

## **ONE-TAP PAYMENT USING A CONTACTLESS CARD**

### **TECHNICAL FIELD**

**[0001]** Embodiments herein generally relate to computing platforms, and more specifically, to tapping a contactless card to a computing device to perform one-tap payment.

### **RELATED APPLICATIONS**

**[0002]** This application claims priority to U.S. Patent Application Serial No. 16/265,974, titled “ONE-TAP PAYMENT USING A CONTACTLESS CARD” filed on February 1, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

### **BACKGROUND**

**[0003]** Users often complete transactions using online software platforms. Conventionally, users must manually enter all relevant payment information in the online software platform to complete a transaction. However, users often make mistakes when entering their payment information. Furthermore, transmitting payment information via a user device may pose security risks.

### **SUMMARY**

**[0003a]** According to an aspect, there is provided 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, and (iii) encrypted data, the encrypted data generated by a contactless card; verifying, by the authentication application, the encrypted data by decrypting the encrypted data; generating, by a virtual account number generator executing on the processor, a virtual account number based on the verification of the encrypted data; and transmitting, by the virtual account number generator, the merchant identifier, the transaction identifier, 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 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.

**[0003b]** According to another aspect, there is provided 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 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, and (iii) encrypted data, the encrypted data generated by a contactless card; verify, by the authentication application, the encrypted data by decrypting the encrypted data; generate, by a virtual account number generator executing on the processor, a virtual account number based on the verification of the encrypted data; and transmit, by the virtual account number generator, the merchant identifier, the transaction identifier, 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 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.

**[0003c]** According to another aspect, there is provided 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 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, and (iii) encrypted data, the encrypted data generated by a contactless card; verify, by the authentication application, the encrypted data by decrypting the encrypted data; generate, by a virtual account number generator executing on the processor, a virtual account number based on the verification of the encrypted data; and transmit, by the virtual account number generator, the merchant identifier, the transaction identifier, 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 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.

**[0004]** Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for tapping a contactless card to a computing device for one-tap payment. In one example, an authentication application may receive, from a merchant application of a client device, a merchant identifier, a transaction identifier

## 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, and (iii) encrypted data, the encrypted data generated by a contactless card;

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

generating, by a virtual account number generator executing on the processor, a virtual account number based on the verification of the encrypted data; and

transmitting, by the virtual account number generator, the merchant identifier, the transaction identifier, 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 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 virtual account number generator further generates 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 virtual account number generator further generates 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 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, and (iii) encrypted data, the encrypted data generated by a contactless card;

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

generate, by a virtual account number generator executing on the processor, a virtual account number based on the verification of the encrypted data; and

transmit, by the virtual account number generator, the merchant identifier, the transaction identifier, 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 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 virtual account number generator further generates 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 virtual account number generator further generates 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 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, and (iii) encrypted data, the encrypted data generated by a contactless card;

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

generate, by a virtual account number generator executing on the processor, a virtual account number based on the verification of the encrypted data; and

transmit, by the virtual account number generator, the merchant identifier, the transaction identifier, 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 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 virtual account number generator further generates 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 virtual account number generator further generates 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 computing apparatus of claim 15, 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.