March 03, 2017

Payment Card Image Backup

Owen Jones
Juancheng Rong

Follow this and additional works at: http://www.tdcommons.org/dpubs_series

Recommended Citation
Jones, Owen and Rong, Juancheng, "Payment Card Image Backup", Technical Disclosure Commons, (March 03, 2017)
http://www.tdcommons.org/dpubs_series/412

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
PAYMENT CARD IMAGE BACKUP

Abstract

In concert with applications that tokenize payment cards, an image of the card can be stored to allow use of the payment card outside an electronic payment process.

Keywords


Description

Mobile wallet technology, also commonly referred to as “electronic wallet” and “digital wallet” technology, allows users to present a mobile device at point of sale (POS) payment equipment to conduct a transaction at a brick-and-mortar merchant location using a payment card. Some electronic wallets allow the user to make online payments via the electronic wallet.

While the present document refers to “payment cards,” such as credit cards and debit cards, the technology described herein can find use with cards of other user accounts, for example, loyalty accounts, coupon account, and travel accounts.

Referring to Figure 1, in typical electronic wallet architectures, the electronic wallet application provider maintains an account for the user in an electronic wallet server. The electronic wallet server interacts with both merchant systems (such as a POS system) and conventional payment card authorization and processing systems via the Internet to complete transactions.
Typical electronic wallet applications do not store the user’s payment card information on the user’s mobile device. Rather, the electronic wallet application “tokenizes” the payment card. With payment card tokenization, an alias or placeholder account number remains stored on the user’s mobile device. The actual payment account information is stored with the electronic wallet server.

A user can initiate a payment transaction with the electronic wallet by presenting the mobile device at a brick-and-mortar merchant’s POS system. Upon presentation, the POS system and the user’s mobile device establish a communications channel. For example, “tapping” the mobile device at a POS system may establish a communications channel between the mobile device and the POS system using Near Field Communication (NFC) technology. Other communications channels, such as a Bluetooth wireless communication technology channel or a Wi-Fi™ wireless communications channel can be used apart from, or in conjunction with, the NFC channel.

The user’s mobile device and the merchant’s POS system exchange information, including user’s mobile device communicating the alias account information to the merchant’s POS system, via the communications channel established between them. The merchant’s POS system interacts with the electronic wallet to receive the actual account information. From this point, the transaction can be processed as if the user had presented a physical payment card to the merchant.

Outside the brick-and-mortar context, electronic wallets can be used to complete transactions online between a user and a merchant. In such cases, the communications channel between the merchant’s web server and the user’s computing device is a network such as the Internet.
Given the convenience of conducting transactions as described above, some users, particularly in areas where many brick-and-mortar merchant locations are equipped with POS systems that can interact with electronic wallets, do not continue to carry the physical payment card. However, other users continue to carry physical payment cards for when they encounter brick-and-mortar merchant locations that are not equipped with POS systems that can interact with electronic wallets.

Typically, when a user establishes an electronic wallet account, the user either enters payment account information into the electronic wallet system manually, or captures an image of the physical payment card using the camera of the user’s mobile device. In the latter case, either of the user’s mobile device or the electronic wallet server can perform optical character recognition (OCR) on the captured image to identify and extract the pertinent payment information from the captured image for use in the electronic wallet. As mentioned above, the payment card information is typically stored on the electronic wallet server and not on the user’s mobile device. In some cases, both the back and the front of the payment card are captured when the user establishes, or updates an electronic wallet account.

The present technology can allow the user to refrain from carrying physical payment cards, yet use the account of the physical payment card for those instances when a merchant brick-and-mortar merchant location lacks a POS system that can interact with electronic wallets. The present technology also applies to those instances when a merchant brick-and-mortar location has an electronic wallet-enabled POS system, but the electronic wallet-enabled POS system fails to complete the requested transaction. The present technology also applies to online transactions, wherein the user can access the details from the image for online transactions, for
example, reading the (non-tokenized) card number from the image and entering it online when
the online merchant does not support mobile wallets.

The present technology stores payment card information on the user’s device. Referring
to Fig. 2, in some instances, when the user captures an image of a payment card, the image is
stored on the user’s device. In particular, the image can be stored within the portion of the
payment application residing on the user’s device. The stored image can be encrypted to protect
the information from unauthorized access. Such encryption can require the user’s fingerprint or
some form of two-factor authentication to decrypt and make the image available via the user’s
device.

In some instances, capturing an image of the payment card to store on the user’s device
can be an activity separate from adding a payment card to the electronic payment account or
updating payment account information.

In some instances, the image of the user’s payment card can be stored in memory
associated with the electronic wallet server, and retrieved for presentation via the user device
after the user device receives and authenticates a request for the stored image. In each case, the
user’s device can present the stored image to the user for use in transactions where the electronic
wallet itself is not an available or acceptable form of payment.

As depicted in the Fig. 1, an architecture for the present technology includes network
devices; each of which may be configured to communicate with one another via a
communications network, such as the Internet. A user associated with a device may have to
install an application and/or make a feature selection to obtain the benefits of the technology
described herein.
In situations in which the technology discussed herein collects personal information about users, or may make use of personal information, the users may be provided with an opportunity or option 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 a 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 personally identifiable information cannot 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 the technology collects and uses information about the user.
FIG. 1

User's mobile device

Merchant POS system

Communications network

Electronic wallet server

Payment processing system
Capture payment card image

Store captured image on the mobile device hosting an electronic wallet application

Receive authenticated request for the stored image

Present the stored image in response to receiving the authenticated request

FIG. 2