

CLAIMS

1. A method, comprising:

receiving, by an authentication application executing on a processor from a merchant application executing on a client device: (i) a merchant identifier of a merchant associated with the merchant application, (ii) a transaction identifier of a transaction, (iii) encrypted data, and (iv) a software fingerprint of the client device, wherein the encrypted data is generated by a contactless card and read by the client device;

verifying, by the authentication application, the encrypted data by decrypting the encrypted data;

determining, by the authentication application, that the software fingerprint matches a stored software fingerprint of the client device;

instructing, by the authentication application based on the verification of the encrypted data and the determination that the software fingerprint matches the stored software fingerprint, a virtual account number generator to generate a virtual account number for the transaction;

generating, by the virtual account number generator the virtual account number, an expiration date associated with the virtual account number, and a card verification value (CVV) associated with the virtual account number based on the instruction; and

transmitting, by the virtual account number generator, the merchant identifier, the transaction identifier, the virtual account number, the expiration date, and the CVV to a merchant server associated with the merchant to process the transaction using the transaction identifier, the virtual account number, the expiration date, and the CVV.

2. The method of claim 1, further comprising:

receiving, by the authentication application, a location of the client device; and

determining, by the authentication application, that the location of the client device is within a threshold distance of a known location associated with the contactless card, wherein the authentication application further instructs the virtual account number generator to generate the virtual account number based on the determination that the client device is within the threshold distance of the known location.

3. The method of claim 1, further comprising:
determining, by the authentication application, that the contactless card has been used to make a previous purchase with the merchant, wherein the authentication application further instructs the virtual account number generator to generate the virtual account number based on the determination that the contactless card has previously been used to make a purchase with the merchant.
4. The method of claim 1, further comprising:
receiving, by the virtual account number generator from an account database, an account holder name of an account associated with the contactless card and an address associated with the account; and
transmitting, by the virtual account number generator, the account holder name and address to the merchant server.
5. The method of claim 1, further comprising:
receiving, by the authentication application, authentication information for a user account associated with the contactless card, the authentication information comprising one or more of: (i) a username and a password, (ii) one or more biometric credentials; and
verifying, by the authentication application, the authentication information for the user account.
6. The method of claim 1, further comprising:
determining, by the authentication application, a device identifier received from the client device is associated with a user account associated with the contactless card.
7. The method of claim 1, wherein the virtual account number is different than an account number associated with the contactless card.
8. A computer-readable storage medium including instructions that when executed by a processor, cause the processor to:
receive, by an authentication application executing on the processor and from a merchant application executing on a client device: (i) a merchant identifier of a merchant associated with the merchant application, (ii) a transaction identifier of a transaction, (iii)

encrypted data, and (iv) a software fingerprint of the client device, wherein the encrypted data is generated by a contactless card and read by the client device;

verify, by the authentication application, the encrypted data by decrypting the encrypted data;

determine, by the authentication application, that the software fingerprint matches a stored software fingerprint of the client device;

instruct, by the authentication application based on the verification of the encrypted data and the determination that the software fingerprint matches the stored software fingerprint, a virtual account number generator to generate a virtual account number for the transaction;

generate, by the virtual account number generator the virtual account number, an expiration date associated with the virtual account number, and a card verification value (CVV) associated with the virtual account number based on the instruction; and

transmit, by the virtual account number generator, the merchant identifier, the transaction identifier, the virtual account number, the expiration date, and the CVV to a merchant server associated with the merchant to process the transaction using the transaction identifier, the virtual account number, the expiration date, and the CVV.

9. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

receive, by the authentication application, a location of the client device; and

determine, by the authentication application, that the location of the client device is within a threshold distance of a known location associated with the contactless card, wherein the authentication application further instructs the virtual account number generator to generate the virtual account number based on the determination that the client device is within the threshold distance of the known location.

10. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

determine, by the authentication application, that the contactless card has been used to make a previous purchase with the merchant, wherein the authentication application further instructs the virtual account number generator to generate the virtual account number

based on the determination that the contactless card has previously been used to make a purchase with the merchant.

11. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

receive, by the virtual account number generator from an account database, an account holder name of an account associated with the contactless card and an address associated with the account; and

transmit, by the virtual account number generator, the account holder name and address to the merchant server.

12. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

receive, by the authentication application, authentication information for a user account associated with the contactless card, the authentication information comprising one or more of: (i) a username and a password, (ii) one or more biometric credentials; and

verify, by the authentication application, the authentication information for the user account.

13. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

determine, by the authentication application, a device identifier received from the client device is associated with a user account associated with the contactless card.

14. The computer-readable storage medium of claim 8, wherein the virtual account number is different than an account number associated with the contactless card.

15. A computing apparatus comprising:

a processor; and

a memory storing instructions that, when executed by the processor, cause the processor to:

receive, by an authentication application executing on the processor and from a merchant application executing on a client device: (i) a merchant identifier of a

merchant associated with the merchant application, (ii) a transaction identifier of a transaction, (iii) encrypted data, and (iv) a software fingerprint of the client device, wherein the encrypted data is generated by a contactless card and read by the client device;

verify, by the authentication application, the encrypted data by decrypting the encrypted data;

determine, by the authentication application, that the software fingerprint matches a stored software fingerprint of the client device;

instruct, by the authentication application based on the verification of the encrypted data and the determination that the software fingerprint matches the stored software fingerprint, a virtual account number generator to generate a virtual account number for the transaction;

generate, by the virtual account number generator the virtual account number, an expiration date associated with the virtual account number, and a card verification value (CVV) associated with the virtual account number based on the instruction; and

transmit, by the virtual account number generator, the merchant identifier, the transaction identifier, the virtual account number, the expiration date, and the CVV to a merchant server associated with the merchant to process the transaction using the transaction identifier, the virtual account number, the expiration date, and the CVV.

16. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

receive, by the authentication application, a location of the client device; and

determine, by the authentication application, that the location of the client device is within a threshold distance of a known location associated with the contactless card, wherein the authentication application further instructs the virtual account number generator to generate the virtual account number based on the determination that the client device is within the threshold distance of the known location.

17. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

determine, by the authentication application, that the contactless card has been used to make a previous purchase with the merchant, wherein the authentication application further instructs the virtual account number generator to generate the virtual account number based on the determination that the contactless card has previously been used to make a purchase with the merchant.

18. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

receive, by the virtual account number generator from an account database, an account holder name of an account associated with the contactless card and an address associated with the account; and

transmit, by the virtual account number generator, the account holder name and address to the merchant server.

19. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

receive, by the authentication application, authentication information for a user account associated with the contactless card, the authentication information comprising one or more of: (i) a username and a password, (ii) one or more biometric credentials; and

verify, by the authentication application, the authentication information for the user account.

20. The method of claim 1, further comprising prior to instructing the virtual account number generator to generate the virtual account number for the transaction:

determining, by the authentication application, to process the transaction without receiving user input specifying payment information associated with the contactless card via the merchant application based on: the verification of the encrypted data, and the determination that the software fingerprint matches the stored software fingerprint,

wherein the authentication application instructs the virtual account number generator to generate the virtual account number for the transaction further based on the determination

to process the transaction without receiving the user input specifying the payment information associated with the contactless card.