WHAT IS CLAIMED

1. A method of performing a transaction comprising:

receiving, by a server computer, user credentials of a user accessing a website;

identifying, by the server computer, that the website accessed by the user is a token-aware website configured to accept a token cryptogram to facilitate the transaction in data fields of a webpage of the website by identifying a unique identifier of the website and transmitting the unique identifier of the website to a processing network to verify the unique identifier of the website;

providing, by the server computer, a transaction data identifier to the website, wherein the transaction data identifier identifies underlying transaction data and is associated with the user credentials;

transmitting, by the server computer, an account token and a cryptogram request comprising the unique identifier of the website to the processing network, wherein the account token is linked to the transaction data identified by the transaction data identifier;

receiving from the processing network, a token cryptogram based on the account token; and

providing, by the server computer, the token cryptogram to at least one of the data fields of the webpage of the website to conduct the transaction.

2. The method of claim 1, further comprising:

assigning, by the server computer, the unique identifier of the website to the website, wherein the unique identifier is included in the cryptogram request; and

providing the unique identifier of the website to the data fields of the webpage, wherein the data fields are not visible to the user viewing the website.

3. The method of claim 1, wherein the data fields of the webpage of the website are hidden data fields.

4. The method of claim 1, wherein identifying that the website is token-aware includes analyzing an HTML (HyperText Markup Language) tag of the website.

5. The method of claim 4, wherein the HTML tag also verifies a trusted identity of the website.

6. The method of claim 1, wherein the server computer further provides tokenized user credentials to at least one of the data fields of the webpage of the website to conduct the transaction.

7. The method of claim 6, further comprising tokenizing at least a subset of the received user credentials to generate the tokenized user credentials.

8. The method of claim 1, wherein the tokenized user credentials are provided to the data fields of the webpage only when the website is identified as token-aware.

9. The method of claim 1, wherein the transaction data identifier is a last four digits of a Primary Account Number (PAN).

10. A computer comprising:

processing logic;

a network interface coupled to the processing logic; and

a non-transitory computer-readable medium accessible to the processing logic, the non-transitory computer-readable medium comprising code, executable by the processing logic, for implementing a method comprising:

receiving, by the computer, user credentials of a user accessing a website;

identifying, by the computer, that the website accessed by the user is a token-aware website configured to accept a token cryptogram to facilitate a transaction in data fields of a webpage of the website by identifying a unique identifier of the website and transmitting the unique identifier of the website to a processing network to verify the unique identifier of the website;

providing, by the computer, a transaction data identifier to the website, wherein the transaction data identifier identifies underlying transaction data and is associated with the user credentials;

transmitting, by the computer, an account token and a cryptogram request comprising the unique identifier of the website to the processing network, wherein the account token is linked to the transaction data identified by the transaction data identifier;

receiving from the processing network, a token cryptogram based on the account token; and

providing, by the computer, the token cryptogram to at least one of the data fields of the webpage of the website to conduct the transaction.

11. A method of performing a transaction comprising:

receiving a transaction data identifier from a server computer;

providing a transaction completion interface of a website to a computing device, the transaction completion interface making the transaction data identifier viewable to a user of the transaction completion interface, wherein the transaction data identifier identifies underlying transaction data;

providing an indication to the server computer that the website is a token-aware website configured to accept a token cryptogram to facilitate the transaction in data fields of a webpage of the website by transmitting a unique identifier of the website to the server computer;

receiving, from the server computer, a token cryptogram in the data fields of the webpage of the website; and

transmitting an authorization request to an acquirer computer, wherein the authorization request includes the token cryptogram and the unique identifier of the website.

12. The method of claim 11, further comprising:

receiving an authorization response from the acquirer computer, the authorization response either approving or declining the transaction.

13. The method of claim 12, further comprising:

sending a transaction completion message to the computing device when the authorization response approves the transaction.

