identifier or a more complex personal identifier in the verification request.

4. The issuer server of claim 1, wherein the executable instructions, when executed by the computer processor, further cause the issuer server to:

calculate a transaction frequency with which the credential for the payment card is used for CNP transactions;

determine whether the transaction frequency is greater than or equal to a transaction frequency threshold, the transaction frequency threshold being associated with the credential for the payment card; and

in response to the transaction frequency being greater than or equal to the transaction frequency threshold, include at least another personal identifier or a more complex personal identifier in the verification request.

5. The issuer server of claim 1, wherein the at least one personal identifier includes at least one of: a personal identification number (PIN), a one-time password (OTP), a gesture, a name of a childhood friend, a wedding anniversary date and/or a biometric identifier.

6. A computer-implemented method for processing a card-not-present (CNP) transaction, the method comprising:

receiving, by an issuer server, from an acquirer associated with a merchant, via a payment network associated with a payment card, an authorisation request for a CNP transaction involving the payment card, the authorisation request including a credential for the payment card and a delivery address;

based on the credential, retrieving, by the issuer server, from a database in communication with the issuer server, a registered address associated with the credential for;

comparing, by the issuer server, the delivery address with the registered address; and

in response to the delivery address not matching the registered address:

generating, by the issuer server, a verification request for at least one personal identifier associated with the credential for the payment card;

sending, by the issuer server, the verification request;

receiving, by the issuer server, a verification response including at least one personal identifier input;

comparing, by the issuer server, the at least one personal identifier input with the at least one personal identifier; and

in response to the at least one personal identifier input matching the at least one personal identifier, generating, by the issuer server, a second-factor authorization response, the second-factor authorisation response including an indication that the CNP transaction is to proceed despite the delivery address not matching the registered address.

7. The method of claim 6, wherein the authorisation request further includes a transaction amount associated with the CNP transaction; and

wherein generating the verification request further includes:

determining, by the issuer server, whether the transaction amount is greater than or equal to a transaction threshold, the transaction threshold being associated with the credential for the payment card; and

in response to the transaction amount being greater than or equal to the transaction threshold, including, by the issuer server, a request for at least another personal identifier or a more complex personal identifier in the verification request.

8. The method of claim 7, wherein generating the verification request further includes:

calculating, by the issuer server, a transaction frequency with which the credential for the payment card is used for CNP transactions;

determining, by the issuer server, whether the transaction frequency is greater than or equal to a transaction frequency threshold, the transaction frequency threshold being associated with the credential for the payment card; and

in response to the transaction frequency being greater than or equal to the transaction frequency threshold, including, by the issuer server, a request for at least another personal identifier or a more complex personal identifier in the verification request.

9. The method of claim 6, wherein retrieving the registered address associated with the indication of the payment card number includes querying a database to ascertain the registered address associated with the credential for the payment card, the database being operationally connected to the issuer server.

10. A non-transitory computer-readable storage medium including executable instructions, which, when executed by at least one processor of an issuer, cause the at least one processor of the issuer to:

receive, from an acquirer associated with a merchant, via a payment network associated with a payment card, an authorization request for a card-not-present (CNP) transaction involving the payment card, the authorization request including a credential for the payment card and a delivery address;

based on the credential for the payment card, retrieve a registered address associated with the credential; compare the delivery address with the registered address; and in response to the delivery address not matching the registered address: generate a verification request for at least one personal identifier associated with the credential for the payment card;

send the verification request to a communication device; receive, from the communication device, a verification response including at least one personal identifier input; in response to the at least one personal identifier input matching the at least one personal identifier, generate a second-factor authorization response including an indication that the CNP transaction is to proceed; and

in response to the at least one personal identifier input not matching the at least one personal identifier, decline the CNP transaction.

11. The non-transitory computer-readable storage medium of claim 10, wherein the executable instructions, when executed by the at least one processor, further cause the at least one processor to compare the at least one personal identifier input with the at least one personal identifier.

12. The issuer of claim 1, wherein the executable instructions, when executed by the computer processor, further cause the computer processor to, in response to the delivery address matching the registered address, generate an authorization response including an indication that the CNP transaction is to proceed.

13. The method of claim 6, further comprising, in response to the delivery address matching the registered address, generating, by the issuer server, an authorization response including an indication that the CNP transaction is to proceed.

14. The non-transitory computer-readable storage medium of claim 10, wherein the executable instructions, when executed by the at least one processor, further cause the at least one processor to, in response to the delivery address matching the registered

address, generate an authorization response including an indication that the CNP transaction is to proceed.