WHAT IS CLAIMED IS

1. A computer-implemented method comprising:

prompting, with at least one processor of a payment gateway configured in an electronic payment processing network, a client device of a consumer to generate a public-private key pair comprising a private key and a public key;

receiving, with at least one processor of the payment gateway, the public key and a primary account number (PAN) of an account of the consumer from the client device;

transmitting, with at least one processor of the payment gateway, the public key and the PAN to a transaction processing system for storage of the public key in association with a device identifier, wherein the transaction processing system is configured in the electronic payment processing network as separate from the payment gateway;

receiving, with at least one processor of the payment gateway, via a merchant interface of a merchant operated on the client device, a transaction request for a transaction between the account of the consumer and an account of the merchant, the transaction request comprising the PAN;

determining, with at least one processor of the payment gateway, whether the PAN has been registered with the public key for use in a client device authentication process;

in response to determining that the PAN has been registered with the public key of the public-private key pair of the client device of the consumer, causing the transaction processing system to cryptographically authenticate the client device based on the public key by transmitting, with at least one processor of the payment gateway, a login request to the transaction processing system comprising the device identifier of the client device based on the PAN;

receiving, with at least one processor of the payment gateway, a login response from the transaction processing system associated with successful cryptographic authentication of the client device based on the public key of the public-private key pair of the client device; and

in response to receiving the login response associated with the successful cryptographic authentication of the client device, processing, with at least one processor of the payment gateway, the transaction by generating a transaction

authorization request message comprising the PAN to the transaction processing system.

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

transmitting, with at least one processor of the payment gateway, a consumer authentication request message to an issuer system associated with an issuer of the account of the consumer, wherein the consumer authentication request message comprises data of the client device authentication process, and wherein the issuer system is configured in the electronic payment processing network as separate from the payment gateway and the transaction processing system; and

receiving, with at least one processor of the payment gateway, a consumer authentication response message from the issuer system indicating successful authentication of the consumer, wherein the transaction is processed further in response to receipt of the consumer authentication response message.

3. The computer-implemented method of claim 1, wherein the login response comprises data indicating that the public key of the public-private key pair of the client device was successfully matched with the private key of the public-private key pair stored on the client device, through execution of the client device authentication process.

4. The computer-implemented method of claim 1, further comprising receiving, with at least one processor of the payment gateway, an initial request from a merchant system for the payment gateway to process the transaction, wherein the initial request comprises the PAN.

5. The computer-implemented method of claim 4, wherein the transaction is an online, card-not-present transaction between the consumer and the merchant associated with the merchant system.

6. A system, comprising:

at least one processor of a payment gateway configured in an electronic payment processing network; and

at least one non-transitory computer-readable medium including one or more instructions that, when executed by the at least one processor, cause the at least one processor to:

prompt a client device of a consumer to generate a public-private key pair comprising a private key and a public key;

receive the public key and a primary account number (PAN) of an account of the consumer from the client device;

transmit the public key and the PAN to a transaction processing system for storage of the public key in association with a device identifier, wherein the transaction processing system is configured in the electronic payment processing network as separate from the payment gateway;

receive, via a merchant interface of a merchant operated on the client device, a transaction request for a transaction between the account of the consumer and an account of the merchant, the transaction request comprising the PAN;

determine whether the PAN has been registered with the public key for use in a client device authentication process;

in response to determining that the PAN has been registered with the public key of the public-private key pair of the client device of the consumer, cause the transaction processing system to cryptographically authenticate the client device based on the public key by transmitting a login request to the transaction processing system comprising the device identifier of the client device based on the PAN;

receive a login response from the transaction processing system associated with successful cryptographic authentication of the client device based on the public key of the public-private key pair of the client device; and

in response to receiving the login response associated with the successful cryptographic authentication of the client device, process the transaction by generating a transaction authorization request message comprising the PAN to the transaction processing system.

7. The system of claim 6, wherein the one or more instructions further cause the at least one processor to:

transmit a consumer authentication request message to an issuer system associated with an issuer of the account of the consumer, wherein the

consumer authentication request message comprises data of the client device authentication process, and wherein the issuer system is configured in the electronic payment processing network as separate from the payment gateway and the transaction processing system; and

receive a consumer authentication response message from the issuer system indicating successful authentication of the consumer, wherein the transaction is processed further in response to receipt of the consumer authentication response message.

8. The system of claim 6, wherein the login response comprises data indicating that the public key of the public-private key pair of the client device was successfully matched with the private key of the public-private key pair stored on the client device, through execution of the client device authentication process.

9. The system of claim 6, wherein the one or more instructions further cause the at least one processor to receive an initial request from a merchant system for the payment gateway to process the transaction, wherein the initial request comprises the PAN.

10. The system of claim 9, wherein the transaction is an online, card-not-present transaction between the consumer and the merchant associated with the merchant system.

11. A 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 of a payment gateway configured in an electronic payment processing network, cause the at least one processor to:

prompt a client device of a consumer to generate a public-private key pair comprising a private key and a public key;

receive the public key and a primary account number (PAN) of an account of the consumer from the client device;

transmit the public key and the PAN to a transaction processing system for storage of the public key in association with a device identifier, wherein the

transaction processing system is configured in the electronic payment processing network as separate from the payment gateway;

receive, via a merchant interface of a merchant operated on the client device, a transaction request for a transaction between the account of the consumer and an account of the merchant, the transaction request comprising the PAN;

determine whether the PAN has been registered with the public key for use in a client device authentication process;

in response to determining that the PAN has been registered with the public key of the public-private key pair of the client device of the consumer, cause the transaction processing system to cryptographically authenticate the client device based on the public key by transmitting a login request to the transaction processing system comprising the device identifier of the client device based on the PAN;

receive a login response from the transaction processing system associated with successful cryptographic authentication of the client device based on the public key of the public-private key pair of the client device; and

in response to receiving the login response associated with the successful cryptographic authentication of the client device, process the transaction by generating a transaction authorization request message comprising the PAN to the transaction processing system.

12. The computer program product of claim 11, wherein the one or more instructions further cause the at least one processor to:

transmit a consumer authentication request message to an issuer system associated with an issuer of the account of the consumer, wherein the consumer authentication request message comprises data of the client device authentication process, and wherein the issuer system is configured in the electronic payment processing network as separate from the payment gateway and the transaction processing system; and

receive a consumer authentication response message from the issuer system indicating successful authentication of the consumer, wherein the transaction is processed further in response to receipt of the consumer authentication response message.

13. The computer program product of claim 11, wherein the login response comprises data indicating that the public key of the public-private key pair of the client device was successfully matched with the private key of the public-private key pair stored on the client device, through execution of the client device authentication process.

14. The computer program product of claim 11, wherein the one or more instructions further cause the at least one processor to receive an initial request from a merchant system for the payment gateway to process the transaction, wherein the initial request comprises the PAN.