CLAIMS

1. A system,

comprising: a

processor; and

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

detect, by an application executing on the processor, a plurality of taps of a contactless card to a device comprising the processor, the contactless card associated with an account, wherein each of the plurality of taps brings the card within wireless communications range of the device for a transaction, wherein each respective tap causes a different data set to be wirelessly transmitted to the application for the transaction;

increment, by the application, a tap counter responsive to each tap of the contactless card to the device, wherein the tap counter counts each respective tap for the transaction;

receive, by an application executing on the processor, an account number associated with the account, an expiration date of the account number, and a card verification value (CVV) associated with the account number;

send, by the application to a server, encrypted data to verify;

receive, by the application from the server, verification of the encrypted data;

copy, by the application responsive to a first tap of the plurality of taps and verification of the encrypted data, one of the account number, the expiration date, and the CVV to a clipboard of an operating system (OS) executing on the processor;

determine, by the application, that a time threshold has expired or the transaction has been completed using the one of the account number, the expiration date, and the CVV copied to the clipboard; and

remove, by the application, the one of the account number, the expiration date, and the CVV from the clipboard based on the time threshold expiring or the transaction being completed.

2. The system of claim 1, the memory storing instructions which when executed by the processor cause the processor to:

receive encrypted data by the application from the contactless card responsive to a second tap of the plurality of taps, wherein the second tap is prior to the first tap;

transmit, by the application, the encrypted data to a server; and

receive, by the application from the server, an indication specifying the server decrypted the encrypted data.

3. The system of claim 2, wherein the account number, the expiration date, and the CVV are received from the server or the contactless card based on the server decrypting the encrypted data, wherein the value of the tap counter counts a number of taps of the card to the device.

4. The system of claim 3, wherein the account number, the expiration date, and the CVV are received from the contactless card based on the number of taps counted by the tap counter.

5. The system of claim 1, the memory storing instructions which when executed by the processor cause the processor to:

determine, by the application, that the value of the tap counter subsequent incrementing the tap counter responsive to the first tap of the plurality of taps is associated with copying the account number to the clipboard;

copy, by the application, the account number to the clipboard; and

paste, by the OS, the account number to an account number form field.

6. The system of claim 1, wherein the account number is encrypted, the memory storing instructions which when executed by the processor cause the processor to:

decrypt the encrypted account number.

7. The system of claim 1, the memory storing instructions which when executed by the processor cause the processor to:

determine, by the device, that a time threshold has expired or the transaction has been completed using the one of the account number, the expiration date, and the CVV to copied to clipboard; and

remove, by the device, the one of the account number, the expiration date, and the CVV from the clipboard based on the time threshold expiring or the transaction being completed.

8. A non-transitory computer-readable storage medium having computer-readable program code for an application embodied therewith, the computer-readable program code executable by a processor to cause the processor to:

detect a plurality of taps of a contactless card to a device comprising the processor, the contactless card associated with an account, wherein each of the plurality of taps brings the card within wireless communications range of the device for a transaction, wherein each respective tap causes a different data set to be wirelessly transmitted to the application for the transaction;

increment a tap counter responsive to each tap of the contactless card to the device, wherein the tap counter counts each respective tap for the transaction;

receive, by the application, an account number associated with the account, an expiration date of the account number, and a card verification value (CVV) associated with the account number;

send encrypted data to a server to verify the encrypted data;

receive verification of the encrypted data;

copy, by the application responsive to a first tap of the plurality of taps and verification of the encrypted data, one of the account number, the expiration date, and the CVV to a clipboard of an operating system (OS) executing on the processor;

determine that a time threshold has expired or the transaction has been completed using the one of the account number, the expiration date, and the CVV copied to the clipboard; and

remove the one of the account number, the expiration date, and the CVV from the clipboard based on the time threshold expiring or the transaction being completed.

