CLAIMS

1. 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, the checkout system 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, the checkout application is adapted 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,

generate a cryptogram using at least one of a checkout token identifying the purchase transaction, timestamp or counter at the time of the purchase transaction,

incorporate the cryptogram in the magnetic stripe data to secure the magnetic stripe data, and

communicate the secured magnetic stripe data to the checkout server to cause the checkout server to complete the purchase transaction.

2. The checkout system of claim 1, wherein the checkout server creates the checkout token identifying the purchase transaction in response to the user initiating the purchase transaction.

3. The checkout system of claim 2, wherein the checkout server sends the checkout token to the merchant application or browser application.

4. The checkout system of claim 3, wherein the checkout application receives the checkout token from the merchant application or browser application.

5. The checkout system of claim 4, wherein the checkout application authenticates the user.

6. The checkout system of claim 5, wherein the checkout application confirms the purchase transaction with the checkout server in response to the user authentication.

7. The checkout system of claim 6, wherein the checkout application sends the checkout token and results of the purchase transaction to the merchant application or browser application during relaunch of the merchant application or browser application.

8. The checkout system of claim 7, wherein the merchant application or browser application displays a results page corresponding to the purchase transaction in response to being relaunched.

9. The checkout system of claim 1, wherein the checkout server completes the purchase transaction by communicating the purchase transaction, including the secured magnetic stripe data incorporated with the cryptogram, to a payment processor.

10. The checkout system of claim 1, wherein the checkout application is adapted to be launched in response to receiving the information corresponding to the purchase transaction from the merchant application or browser application.

11. The checkout system of claim 1, wherein the checkout application is adapted to be launched in response to receiving the information corresponding to the purchase transaction from the checkout server.

12. The checkout system of claim 1, wherein the checkout application is adapted to be launched in response to receiving the information corresponding to the purchase transaction from the checkout server through a push notification, email, or short message service.

13. The checkout system of claim 1, wherein the checkout application is adapted to be launched in response to receiving the information corresponding to the purchase transaction from a quick response (QR) code scanned by the mobile communication device.

14. A method, comprising:

allowing a user to browse and select items for purchase from a merchant through a merchant application or browser application available on a mobile communication device;

launching a checkout application installed on the mobile communication device in response to the mobile communication device receiving information corresponding to a purchase transaction;

receiving, by the checkout application, a checkout token identifying the purchase transaction;

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;

generating, by the checkout application, a cryptogram using at least one of the checkout token, timestamp or counter at the time of the purchase transaction;

incorporating, by the checkout application, the cryptogram in the magnetic stripe data to secure the magnetic stripe data;

communicating, by the checkout application, the secured magnetic stripe data to the checkout server to cause the checkout server to complete the purchase transaction; and

relaunching, by the mobile communication device, the merchant application or browser application in response to completion of the purchase transaction.

15. The method of claim 14, wherein the receiving of the checkout token includes receiving the checkout token from the merchant application or browser application.

16. The method of claim 14, further comprising authenticating, by the checkout application, the user prior to the communicating with the checkout server.

17. The method of claim 14, wherein the launching of the checkout application includes launching the checkout application in response to receiving the information corresponding to the purchase transaction from the checkout server through a push notification, email, or short message service.

18. The method of claim 14, wherein the launching of the checkout application includes launching the checkout application in response to receiving the information corresponding to the purchase transaction from user scanning a quick response (QR) code.