magnetic stripe capture, storage and transmission device for use in conjunction with a mobile wallet application to capture, store and transmit magnetic stripe card data to merchants' conventional point of sale (POS) terminals and other devices with magnetic stripe readers (MSRs) or checkout systems, in physical and virtual environments. The disclosure also relates to mobile checkout systems and methods. The system provides a convenient buying experience for consumers, a secure and informative transaction for merchants, and in some cases additional data to be transmitted to a MSR for the purpose of loyalty, identification (ID), or access control.

In accordance with a first aspect, there is provided a checkout system implemented on a mobile communication device including a merchant application or browser application available on the mobile communication device and adapted to allow a user to select items to purchase from a merchant, comprising: a communication processor in communication with a checkout server hosting one or more web service checkout application program interfaces (APIs) adapted to communicate with the mobile communication device; and a checkout application installed on the mobile communication device and adapted: to be launched in response to receiving information corresponding to a purchase transaction; to receive user payment information, including magnetic stripe data, from a magnetic stripe transporter (MST) embedded in or in communication with the mobile communication device, wherein a cryptogram is generated at the time of the purchase transaction and included in the magnetic stripe data to secure the magnetic stripe data; and to communicate with the checkout server and cause the checkout server to complete the purchase transaction using the magnetic stripe data from the magnetic stripe transporter.

In accordance with a second aspect, there is provided a method, comprising: allowing a user to browse and select items for purchase from a merchant through a first application or browser; launching a checkout application installed on a mobile communication device in response to the checkout application receiving information corresponding to a purchase transaction; receiving, by the checkout application, a checkout token identifying the purchase transaction created by a checkout server; receiving, by the checkout application, user payment information, including magnetic stripe data, from a magnetic stripe transporter (MST) embedded in, or in communication

with the mobile communication device, wherein a cryptogram is at the time of the purchase transaction and included in the magnetic stripe data to secure the magnetic stripe data; and communicating, by the checkout application, with the checkout server to cause the checkout server to complete the purchase transaction using secured magnetic stripe data from the magnetic stripe transporter; and relaunching the first application or browser in response to completion of the transaction.

In one embodiment, a system for securely capturing, storing and transmitting magnetic stripe payment card data includes a mobile communication device and mobile application, and a magnetic stripe transporter (MST), which can be in the form of an external dongle, or its necessary components be part of the consumer mobile communication device. The MST dongle or built in MST includes a microprocessor, magnetic field transmitter which includes a driver and an inductor that can generate varying magnetic fields, a battery, a charging circuit, a magnetic stripe reader (MSR), a memory means or secure element, plus for the embodiment of a dongle, an audio jack interface, and a communication interface (for example, a USB interface, a 30pin or 9pin Apple interface, a Bluetooth interface, etc.) working in conjunction with a consumer mobile device and wallet application for capturing magnetic stripe card data, storing the data securely (which may include incorporating a cryptogram in the magnetic stripe card data), and transmitting such data to merchants' point of sale (POS) or checkout systems, in the physical and virtual environments.

Embodiments of the disclosure may include one or more features. The mobile communication device may include a mobile application that initializes the MST for use with a specific wallet account and unlocks the MST for transmission and use. The mobile communication device may be used with a payment checkout application on the mobile communication device or the Internet that interacts with the MST to accept payment card data, which may include a dynamic cryptogram to secure the payment data, from the MST and transmit the payment card data to a payment server for processing a transaction either as a merchant POS application or a consumer checkout application. The mobile wallet application may interact with the MST via the audio jack or other

communication interface, in various modes of operation including, for example, an Initialize and Reset Mode, a Load Card Delete Card Mode, a Transmit and Use Mode, a Disconnected Transmit Mode, and a POS Card Read Mode.

In one embodiment, the MST operated in the Initialize and Reset Mode is configured to allow a user to pair and unpair/reset a specific MST with a mobile wallet account and only allow one device per account. The MST operated in the Load Card Delete Card Mode is configured to allow a user to load magnetic stripe card data by swiping the user's existing plastic magnetic stripe card on the MSR on board the MST and store the card track data in a memory means or secure element. For payment cards, the application loads the primary account number (PAN) data of the card to an online digital wallet via the mobile wallet application. Card information can also be deleted from the memory means and the server using the application. The MST operated in the Transmit and Use Mode is configured to allow a user to select a specific payment card as a top of wallet or default card for use in transmission of the stored track data to the merchant POS system when a button is activated or pressed. In another embodiment, if non-payment cards are stored in the MST, one non-payment card can be stored as the default card to transmit without authenticating to the wallet application and selecting such a card. Non-payment cards include hotel keys, door passes, or ID and Loyalty cards that can be loaded to the MST in a separate memory means for transmission later.

