

embodiments, the replacement transaction may be packaged and forwarded to the user/cardholder.

[051] Continuing to refer to Figure 4, at block 416, on receipt of a request for a bypass authorization code from a false fraudulent correction service of a payment processor, process 400b for false fraudulent correction service by a merchant may respond with the requested bypass authorization code. As described earlier, the exchange may be provided over a secure communication channel between the false fraudulent correction service of a payment processor and the counterpart of a merchant.

[052] At block 418, on receipt of the replacement transaction with the bypass authorization code from the user/cardholder, process 400b may validate the bypass authorization code. At block 420, on validation of the bypass authorization code, the merchant may proceed to complete the replacement transaction, successfully remedying the falsely declined transaction, and thereby reducing the amount of false fraudulent declines.

[053] Figure 6 illustrates in further detail components of the false fraudulent correction service of the payment systems provider, according to some embodiments. For the illustrated embodiments, false fraudulent correction service 600, which may be false fraudulent correction service 120 of Figure 1, may include registrar 602, request acceptor 604, user communicator 606, merchant communicator 608, transaction data collector 610 and replacement transaction builder 612.

[054] Registrar 602 may be configured to register merchants having the complementary ability to provide the bypass authentication codes for inclusion in replacement transactions as partner false fraudulent correction merchants. In various embodiments, the registrations may include identifications of the merchants, communication addresses and protocols of the merchants, in particular, the secure communication protocols supported by the merchants.

[055] Request acceptor 604 may be configured to accept notifications of declined transactions and requests to determine whether the declined transactions are indeed fraudulent, and if not, remedy the declined transactions. In various embodiments, request acceptor 604 may include a communication interface for any of the merchants, acquirers, fraud detection services of payment processors, and/or issuers to provide the notifications

languages known in the art, and compiled into executable object codes, executable on the one or more servers of the payment processor. In other embodiments, some or aspects of registrar 602, request acceptor 604, user communicator 606, merchant communicator 608, transaction data collector 610 and replacement transaction builder 612 may be implemented as firmware, and/or accelerated using hardware accelerators. In still other embodiments, some or aspects of registrar 602, request acceptor 604, user communicator 606, merchant communicator 608, transaction data collector 610 and replacement transaction builder 612 may be implemented in hardware, e.g., application specific integrated circuits (ASICs).

[061] Figure 7 illustrates in further detail components of the false fraudulent correction service of a merchant, according to some embodiments. For the illustrated embodiments, false fraudulent correction service 700, which may be false fraudulent correction service 122 of Figure 1, may include payment processor communicator 702 and bypass authentication code generator 704.

[062] Payment processor communicator 702 may be configured to communicate with a payment processor. In various embodiments, payment processor communicator 702 may be configured to report to the payment processor, notifications of declined transactions and requests to determine whether the declined transactions are indeed fraudulent, and if not, remedy the declined transactions. In various embodiments, payment processor communicator 702 may be further configured to securely provide the bypass authentication codes to the payment processor for inclusion in replacement transactions.

[063] Bypass authentication code generator 704 may be configured to generate the bypass authentication codes to be provided to the payment processor for inclusion in replacement transactions. Various secure/cryptographic authentication code generation schemes may be employed to generate the bypass authentication codes.

[064] In various embodiments, payment processor communicator 702 and bypass authentication code generator 704 may be implemented in any one of a number high level programming languages known in the art, and compiled into executable object codes, executable on the one or more servers of the payment processor. In other embodiments, some or aspects of payment processor communicator 702 and bypass authentication