TAP CARD TO SECURELY GENERATE CARD DATA TO COPY TO CLIPBOARD

TECHNICAL FIELD

[0001] Embodiments herein generally relate to computing platforms, and more specifically, to tapping a card to a computing device to securely generate card data which can be copied to a clipboard of the computing device.

RELATED APPLICATIONS

[0002] This application claims priority to U.S. Patent Application Serial No. 16/265,937, titled "TAP CARD TO SECURELY GENERATE CARD DATA TO COPY TO CLIPBOARD" filed on February 1, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

BACKGROUND

[0003] Account identifiers for payment cards are often long numeric and/or character strings. As such, it is difficult for a user to manually enter the account identifier correctly. Indeed, users often make mistakes and enter incorrect account identifiers into computing interfaces (e.g., payment interfaces). Furthermore, processes have been developed that allow cameras to capture and identify account identifiers entered in a device, thereby posing security risks to account identifiers. Further still, certain operating systems restrict the ability to access identifiers stored on a contactless card, which blocks conventional attempts to programmatically copy and/or paste the account identifier.

SUMMARY

[0003a] According to an aspect, there is provided a method comprising: receiving, by a processor of a computing device from a contactless card, a uniform resource locator (URL), the URL comprising a cryptogram; opening, by an operating system (OS) executing on the processor, an application based on the URL; transmitting, by the application, the cryptogram to an authentication server; receiving, by the application, a virtual account number from a virtual account number server;

copying, by the application, the virtual account number to a clipboard of the OS; and pasting, by the OS, the virtual account number from the clipboard to a payment field of a form.

[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, from a contactless card, a uniform resource locator (URL), the URL comprising a cryptogram; open, by an operating system (OS), an application based on the URL; transmit, by the application, the cryptogram to an authentication server; receive, by the application, a virtual account number from a virtual account number server; copy, by the application, the virtual account number to a clipboard of the OS; and paste, by the OS, the virtual account number from the clipboard to a payment field of a form.

[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, from a contactless card, a uniform resource locator (URL), the URL comprising a cryptogram; open, by an operating system (OS), an application based on the URL; transmit, by the application, the cryptogram to an authentication server; receive, by the application, a virtual account number from a virtual account number server; copy, by the application, the virtual account number to a clipboard of the OS; and paste, by the OS, the virtual account number from the clipboard to a payment field of a form.

[0004] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for tapping a contactless card to securely

CLAIMS

1. A method, comprising:

receiving, by a processor of a computing device from a contactless card, a uniform resource locator (URL), the URL comprising a cryptogram;

opening, by an operating system (OS) executing on the processor, an application based on the URL;

transmitting, by the application, the cryptogram to an authentication server;

receiving, by the application, a virtual account number from a virtual account number server;

copying, by the application, the virtual account number to a clipboard of the OS; and

pasting, by the OS, the virtual account number from the clipboard to a payment field of a form.

2. The method of claim 1, further comprising, prior to receiving the URL:

determining, by the application, that the payment field of the form has received focus.

3. The method of claim 1, wherein the URL comprises a universal link URL directed to a page of the application.

4. The method of claim 1, further comprising:

receiving, by the application, an expiration date of the virtual account number, a card verification value (CVV) of the virtual account number, and a billing address from the virtual account number server; and

copying, by the application, one of the expiration date, the CVV, and the billing address to the clipboard; and

pasting, by the OS, the one of the expiration date, the CVV, and the billing address from the clipboard to another field of the form.

5. The method of claim 1, wherein the virtual account number includes a restriction, the restriction comprising one or more of a merchant restriction, a time restriction, a location restriction, or an amount restriction.

6. The method of claim 1, further comprising:

authenticating, by the application, an account associated with the contactless card.

7. The method of claim 1, further comprising:

receiving, via one of a push notification or the application, input specifying to copy the virtual account number to the clipboard.

8. A computer-readable storage medium including instructions that when executed by a processor, cause the processor to:

receive, from a contactless card, a uniform resource locator (URL), the URL comprising a cryptogram;

open, by an operating system (OS), an application based on the URL;

transmit, by the application, the cryptogram to an authentication server;

receive, by the application, a virtual account number from a virtual account number server;

copy, by the application, the virtual account number to a clipboard of the OS; and

paste, by the OS, the virtual account number from the clipboard to a payment field of a form.

9. The computer-readable storage medium of claim 8, wherein the instructions further configure the computer to, prior to receiving the URL:

determine, by the application, that the payment field of the form has received focus.

10. The computer-readable storage medium of claim 8, wherein the URL comprises a universal link URL directed to a page of the application.

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

receive an expiration date of the virtual account number, a card verification value (CVV) of the virtual account number, and a billing address from the virtual account number server; and

copy, by the application, one of the expiration date, the CVV, and the billing address to the clipboard; and

paste, by the OS, the one of the expiration date, the CVV, and the billing address from the clipboard to another field of the form.

12. The computer-readable storage medium of claim 8, wherein the virtual account number includes a restriction, the restriction comprising one or more of a merchant restriction, a time restriction, a location restriction, or an amount restriction.

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

authenticate, by the application, an account associated with the contactless card.

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

receive, via one of a push notification or the application, input specifying to copy the virtual account number to the clipboard.

15. A computing apparatus comprising:

a processor; and

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

receive, from a contactless card, a uniform resource locator (URL), the URL comprising a cryptogram;

open, by an operating system (OS), an application based on the URL;

transmit, by the application, the cryptogram to an authentication server;

receive, by the application, a virtual account number from a virtual account number server;

copy, by the application, the virtual account number to a clipboard of the OS; and

paste, by the OS, the virtual account number from the clipboard to a payment field of a form.

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

determine, by the application, that the payment field of the form has received focus.

17. The computing apparatus of claim 15, wherein the URL comprises a universal link URL directed to a page of the application.

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

receive, by the application, an expiration date of the virtual account number, a card verification value (CVV) of the virtual account number, and a billing address from the virtual account number server; and

copy, by the application, one of the expiration date, the CVV, and the billing address to the clipboard; and

paste, by the OS, the one of the expiration date, the CVV, and the billing address from the clipboard to another field of the form.

19. The computing apparatus of claim 15, wherein the virtual account number includes a restriction, the restriction comprising one or more of a merchant restriction, a time restriction, a location restriction, or an amount restriction.

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

authenticate, by the application, an account associated with the contactless card.