WE CLAIM:

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.