[0004] Many payment transactions enabled by online or mobile payment service providers such as, for example, retail purchases, payment transactions, and the like, are made electronically using electronic devices, such as mobile phones or mobile computing devices. For example, a consumer may install a payment application provided by the payment service provider on his or her mobile device to facilitate payments to various merchants or recipients. An online or mobile payment process utilizing the payment application typically includes user authentication that requires a user to enter a login identifier (ID) and/or a password to authenticate the user.

SUMMARY

[0004a] According to one embodiment of the present invention, a verification system, comprises a non-transitory memory storing a common identifier that identifies a user; and one or more hardware processors coupled to the memory and configured to read instructions from the memory to perform the steps of: receiving a token associated with a request to complete a transaction with an environment; determining the common identifier associated with the token, the common identifier being associated with an identifier of a merchant, an identifier of the user requesting the transaction, and a funding instrument associated with the user; and determining, based on information associated with the common identifier, whether to approve the transaction.

[0004b] According to another embodiment, a method of verifying a transaction, comprises receiving a token associated with a request to complete a transaction with an environment; determining the common identifier associated with the token, the common identifier being associated with an identifier of a merchant, an identifier of the user requesting the transaction, and a funding instrument associated with the user; and determining, based on information associated with the common identifier, whether to approve the transaction.

[0004c] According to another embodiment, a non-transitory machine-readable medium comprises a plurality of machine-readable instructions which, when executed by one or more processors, are adapted to cause the one or more processors to perform a method comprising receiving a token associated with a request to complete a transaction in an environment; determining the common identifier associated with the token, the common identifier being associated with an identifier of a merchant, an identifier of the user requesting the transaction,

and a funding instrument associated with the user; and determining, based on information associated with the common identifier, whether to approve the transaction.

BRIEF DESCRIPTION OF THE FIGURES

[0005] **Fig. 1** is an example process flow for issuing one or more tokens having a particular scope based on one or more rules.

[0006] **Fig. 2** is a flowchart illustrating an embodiment of a method of linking a common identifier (ID) to a user account and financial information provided by the user.

[0007] **Fig. 3** are example snapshots displayed on a mobile device illustrating the linking of the user's account to financial information.

[0008] **Fig. 4** is a flowchart illustrating an embodiment of a method of constructing a social graph.

[0009] **Fig. 5** is a flowchart illustrating an embodiment of a method of using a common ID to verify a transaction requested by the user, after the user's account has been linked to the user's financial information.

[0010] **Fig. 6** are example snapshots displayed on a mobile device illustrating the purchase of an item using the financial information linked to the user's account.

[0011] **Fig. 7** is an example process flow for user authentication.

[0012] **Fig. 8** is an example process flow for providing a token to a website with which the user is interacting to purchase a good from a third party.

[0013] **Fig. 9** is an example process flow for providing a token to the website.

[0014] **Fig. 10** is an example process flow for providing transaction information to a merchant or website.

[0015] **Fig. 11** is a block diagram illustrating the token service provider providing de-tokenized information to a funding source.

application accessible via a uniform resource locator (URL) to which a browser executing on the user device points. The user may interact with the merchant application to purchase items by placing them into an electronic shopping cart provided by the merchant application. Additionally, the merchant application may provide the user with the option to complete the purchase (or any transaction) using an account the user has with a payment service provider.

[0030] As will be discussed further below, the verification system may construct a social graph to determine the riskiness of approving the transaction.

[0031] A growing number of users interact with some type of social media platform, operating system, or other user environments. Users may communicate with their friends and a wider population by, for example, posting comments on a social media website. In this developing ecosystem, users typically share information on social media websites that are viewable by others. Additionally, users may interact more with social media websites than with their banks or financial institutions.

[0032] A user may be uneasy about providing their personal information (e.g., date of birth, mother's maiden name, or social security number) and financial information to a social media website. It may be more acceptable for the user to post information about herself on a social media website. Social media websites allow a user to connect with other users and post comments, which may be visible to the public. In some embodiments, the user's social characteristics/identity, relationships (e.g., friends on the social media website), and information (e.g., user's city of residence, places traveled) provided to the social media website are used to create a map of the user's life history. The user's life history may be illustrated in a social graph and may be more accurate and up-to-date regarding the user's habits and personality than information that is typically used to identify a user (e.g., social

WHAT IS CLAIMED IS:

