WE CLAIM:

1. An authenticated data transfer system comprising:

a contactless card comprising a processor and a memory,

wherein, after entering a communication field, the processor is configured to:

dynamically generate a uniform resource locator (URL), wherein the URL comprises:

a first set of information including abstracted identifier information, and

a second set of information including user information; and

and transmit the URL to initiate data transfer; and

wherein the data transfer is completed upon verification of a received response and confirmation of a third set of information associated with the data transfer.

2. The authenticated data transfer system of claim 1, wherein one or more actions, based on the link, are configured to identify a user.

3. The authenticated data transfer system of claim 2, wherein at least one action from the one or more actions comprises launching a website configured to identify the user associated with a first device.

4. The authenticated data transfer system of claim 3, wherein the user associated with the first device is identified by at least one selected from the group of device fingerprinting and a cookie.

5. The authenticated data transfer system of claim 4, wherein login information is requested upon determination of an unsuccessful identification.

6. The authenticated data transfer system of claim 4, wherein the website is configured to display the second set of information and the third set of information.

~~7. The authenticated data transfer system of claim 6, wherein a notification comprises the one or more responses associated with confirmation of the third set of information.~~

~~8. The authenticated data transfer system of claim 7, wherein one or more authentication communications associated with confirmation of the third set of information are performed, the one or more authentication communications including at least one selected from the group of biometric communication and login communication.~~

~~9. The authenticated data transfer system of claim 1, wherein the first set of information comprises an abstracted user name generated by the processor after entry of the contactless card into the communication field.~~

~~10. The authenticated data transfer system of claim 1, wherein the link comprises a near field communication data exchange format uniform resource locator.~~

~~11. The authenticated data transfer system of claim 3, wherein the first device comprises at least one selected from the group of a mobile device, a wearable device, and a kiosk.~~

~~12. The authenticated data transfer system of claim 2, wherein at least one action from the one or more actions comprises requesting one or more login credentials.~~

~~13. The authenticated data transfer system of claim 12, wherein a deep link to a screen including the second set of information and the third set of information is performed upon submission of the requested one or more login credentials and upon authentication of the one or more login credentials.~~

~~14. The authenticated data transfer system of claim 1, wherein the third set of information includes at least one selected from the group of a quantity, digital asset, and recipient information.~~

15. The authenticated data transfer system of claim 14, wherein a notification comprises the one or more responses associated with confirmation of the third set of information.

16. The authenticated data transfer system of claim 15, wherein one or more authentication communications associated with confirmation of the third set of information are performed, the one or more authentication communications including at least one selected from the group of biometric communication and login communication.

17. The authenticated data transfer system of claim 1, wherein the data transfer is scheduled at a predetermined time.

18. A method of authenticating data transfer, comprising:

dynamically generating, after entry of one or more processors of a transmitting device into a communication field, the link comprising a near field communication data exchange format uniform resource locator including identifier data and user data;

transmitting, to a first application comprising instructions for execution on a first device, the link to initiate data transfer;

authenticating a user associated with the first device by activating one or more actions based on the link;

transmitting one or more requests for confirmation of quantity and recipient data associated with the data transfer;

receiving one or more notifications that are based on the one or more requests for confirmation of quantity and recipient data associated with the data transfer; and

performing one or more login credentials that are responsive to the one or more notifications so as to complete the data transfer.

~~19. The method of claim 18, wherein at least one action from the one or more actions comprises launching a website configured to identify the user associated with the first device.~~

~~20. A computer readable non-transitory medium comprising computer-executable instructions that, when executed by a processor, perform procedures comprising the steps of:~~

~~dynamically generating , after entry of a contactless card into a communication field, a link, the link comprising a first set of information and a second set of information, the first set of information including identifier information, the second set of information including user information;~~

~~transmitting, to a first application comprising instructions for execution on a first device, the link to initiate data transfer;~~

~~identifying a user associated with the first device by activating one or more actions based on the link, the one or more actions configured to request confirmation of a third set of information associated with the data transfer; and~~

~~transmitting one or more responses based on authentication of the third set of information so as to complete the data transfer.~~

1. A secure peer-to-peer data transfer system, comprising:

a contactless card associated with a cardholder, comprising a processor and a memory, wherein the processor is configured to:

generate a link after the contactless card enters a communication field associated with a communication device of a recipient user distinct from the cardholder, the link being operative to initiate a secure peer-to-peer data transfer involving the recipient user and the cardholder, wherein the link comprises:

a first set of information comprising one or more abstracted identification information uniquely identifying the contactless card and a specific peer-to peer data transfer session,

a second set of information including information associated with the cardholder loaded on to the contactless card at the time of personalization of the card, and

one or more data fields for specifying one or more transfer parameters.

