CLAIMS

1. A computer-implemented method, comprising:

receiving, by a web browser executing on a processor of a device, selection of a link in a merchant web page, the merchant web page associated with a transaction;

downloading, by an operating system (OS) executing on the processor, an application from an application server based on the link;

identifying, by the application, a plurality of financial institution applications installed on the device;

selecting, by the application, a first financial institution corresponding to a first financial institution application of the plurality of financial institution applications installed on the device;

receiving, by the application, a cryptogram from a contactless card associated with the first financial institution;

transmitting, by the application, the cryptogram to an authentication server of the first financial institution;

receiving, by the application, an authentication result specifying the authentication server decrypted the cryptogram;

receiving, by the web browser based on the decryption of the cryptogram by the authentication server, an account number, an expiration date associated with the account number, and a card verification value (CVV) associated with the account number; and

providing, by the web browser, the account number, the expiration date, and the CVV to a server associated with the application to process the transaction.

2. The method of claim 1, the method further comprising:

receiving, by the web browser, a confirmation for the processed transaction; and

displaying, by the web browser, the confirmation.

3. The method of claim 1, further comprising:

storing, by the web browser, a cookie on the device based on an indication received from the server associated with the application, the indication specifying payment for the transaction has been processed using the account number, the expiration date, and the CVV.

4. The method of claim 3, further comprising subsequent to providing the account number, the expiration date, and the CVV to the server associated with the application:

receiving, by the web browser, a second selection of the link in the merchant web page, the second selection of the link to process a second transaction using the application;

downloading, by the OS, the application from the application server based on the link;

identifying, by the application, the cookie on the device;

selecting, by the application based on the cookie, the contactless card associated with the first financial institution;

receiving, by the application from the authentication server, the account number, the expiration date, and the CVV; and

providing, by the application, the account number, the expiration date, and the CVV to the server associated with the application to process the second transaction.

5. The method of claim 1, further comprising prior to providing the account number, the expiration date, and the CVV to the server associated with the application:

receiving, by the device at a phone number of the device, a one-time passcode from the authentication server;

receiving, by the application, an input value;

comparing, by the application, the input value to the one-time passcode; and

determining, by the application based on the comparison, that the input value matches the one-time passcode, wherein the application transmits the cryptogram to the authentication server based at least in part on the determination that the input value matches the one-time passcode.

6. The method of claim 5, further comprising prior to receiving the one-time passcode:

receiving, by the application, input comprising an email address; and

transmitting, by the application, the email address to the authentication server, wherein the authentication server determines the phone number of the device based on the email address.

7. The method of claim 1, wherein the link comprises a first identifier of a first merchant associated with the merchant web page and a transaction identifier associated with the transaction, wherein the first merchant is one of a plurality of merchants, wherein the merchant web page is one of a plurality of merchant web pages on a web server.

8. The method of claim 7, wherein the web server hosts the plurality of merchant web pages, wherein each merchant web page is associated with a respective one of the plurality of merchants, wherein each merchant is associated with a respective identifier of a plurality of

identifiers, the plurality of identifiers including the first identifier, wherein the server associated with the application comprises one of a payment processing server or the web server.

9. The method of claim 1, wherein the application is a non-persistent on-demand application.

10. The method of claim 1, wherein the link is a deep link uniform resource locator (URL) or a universal link URL.

11. The method of claim 1, wherein a page identifier parameter of the link identifies a page of the application, the method further comprising:

identifying, by the application, the page identifier parameter; and

opening, by the application, the page of the application based on the page identifier parameter.

12. The method of claim 1, further comprising:

receiving, by the web browser, a selection of a second link in a second merchant web page, the selection of the second link to process a second transaction;

downloading, by the OS, a second application from the application server based on the second link;

selecting, by the second application, a second financial institution corresponding to a second financial institution application of the plurality of financial institution applications installed on the device;

receiving, by the second application, a second cryptogram from a second contactless card associated with the second financial institution;

receiving, by the second application, an authentication result specifying a second authentication server associated with the second financial institution decrypted the second cryptogram;

receiving, by the web browser from the second authentication server and based on decryption of the second cryptogram by the second authentication server, a virtual account number, an expiration date for the virtual account number, and a CVV for the virtual account number; and

providing, by the web browser, the virtual account number, the expiration date for the virtual account number, and CVV for the virtual account number to a web server hosting the second merchant web page to process the second transaction.

13. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor of a device, cause the processor to:

receive, by a web browser, selection of a link in a merchant web page, the merchant web page associated with a transaction;

download, by an operating system (OS), an application from an application server based on the link;

identify, by the application, a plurality of financial institution applications installed on the device;

select, by the application, a first financial institution corresponding to a first financial institution application of the plurality of financial institution applications installed on the device;

receive, by the application, a cryptogram from a contactless card associated with the first financial institution;

transmit, by the application, the cryptogram to an authentication server of the first financial institution;

receive, by the application, an authentication result specifying the authentication server decrypted the cryptogram;

receive, by the web browser based on the decryption of the cryptogram by the authentication server, an account number, an expiration date associated with the account number, and a card verification value (CVV) associated with the account number; and

provide, by the web browser, the account number, the expiration date, and the CVV to a server associated with the application to process the transaction.

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

receive, by the web browser, a confirmation for the processed transaction; and

display, by the web browser, the confirmation.

15. The computer-readable storage medium of claim 13 or 14, wherein the instructions further cause the processor to:

store, by the web browser, a cookie on the device based on an indication received from the server associated with the application, the indication specifying payment for the transaction has been processed using the account number, the expiration date, and the CVV.

16. The computer-readable storage medium of claim 15, wherein the instructions further cause the processor to, subsequent to providing the account number, the expiration date, and the CVV to the server associated with the application:

receive, by the web browser, a second selection of the link in the merchant web page, the second selection of the link to process a second transaction using the application;

download, by the OS, the application from the application server based on the link;

identify, by the application, the cookie on the device;

select, by the application based on the cookie, the contactless card associated with the first financial institution;

receive, by the application from the authentication server, the account number, the expiration date, and the CVV; and

provide, by the application, the account number, the expiration date, and the CVV to the server associated with the application to process the second transaction.

17. The computer-readable storage medium of claim 13 or 14, wherein the instructions further cause the processor to, prior to providing the account number, the expiration date, and the CVV to the server associated with the application:

receive, by the device at a phone number of the device, a one-time passcode from the authentication server;

receive, by the application, an input value;

compare, by the application, the input value to the one-time passcode; and

determine, by the application based on the comparison, that the input value matches the one-time passcode, wherein the application transmits the cryptogram to the authentication server based at least in part on the determination that the input value matches the one-time passcode.

18. A computing apparatus comprising:

a processor; and

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

receive, by a web browser, selection of a link in a merchant web page, the merchant web page associated with a transaction;

download, by an operating system (OS), an application from an application server based on the link;

identify, by the application, a plurality of financial institution applications installed on the apparatus;

select, by the application, a first financial institution corresponding to a first financial institution application of the plurality of financial institution applications installed on the apparatus;

receive, by the application, a cryptogram from a contactless card associated with the first financial institution;

transmit, by the application, the cryptogram to an authentication server of the first financial institution;

receive, by the application, an authentication result specifying the authentication server decrypted the cryptogram;

receive, by the web browser based on the decryption of the cryptogram by the authentication server, an account number, an expiration date associated with the account number, and a card verification value (CVV) associated with the account number; and

provide, by the web browser, the account number, the expiration date, and the CVV to a server associated with the application to process the transaction.

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

receive, by the web browser, a confirmation for the processed transaction; and

display, by the web browser, the confirmation.

20. The computing apparatus of claim 18 or 19, wherein the instructions further cause the processor to:

store, by the web browser, a cookie in the memory based on an indication received from the server associated with the application, the indication specifying payment for the transaction has been processed using the account number, the expiration date, and the CVV.