14. The method of claim 11, wherein the data fields of the webpage of the website are hidden data fields.

15. The method of claim 11, wherein the token-aware indication includes an HTML (HyperText Markup Language) tag.

16. The method of claim 11, wherein tokenized user credentials are further received from the server computer and included in the authorization request.

17. The method of claim 11, wherein the token-aware indication includes an Extended Validation Certificate.

18. The method of claim 17, wherein receiving the unique identifier includes receiving the unique identifier in one of the data fields of the webpage, and wherein the data fields are not rendered for viewing by the user.

19. The method of claim 11, wherein the transaction data identifier is associated with credentials associated with a browser publisher of a browser in which the website is rendered.

20. A computer comprising:

processing logic;

a network interface coupled to the processing logic; and

a non-transitory computer-readable medium accessible to the processing logic, the non-transitory computer-readable medium comprising code, executable by the processing logic, for implementing a method comprising:

receiving a transaction data identifier, associated with a transaction, from a server computer;

providing a transaction completion interface of a website to a computing device, the transaction completion interface making the transaction data identifier viewable to a user of the transaction completion interface, wherein the transaction data identifier identifies underlying transaction data;

providing an indication to the server computer that the website is a token-aware website configured to accept a token cryptogram to facilitate the transaction in data fields of a webpage of the website by transmitting a unique identifier of the website to the server computer;

~~receiving, from the server computer a token cryptogram in the data fields of the webpage of the website; and~~

~~transmitting an authorization request to an acquirer computer, wherein the authorization request includes the token cryptogram, and the unique identifier of the website.~~

WHAT IS CLAIMED

1. A method of performing a payment transaction comprising:

receiving, by a server computer, credentials of a user accessing a merchant website;

identifying, by the server computer, that the merchant website accessed by the user is a token-aware website configured to accept a token cryptogram to facilitate the payment transaction in data fields of a webpage of the merchant website by identifying a unique identifier of the merchant website and transmitting the unique identifier of the merchant website to a processing network to verify the unique identifier of the merchant website;

providing, by the server computer, a transaction data identifier to the merchant website, wherein the transaction data identifier identifies underlying payment transaction data and is associated with the credentials;

receiving, by the server computer, a confirmation that the payment transaction data identified by the transaction data identifier is approved by the user to complete the payment transaction;

transmitting, by the server computer, a token and a cryptogram request comprising the unique identifier of the merchant website to the processing network, wherein the token is linked to the payment transaction data identified by the transaction data identifier;

receiving from the processing network, a token cryptogram based on the token; and

providing, by the server computer, tokenized credentials and the token cryptogram to the data fields of the webpage of the merchant website to conduct the payment transaction.

2. The method of claim 1, further comprising:

assigning, by the server computer, the unique identifier of the merchant website to the merchant website, wherein the unique identifier is included in the cryptogram request; and

providing the unique identifier of the merchant website to the data fields of the webpage, wherein the data fields are not visible to the user viewing the merchant website.

3. The method of claim 1, wherein the data fields of the webpage of the merchant website are hidden data fields.

4. The method of claim 1, wherein identifying that the merchant website is token-aware includes analyzing an HTML (HyperText Markup Language) tag of the merchant website.

5. The method of claim 4, wherein the HTML tag also verifies a trusted identity of the merchant website.

6. The method of claim 1, wherein the tokenized credentials are provided to the data fields of the webpage only when the merchant website is identified as token-aware.

7. The method of claim 1, wherein the payment transaction data is the tokenized credentials.

8. The method of claim 1, wherein the transaction data identifier is a last four digits of a Primary Account Number (PAN).

