Technical Disclosure Commons

Defensive Publications Series

June 03, 2016

AUTHENTICATING FINANCIAL ACCOUNTS

Ryan Weber

Andrew Nelson

AUTHENTICATING FINANCIAL ACCOUNTS

ABSTRACT

A transaction manager system associates a payment account with a user to allow future transactions with the payment account to be conducted in online transactions, mobile transactions, and other transactions. A user enters payment account information, such as a credit card account or a debit card account, into a user interface of the transaction manager system. The user enters user credentials for the user account on the card issuer that issued the payment account. The transaction manager system requests an authorization hold on the user account with the card issuer system. The transaction manager system submits the provided user credentials to the card issuer system to verify that the authorization hold has been processed. The success of the verification is an indication that the user possesses the proper credentials for the user account. After the verification, the transaction manager system allows future transactions to be conducted.

BACKGROUND

Payment accounts, such as credit card accounts and debit card accounts, are used to conduct transactions with merchants. A payment account may be employed by a user to conduct transactions over the Internet with a merchant, via a digital wallet application on a user computing device, and in many other suitable ways. The user may upload credentials of a payment account to a merchant website to be used for transactions. The user also may upload credentials of the payment account to a digital wallet application or a digital wallet account to be used to fund transactions. Merchants, digital wallet systems, third party fund transfer systems, or other systems that associate the payment account with the user for transactions are collectively referred to herein as transaction manager systems.

When a user chooses to upload a payment account, the transaction manager system that manages the future transactions often desires to verify that the payment account is associated with the user and is not being uploaded fraudulently. Conventional systems do not allow a transaction manager system to authenticate that the payment account belongs to the user.

OVERVIEW

A transaction manager system associates a payment account with a user to allow future transactions with the payment account to be conducted in online transactions, mobile transactions, and other transactions. A user enters payment account information, such as a credit card account or a debit card account, into a user interface of the transaction manager system. The user further enters user credentials for the user account on the card issuer system that issued the payment account, such as information required to log into the user account on a website of the card issuer system.

The transaction manager system requests an authorization hold on the user account with the card issuer system. The transaction manager system submits the provided user credentials to the card issuer system to verify that the authorization hold has been processed. The success of the verification is an indication that the user possesses the proper credentials for the user account at the card issuer system. After the verification, the transaction manager system determines that the payment account belongs to the user and allows future transactions to be conducted.

DETAILED DESCRIPTION

Figure 1 is a block diagram depicting a system to associate a payment account with a user to allow future transactions with the payment account to be conducted in online transactions, mobile transactions, and other transactions. As depicted in Figure 1, the system includes network computing devices that are configured to communicate with one another via one or more networks or via any suitable communication technology.

To conduct virtual transactions, such as mobile payments, online transactions, or other virtual transactions, a user uploads payment accounts to merchant systems, digital wallet systems, payment transfer systems, or other transaction manager systems. A user accesses a user interface of the transaction manager system, such as a website of a merchant, an interface page of an application, an online form entry page, or any other suitable user interface. The user interface may be hosted by the web server of the transaction manager system on a website of the transaction manager systems. The user

may utilize a communication application on the user computing device to upload the payment account and to perform other tasks.

The user selects a payment account to enter into the transaction manager system, such as a credit card account, a debit card account, a stored value card account, a bank account, or any other suitable payment account. The user enters the relevant data from the payment account into the user interface. For example, the user enters the payment account identification number, an expiration data of the account, information relating to the type of account, a user name, or any other suitable information. The user may enter the data by inputting the data into an online form, using an optical character recognition process on a card associated with the payment account or an image of the card, or by any other suitable method.

The user further enters user credentials for the user account on the card issuer system that issued the payment account. For example, the card issuer system may have a configured user name and password that allows the user to access the payment account on a web server of the card issuer system. The user may use the access to configure the payment account, check account balances, add funds to the account, verify purchase histories, and perform other suitable functions.

After receiving the payment account data and the user payment account credentials, the transaction manager system requests an authorization hold on the user account with the card issuer system. The hold may be for a nominal amount, such as $0.10 or $0.50. The transaction manager system may request the hold by utilizing the card network as used in a conventional transaction. For example, the transaction manager system may submit the authorization hold request to an acquirer, which submits the request to an appropriate credit card network. The credit card network submits the request to the card issuer system that issued the payment account.

