should be applied. The authenticity assessment request may include at least a portion of the transaction data, including, but not limited to, a payment device identifier, a user identifier, an issuer institution identifier, and/or the like. At step 208, the transaction service provider system receives, from the behavioral biometrics server computer, an authenticity assessment response generated by the behavioral biometrics server computer in response to the authenticity assessment request. The authenticity assessment response may be based on the portion or all of transaction data communicated to the behavioral biometrics server computer.

[0088] At step 210, the transaction service provider system generates an authentication response message configured to authenticate or decline the transaction. The authentication response message is based on (e.g., at least partly on) the authenticity assessment response. For example, the authentication assessment may indicate a likelihood of the transaction being authentic such that, when evaluated by the transaction service provider system in combination with a second factor authentication (e.g., one-time password), there is a strong likelihood the transaction is not fraudulent. Based on that combined evaluation, the transaction service provider system may authenticate the transaction. In another example, if the authenticity assessment indicates a strong likelihood the transaction was not authorized by the user, the transaction service provider system may decline the transaction even if a second factor authentication test is passed.

[0089] Referring now to FIG. 3, illustrated is a flowchart of a non-limiting embodiment of a process 300 for authenticating a transaction based on behavioral biometric data. It will be appreciated that, in non-limiting embodiments, a process 300 may include additional, fewer, and/or different steps and a different order of steps. In some non-limiting embodiments, one or more of the steps of process 300 may be performed (e.g., completely, partially, and/or the like) by transaction service provider system 108 (e.g., one or more devices of transaction service provider system 108, such as directory server computer 110). In some non-limiting embodiments, one or more of the steps of process 300 may be performed (e.g., completely, partially, and/or the like) by another device or a group of devices separate from or including transaction service provider system 108, such as payment device 104 (e.g., one or more devices of payment device 104), merchant system 106 (e.g., one or more devices of merchant system 106), behavioral biometrics server computer 112 (e.g., one or more devices of

passwords). BBCS provides an efficient, non-time-consuming authentication while allowing for a modular, independent integration with existing authentication systems. BBCS can provide multifactor compliance in both 3DS 2.x and 3DS 1.0 environments. BBCS may be employed for web applications, native applications, and other channels.

[0104] BBCS may be provided as a standalone service, such as part of the transaction service provider system, e.g., a directory server service. BBCS may be provided directly to the issuer/ACS provider. BBCS provides the ability to gather behavioral biometrics signals for a given 3DS transaction. BBCS provides the ability to evaluate and make decisions based on behavioral biometrics signals. BBCS further provides the ability to combine the success/failure of another authentication process (e.g., one-time passwords) with the behavioral biometrics authentication to provide a final response to components within the 3DS ecosystem (e.g., a directory server of a transaction processing system, a 3DS server, a merchant system, etc.).

[0105] In a 3DS 2.x web browser process flow, the directory server may register the method URL endpoint that supports both the behavioral biometrics code as well as the issuer/ACS provider's method URL. In a 3DS 2.x native application flow, a software development kit (SDK) may be provided for first party or third party behavioral biometrics that will collect and send the signals to a BBCS server in parallel to device data collected according to EMV specifications. In a 3DS 1.0 process flow, the issuer ACS step-up window may be framed within a BBCS-provided URL, which may allow for signal collection code to be executed during the step-up authentication process.

[0106] In non-limiting embodiments, evaluation and decision making based on behavioral biometric signals may be performed based on the technology framework for the BBCS implementation, e.g., as a local or remote callout to the technology provider. BBCS may be a learning system, where profiles of behavioral biometric data may be maintained and improved over time. Depending on the point of integration of BBCS, different approaches may be taken to combine responses from BBCS and from alternative means of authentication (e.g., one-time passwords), and to provide the outcome. For example, a transaction identifier captured during behavioral biometric signal collection may be provided to a directory server, which can update a transaction request or response based on the decision from the BBCS server and drop the cardholder verification value (CVV) if a transaction fails the BBCS evaluation. Alternatively, the URL for BBCS integration may be overridden to allow for transaction request values to be updated based on behavioral biometric decision making.