9. A computer comprising:

processing logic;

a network interface coupled to the processing logic; and

a non-transitory computer-readable medium accessible to the processing logic, the non-transitory computer-readable medium comprising code, executable by the processing logic, for implementing a method comprising:

receiving, by the computer, credentials of a user accessing a merchant website;

identifying, by the computer, that the merchant website accessed by the user is a token-aware website configured to accept a token cryptogram to facilitate a payment transaction in data fields of a webpage of the merchant website by identifying a unique identifier of the merchant website and transmitting the unique identifier of the merchant website to a processing network to verify the unique identifier of the merchant website;

providing, by the computer, a transaction data identifier to the merchant website, wherein the transaction data identifier identifies underlying payment transaction data and is associated with the credentials;

receiving, by the computer, a confirmation that the payment transaction data identified by the transaction data identifier is approved by the user to complete the payment transaction;

transmitting, by the computer, a token and a cryptogram request comprising the unique identifier of the merchant website to the processing network, wherein the token is linked to the payment transaction data identified by the transaction data identifier;

receiving from the processing network, a token cryptogram based on the token; and

providing, by the computer, tokenized credentials and the token cryptogram to the data fields of the webpage of the merchant website to conduct the payment transaction.

10. A method of performing a payment transaction comprising:

receiving a transaction data identifier from a server computer;

providing a transaction completion interface of a merchant website to a computing device, the transaction completion interface making the transaction data identifier viewable to a user of the transaction completion interface, wherein the transaction data identifier identifies underlying payment transaction data;

receiving a confirmation from the user that the payment transaction data identified by the transaction data identifier is approved to complete the payment transaction;

providing an indication to the server computer that the merchant website is a token-aware website configured to accept a token cryptogram to facilitate the payment transaction in data fields of a webpage of the merchant website by transmitting a unique identifier of the merchant website to the server computer;

receiving, from the server computer, tokenized credentials and a token cryptogram in the data fields of the webpage of the merchant website; and

transmitting an authorization request to an acquirer computer, wherein the authorization request includes the tokenized credentials, the token cryptogram, and the unique identifier of the merchant website.

11. The method of claim 10, further comprising:

receiving an authorization response from the acquirer computer, the authorization response either approving or declining the payment transaction.

12. The method of claim 11, further comprising:

sending a transaction completion message to the computing device when the authorization response approves the payment transaction.

13. The method of claim 10, wherein the data fields of the webpage of the merchant website are hidden data fields.

14. The method of claim 10, wherein the token-aware indication includes an HTML (HyperText Markup Language) tag.

15. The method of claim 14, wherein the token-aware indication also serves to verify the merchant website as a trusted website.

16. The method of claim 10, wherein the token-aware indication includes an Extended Validation Certificate.

17. The method of claim 10, further comprising:

receiving the unique identifier from the server computer.

18. The method of claim 17, wherein receiving the unique identifier includes receiving the unique identifier in one of the data fields of the webpage, and wherein the data fields are not rendered for viewing by the user.

19. The method of claim 10, wherein the transaction data identifier is associated with credentials associated with a browser publisher of a browser in which the merchant website is rendered.

20. A computer comprising:

processing logic;

a network interface coupled to the processing logic; and

a non-transitory computer-readable medium accessible to the processing logic, the non-transitory computer-readable medium comprising code, executable by the processing logic, for implementing a method comprising:

receiving a transaction data identifier, associated with a payment transaction, from a server computer;

providing a transaction completion interface of a merchant website to a computing device, the transaction completion interface making the transaction data identifier viewable to a user of the transaction completion interface, wherein the transaction data identifier identifies underlying payment transaction data;

receiving a confirmation from the user that the payment transaction data identified by the transaction data identifier is approved to complete the payment transaction;

providing an indication to the server computer that the merchant website is a token-aware website configured to accept a token cryptogram to facilitate the payment transaction in data fields of a webpage of the merchant website by transmitting a unique identifier of the merchant website to the server computer;

receiving, from the server computer, tokenized credentials and a token cryptogram in the data fields of the webpage of the merchant website; and

transmitting an authorization request to an acquirer computer, wherein the authorization request includes the tokenized credentials, the token cryptogram, and the unique identifier of the merchant website.