The card issuer system receives the request and determines if the authorization request is approved. The approval may be based on the available balance on the user account, rules configured by the user on the account, or any other criteria. If the authorization request is approved, then the card issuer system supplies an approval back to the transaction manager system.

After receipt of the approved authorization hold request, the transaction manager system submits the provided user credentials to the card issuer system to verify that the authorization hold has been processed. For example, the transaction manager system communicates with the card issuer system and presents the user credentials to request access to the user account. The credit card system compares the provided credentials to the configured credentials for the user account. If the credentials match and are approved, the credit card issuer provides access to the user account to the transaction manager system.

The transaction manager verifies that the authorization hold has been placed on the user account by the card issuer system. For example, the transaction manager system submits a request to the credit card system to display recent transactions of the user account. The transaction manager system searches the recent transactions and identifies the requestor and/or the hold amount in the recent transactions. For example, if the transaction manager system placed a request for an authorization hold in the name of the transaction manager system for $0.50, then the transaction manager system can verify that the name and/or the pending charge for $0.50 are represented in the recent transactions.

The success of the verification is an indication that the user possesses the proper credentials for the user account at the card issuer system. That is, the transaction manager system would consider it unlikely that a fraudulent user would have access to the payment account data of the user and also the credentials for the user account on the card issuer system.

After the verification, the transaction manager system determines that the payment account belongs to the user. The transaction manager system performs any appropriate action with the payment account. For example, if the transaction manager system is a digital wallet system, then the payment account is loaded onto the digital wallet account of the user for use in virtual transactions using the digital wallet. In another example, if the transaction manager system is a merchant system, the payment account is stored in the user account on the transaction manager system to be used in transactions with the merchant system. In another example, if the transaction manager system is a third party fund transfer system, the payment account is loaded as a payment

instrument to be used when the user makes a purchase at a merchant and requests that the fund transfer system provide a payment to the merchant. After the verification process is completed, the transaction manager system cancels the authorization hold with the card issuer system. Additionally, the transaction manager system may delete all instances of the user credentials held by the transaction manager system to maintain security of the user's account.

In an alternative example, the user does not provide the user credentials at the card issuer system to the transaction manager system. Instead, after the authorization hold request has been provided by the transaction manager system, the user verifies the amount of the authorization hold.

In this example, the user enters the payment account information into the user interface of the transaction manager system. The user does not enter user credentials for the user account on the card issuer system that issued the payment account. The transaction manager system requests an authorization hold on the user account with the card issuer system. The transaction manager system informs the user of the request and instructs the user to verify the amount of the request. The user employs the user credentials to log into the card issuer system and access the user account. The user accesses the transaction history of the account and identifies the authorization hold requested by the transaction manager system. The user notes the amount of the hold, such as $0.50.

The user leaves the card issuer system and returns to the user interface of the transaction manager system. The user enters the amount of the hold into the user interface of the transaction manager system. If the amount entered by the user equals the amount requested by the transaction manager system, then the transaction manager system presumes that the user is the holder of the payment account. The transaction manager system stores the payment account in the user account and allows future transactions to be conducted. After the verification process is completed, the transaction manager system cancels the authorization hold with the card issuer system.

By using and relying on the methods and systems described herein, a transaction manager system associates a payment account with a user to allow future transactions with the payment account to be conducted in online transactions, mobile transactions, and

other transactions. By authenticating the user via the methods described herein, the transaction manager system prevents fraudulent users from uploading a payment account of the user. The authentication of the user is performed in a manner that is safe, secure, efficient, and swift. The system is improved for a user in that the user payment accounts will be more secure, and the user will be able to be authenticated seamlessly and securely. As the transaction manager system will not require a burdensome amount of secure data from the user, and impediments to completing the authentication are removed. Hence, the methods and systems described herein improve the user experience and provide improved security for user accounts.

In some embodiments, a user associated with a user computing device must install an application and/or make a feature selection to obtain the benefits of the techniques described herein.