2. The secure peer-to-peer data transfer system of claim 1, wherein the one or more transfer parameters comprise a peer-to-peer data transfer directionality.

3. The secure peer-to-peer data transfer system of claim 1, wherein:

the link comprises a near field communication data exchange format uniform resource locator (NDEF URL), and

the processor is further configured to transmit the NDEF URL via near field communication.

4. The secure peer-to-peer data transfer system of claim 1, wherein the processor is further configured to transmit the link to the communication device to initiate a data transfer associated with a third set of information.

5. The secure peer-to-peer data transfer system of claim 4, wherein:

the third set of information comprises at least one selected from the group of a quantity, a digital asset, and recipient information, and

the processor is further configured to initiate the data transfer responsive to a confirmation of the third set of information via an authenticated response from the cardholder.

6. The secure peer-to-peer data transfer system of claim 1, wherein:

the link is operative to initiate the data transfer session by launching a website on the communication device, and

the website is operative to initiate the secure peer-to-peer data transfer.

7. The secure peer-to-peer data transfer system of claim 6, wherein the third set of information is entered into the website based on one or more inputs provided by the recipient user.

8. The secure peer-to-peer data transfer system of claim 6, wherein one or more actions, based on the link, are configured to identify a user.

9. The secure peer-to-peer data transfer system of claim 8, at least one action from the one or more actions comprises launching a website configured to initiate the data transfer upon receiving one or more valid authentication inputs from the communication device associated with the recipient user and an authenticated confirmation from a computing device associated with the cardholder.

10. The secure peer-to-peer data transfer system of claim 1, wherein the recipient user associated with the communication device is identified by at least one selected from the group of device fingerprinting and a cookie.

11. A method of implementing a secure peer-to-peer data transfer, comprising:

generating, after entry of the processors of the contactless card into a communication field of a first device associated with a recipient, a link, the link including abstracted identifier information and one or more account and identity information associated with the cardholder; and

transmitting, the link to a first application running on the first device, the link being operative to initiate a secure peer-to-peer data transfer in accordance to one or more transfer parameters.

12. The method of claim 11, further comprising authenticating a user associated with the first device by activating one or more actions based on the link.

13. The method of claim 12, wherein the one or more actions comprise at least one selected from the group of requesting confirmation of a third set of information associate with the secure

peer-to-peer data transfer, launching a second website configured to identify the user associated with the first device, and requesting one or more login credentials.

14. The method of claim 11, wherein:

the link is operative to initiate the data transfer by launching a website on the first device displaying one or more identity information associated with the cardholder, and

the website comprises one or more data fields for specifying the one or more transfer parameters.

15. The method of claim 11, wherein the abstracted identifier information is generated using a unique identifier and a cryptographic algorithm.

16. The method of claim 11, wherein the abstracted identifier information is generated using a unique identifier, a counter, and a cryptographic algorithm.

17. The method of claim 11, wherein the data transfer is scheduled at a predetermined time.

18. A computer readable non-transitory medium comprising computer-executable instructions that, when executed by a processor, perform procedures comprising the steps of:

generating, after entry of the processors of the contactless card into a communication field of a first device associated with a recipient, a link, the link including abstracted identifier information and one or more account and identity information associated with the cardholder; and

transmitting, the link to a first application running on the first device, the link being operative to initiate the secure peer-to-peer data transfer in accordance to one or more transfer parameters.

19. The computer readable non-transitory medium of claim 18, wherein:

the link is operative to initiate the data transfer by launching a website on the first device displaying one or more identity information associated with the cardholder, and

the website comprises one or more data fields for specifying the one or more transfer parameters.

20. The computer readable non-transitory medium of claim 18, the procedures further comprising:

authenticating a user associated with the first device by activating one or more actions based on the link,

wherein the one or more actions comprise at least one selected from the group of requesting confirmation of a third set of information associate with the secure peer-to-peer data transfer, launching a second website configured to identify the user associated with the first device, and requesting one or more login credentials.