1. A system, comprising:

a server associated with a token service provider, the server including a non-transitory memory and one or more hardware processors coupled to the non-transitory memory and configured to read instructions from the non-transitory memory to perform operations comprising:

receiving, from a token requestor, a request to generate a transactable token corresponding to a payment request for a transaction between a user and a merchant and corresponding to a common identifier associated with a funding instrument housing one or more payment methods;

generating the transactable token, the transactable token having a set of parameters defining a use of the transactable token, wherein the transactable token includes a token identifier that is not a funding instrument, and wherein the token identifier is used by the merchant to obtain funding for the transaction from the corresponding funding instrument; and

invoking a first application programming interface (API) exposed by the token requestor to store the transactable token in a token vault maintained by the token requestor.

2. The system of claim 1, further comprising:

a database maintained by the token service provider, the database storing a plurality of common identifiers and a plurality of funding instruments corresponding to a plurality of tokens generated by the token service provider,

wherein the server is further configured to perform operations comprising:

receiving the transactable token routed to the token service provider using the token identifier;

de-tokenizing the transactable token by searching the token vault to identify the common identifier associated with the token and using the common identifier to identify the corresponding funding instrument in the database; and

invoking a second API exposed by a payment server associated with the funding instrument to transmit transaction information to the payment server.

3. The system of claim 1, wherein the set of parameters defining the use of the transactable token includes a time to live of the transactable token, the time to live specifying a period of time from generation of the transactable token to expiration of the transactable token.

4. The system of claim 1, wherein the transactable token comprises a cryptogram.

5. The system of claim 1, wherein the transactable token is a single use token.

6. The system of claim 1, wherein the transactable token is an open loop token that is routable back to the token service provider that generated the transactable token.

7. The system of claim 1, wherein the transactable token is a closed loop token that is recognizable only by the token service provider that generated the transactable token.

8. A method, comprising:

receiving, by a token service provider from a token requestor, a request to generate a transactable token corresponding to a payment request for a transaction between a user and a merchant and corresponding to a common identifier associated with a funding instrument housing one or more payment methods;

generating the transactable token, the transactable token having a set of parameters defining a use of the transactable token, wherein the transactable token includes a token identifier that is not a funding instrument, and wherein the token identifier is used by the merchant to obtain funding for the transaction from the corresponding funding instrument; and

invoking a first application programming interface (API) exposed by the token requestor to store the transactable token in a token vault maintained by the token requestor.

9. The method of claim 8, further comprising:

receiving the transactable token routed to the token service provider using the token identifier;

de-tokenizing the transactable token by searching the token vault to identify the common identifier associated with the token and using the common identifier to identify the corresponding funding instrument in the database; and

invoking a second API exposed by a payment server associated with the funding instrument to transmit transaction information to the payment server.

10. The method of claim 8, wherein the set of parameters defining the use of the transactable token includes a time to live of the transactable token, the time to live specifying a period of time from generation of the transactable token to expiration of the transactable token.

11. The method of claim 8, wherein the transactable token is an open loop token that is routable back to the token service provider that generated the transactable token.

12. The method of claim 8, wherein the transactable token is a closed loop token that is recognizable only by the token service provider that generated the transactable token.

13. A non-transitory machine-readable medium comprising a plurality of machine-readable instructions which, when executed by one or more processors, are adapted to cause the one or more processors to perform operations comprising:

receiving, by a token service provider from a token requestor, a request to generate a transactable token corresponding to a payment request for a transaction between a user and a merchant and corresponding to a common identifier associated with a funding instrument housing one or more payment methods;

generating the transactable token, the transactable token having a set of parameters defining a use of the transactable token, wherein the transactable token includes a token identifier that is not a funding instrument, and wherein the token identifier is used by the merchant to obtain funding for the transaction from the corresponding funding instrument; and

invoking a first application programming interface (API) exposed by the token requestor to store the transactable token in a token vault maintained by the token requestor.

14. The non-transitory machine-readable medium of claim 11, wherein the operations further comprise:

receiving the transactable token routed to the token service provider using the token identifier;

de-tokenizing the transactable token by searching the token vault to identify the common identifier associated with the token and using the common identifier to identify the corresponding funding instrument in the database; and

invoking a second API exposed by a payment server associated with the funding instrument to transmit transaction information to the payment server.

15. The non-transitory machine-readable medium of claim 11, wherein the set of parameters defining use of the transactable token includes a time to live of the transactable token, the time to live specifying a period of time from generation of the transactable token to expiration of the transactable token.