9. The non-transitory computer-readable storage medium of claim 8, further comprising computer-readable program code executable by the processor to cause the processor to:

receive encrypted data by the application from the contactless card responsive to a second tap of the plurality of taps, wherein the second tap is prior to the first tap;

transmit, by the application, the encrypted data to a server; and

receive, by the application from the server, an indication specifying the server decrypted the encrypted data.

10. The non-transitory computer-readable storage medium of claim 9, wherein the account number, the expiration date, and the CVV are received from the server or the contactless card based on the server decrypting the encrypted data, wherein the value of the tap counter counts a number of taps of the card to the device.

11. The non-transitory computer-readable storage medium of claim 10, wherein the account number, the expiration date, and the CVV are received from the contactless card based on the number of taps counted by the tap counter.

12. The non-transitory computer-readable storage medium of claim 9, further comprising computer-readable program code executable by the processor to cause the processor to:

determine, by the application, that the value of the tap counter subsequent incrementing the tap counter responsive to the first tap of the plurality of taps is associated with copying the account number to the clipboard;

copy, by the application, the account number to the clipboard; and

paste, by the OS, the account number to an account number form field.

13. The non-transitory computer-readable storage medium of claim 9, further comprising computer-readable program code executable by the processor to cause the processor to:

determine, by the device, that a time threshold has expired or the transaction has been completed using the one of the account number, the expiration date, and the CVV to copied to clipboard; and

remove, by the device, the one of the account number, the expiration date, and the CVV from the clipboard based on the time threshold expiring or the transaction being completed.

14. A method, comprising:

detecting, by an application executing on a device, a plurality of taps of a contactless card to the device, the contactless card associated with an account, wherein each of the

plurality of taps brings the card within wireless communications range of the device for a transaction, wherein each respective tap causes a different data set to be wirelessly transmitted to the application for the transaction;

incrementing, by the application, a tap counter responsive to each tap of the contactless card to the device, wherein the tap counter counts each respective tap for the transaction;

receiving, by the application, an account number associated with the account, an expiration date of the account number, and a card verification value (CVV) associated with the account number;

sending, by the application, encrypted data to a server;

receiving, by the application from the server, verification of the encrypted data;

copying, by the application responsive to a first tap of the plurality of taps and verification of the encrypted data, one of the account number, the expiration date, and the CVV to a clipboard of an operating system (OS) executing on the device based on a value of the tap counter subsequent to incrementing the tap counter responsive to the first tap of the plurality of taps;

determining, by the application, that a time threshold has expired or the transaction has been completed using the one of the account number, the expiration date, and the CVV copied to the clipboard; and

removing, by the application, the one of the account number, the expiration date, and the CVV from the clipboard based on the time threshold expiring or the transaction being completed.

15. The method of claim 14, further comprising:

receiving encrypted data by the application from the contactless card responsive to a second tap of the plurality of taps, wherein the second tap is prior to the first tap;

transmitting, by the application, the encrypted data to a server; and

receiving, by the application from the server, an indication specifying the server decrypted the encrypted data.

16. The method of claim 15, wherein the account number, the expiration date, and the CVV are received from the server or the contactless card based on the server decrypting the encrypted data, wherein the value of the tap counter counts a number of taps of the card to the device.

17. The method of claim 16, wherein the account number, the expiration date, and the CVV are received from the contactless card based on the number of taps counted by the tap counter.

18. The method of claim 14, further comprising:

determining, by the application, that the value of the tap counter subsequent incrementing the tap counter responsive to the first tap of the plurality of taps is associated with copying the account number to the clipboard;

copying, by the application, the account number to the clipboard; and

pasting, by the OS, the account number to an account number form field.

19. The method of claim 14, wherein the account number is encrypted, the method further comprising decrypting the encrypted account number.

20. The method of claim 14, further comprising:

determining, by the device, that a time threshold has expired or the transaction has been completed using the one of the account number, the expiration date, and the CVV to copied to clipboard; and

removing, by the device, the one of the account number, the expiration date, and the CVV from the clipboard based on the time threshold expiring or the transaction being completed.