The MST operated in the POS Card read Mode is configured to allow a user to swipe a payment card with the MST's MSR and transmit the card data to a POS application on the mobile communication device then to the payment server and processor. The mobile communication device may be a smartphone, a tablet, or a personal computer. The MST further includes a battery and a charging circuit. The microprocessor is configured to provide security and communications with the mobile communication device. The memory means stores payment card data securely. The MST is configured to transmit card track data to a merchant checkout application on the mobile communication device to create a card-present transaction for the merchant. The MST may also be configured to read payment cards and to transmit payment card data to the mobile communication device and associated POS application that in turn then transmits the transaction and card data to the payment servers and processors like a POS.

In another embodiment, the disclosure features a method for securely capturing, storing and transmitting magnetic stripe card data. A magnetic stripe transporter (MST) dongle includes a microprocessor, a driver configured to send current and signal to an inductor that creates varying magnetic fields, a battery, a charging circuit, a magnetic stripe card reader, a memory means or secure element, an audio jack interface, and a communication interface (for example, a USB interface, a 30pin or 9pin Apple interface, and a Bluetooth interface, etc.) working in conjunction with a consumer mobile communication device and a wallet application or mobile application for capturing magnetic stripe card data, storing the card data securely, and transmitting such data to merchants' point of sale (POS) terminals, checkout systems, or other MSR devices, in a physical and virtual environment.

The systems and methods disclosed herein provide a number of advantages, for example, the magnetic card track data can be captured and stored in the MST's secure memory means directly by the user or from the server without modification of the magnetic stripe data, to be used later with a MSR device. For payment cards, no change to the magnetic stripe data is needed as opposed to contactless or NFC track data that has special fields that must be encoded by the card issuers in order to function properly with a contactless POS. The MST may include a button that allows transmission of the magnetic card data to a POS while the MST is disconnected or detached from the mobile device.

In an embodiment, the unique paring of a MST to a specific wallet account can provide better security, and the ability to reset a MST allows un-pairing and reuse of a MST. Further, the system and method according to the disclosure provides the ability to connect to mobile communication devices via different interfaces beyond audio jack and USB. Also, the process of loading encrypted magnetic stripe track data into memory means of the MST may later be decrypted and transmitted to the MSR of the POS, or for the data to be transmitted encrypted to the mobile communication device and then routed to the payment server for decryption and processing for loading a wallet account on the server or processing a POS transaction.

The system and method according to the disclosure provides the ability to use the stored track data or swiped track data for virtual checkout environments for a more secure

and lower cost transaction for merchants, and the remote loading of track data from a card issuer to the wallet server provider to the wallet application on the mobile communication device, to the secure element (SE) or memory means of the MST to be used later. Still further, the system and method provides the ability to load loyalty account information along with the payment card data into discretionary fields of the track data to be read by the issuer upon a transaction, which can lead to offers and loyalty programs combined with a payment transaction.

The combined use of all of the above technologies in a seamless user experience for consumers may increase the frequency of use of mobile wallets and allow a host of applications and functionalities, such as, offers and loyalty with consumers that make it more compelling and deliver value to the consumers and the merchants.

In another embodiment, the magnetic stripe card data may be transmitted to the mobile communication device's checkout application and used in a mobile checkout system. Mobile checkout systems and methods are disclosed that aid in reducing drop-out rates of shopping carts and increasing conversion rates into sales. However, it should be appreciated that the mobile checkout systems and methods disclosed herein may be implemented with or without the MST.

In general, the mobile checkout systems and methods include a mobile communication device having a merchant application and/or browser application installed on the mobile communication device that allows a user to select items to purchase from a merchant website. A checkout application is also installed on the mobile communication device that communicates with a checkout server hosting one or more web service checkout application program interfaces (APIs). The checkout application may be launched in response to receiving information corresponding to a purchase transaction, such as when a user selects items to purchase and selects checkout. The checkout application communicates with the checkout server to cause the checkout server to complete the purchase transaction, by communicating with a payment processor. When the transaction is complete the merchant application or browser application that was used to browse and select the items for purchase is relaunched.

In other embodiments, the checkout application may be launched in response to receiving the information corresponding to the purchase transaction from the checkout