In situations in which the systems discussed here collect personal information about users, or may make use of personal information, the users may be provided with a opportunity to control whether programs or features collect user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), or to control whether and/or how to receive content from the content server that may be more relevant to the user. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over how information is collected about the user and used by a content server.

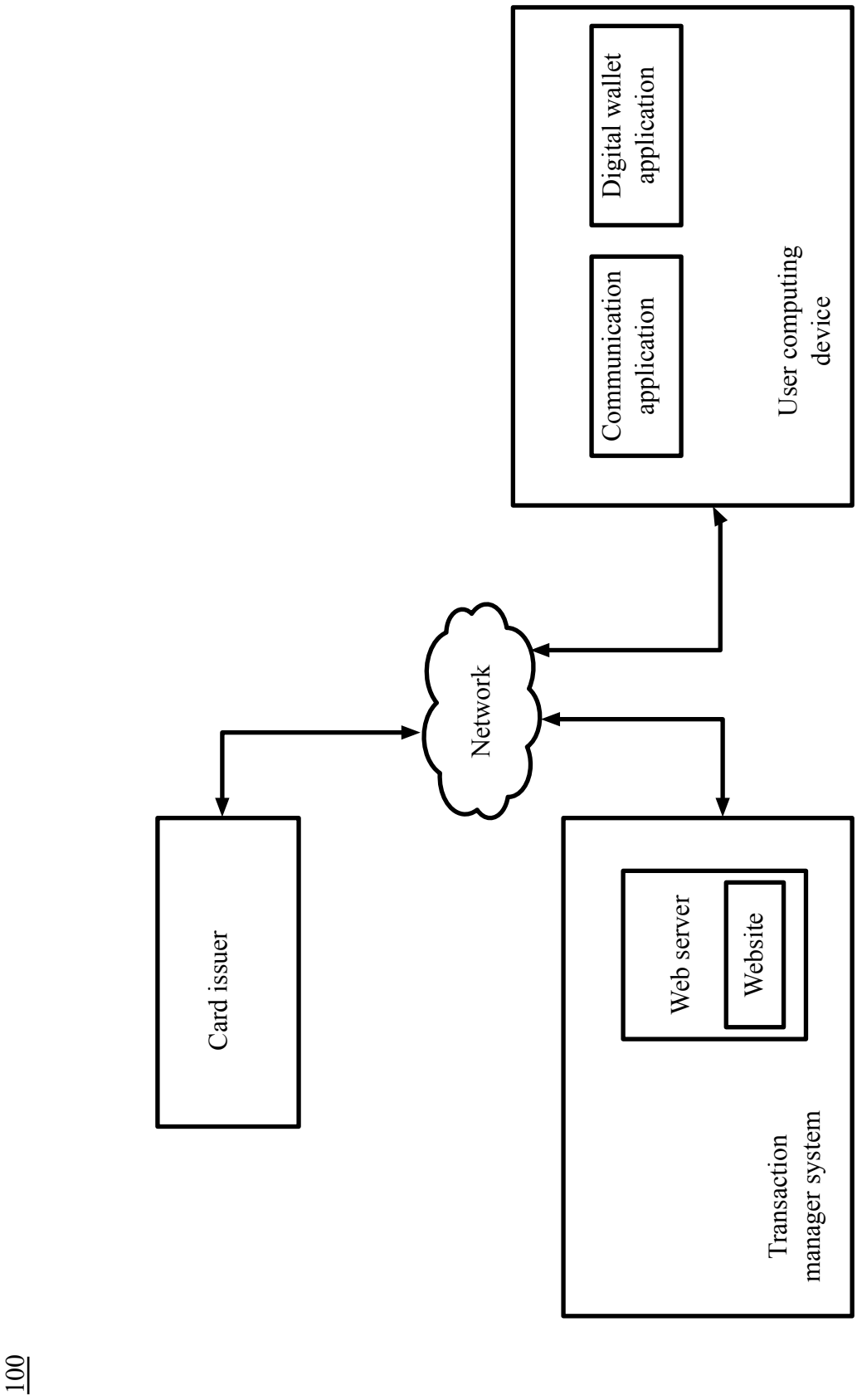
100
Card issuer
Network
User computing device
Digital wallet application
Communication application
Transaction manager system
Web server
Website

Fig. 1