WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

receiving, with a transaction service provider system comprising at least one processor, an authorization request message from a merchant system, the authorization request message associated with a transaction between the merchant system and a payment device, the authorization request message initiated by a user of the payment device through a merchant webpage or mobile application, and the authorization request message comprising transaction data;

determining, with the at least one processor, that an additional security authentication should be applied to the authorization request message, based on the payment device being associated with an issuer that has specified that behavioral biometrics should be employed as a secondary form of authentication;

in response to determining that the additional security authentication should be applied, and before the authorization request message is transmitted to an issuer system of the issuer, communicating, with the at least one processor, an authenticity assessment request to a behavioral biometrics server computer that is associated with the transaction service provider system and independent of the issuer system, the authenticity assessment request communicated to the behavioral biometrics server computer while the user is responding to a second factor authentication process in the merchant webpage or the mobile application, and the authenticity assessment request comprising at least a portion of the transaction data;

receiving, with the at least one processor from the behavioral biometrics server computer, an authenticity assessment response generated by the behavioral biometrics server computer in response to the authenticity assessment request and based on the at least a portion of the transaction data; and

generating, with the at least one processor based on the authenticity assessment response, an authentication response message configured to authenticate or decline the transaction.

2. The computer-implemented method of claim 1, further comprising embedding a behavioral biometrics service in the merchant webpage or the mobile application based on a first uniform resource locator (URL) and a second URL, wherein the first URL points to a domain of the issuer system and the second URL points to a domain of the behavioral biometrics server computer.

3. The computer-implemented method of claim 2, further comprising, in response to the authenticity assessment response indicating a lack of authenticity of the user and/or the payment device, communicating an alert to at least one of the merchant webpage, the mobile application, and the issuer system.

4. The computer-implemented method of claim 1, further comprising communicating, with the at least one processor, the authentication response message to the issuer system associated with the issuer of the payment device, the authentication response message configured to authenticate or decline the transaction when evaluated by the issuer system in combination with a user response to the second factor authentication process.

5. The computer-implemented method of claim 1, wherein the authentication assessment response is based on behavioral biometrics signals associated with the payment device and/or user that are collected, prior to the transaction being initiated, by the behavioral biometrics server computer in a separate communication channel to a transaction processing network of the transaction service provider system.

6. The computer-implemented method of claim 1, further comprising configuring the authentication response message to authenticate or decline the transaction based on a comparison of the authenticity assessment response to a predetermined threshold provided by the merchant system.

7. A system comprising at least one server computer including at least one processor, the at least one server computer programmed and/or configured to:

receive an authorization request message from a merchant system, the authorization request message associated with a transaction between the merchant system and a payment device, the authorization request message initiated by a user of the payment device through a merchant webpage or mobile application, and the authorization request message comprising transaction data;

determine based on the transaction data that an additional security authentication should be applied to the authorization request message, based on the payment device being associated with an issuer that has specified that behavioral biometrics should be employed as a secondary form of authentication;

in response to determining that the additional security authentication should be applied, and before the authorization request message is transmitted to an issuer system of the issuer, communicate an authenticity assessment request to a behavioral biometrics server computer that is associated with a transaction service provider system and independent of the issuer system, the authenticity assessment request communicated to the behavioral biometrics server computer while the user is responding to a second factor authentication process in the merchant webpage or the mobile application, and the authenticity assessment request comprising at least a portion of the transaction data;

receive, from the behavioral biometrics server computer, an authenticity assessment response generated by the behavioral biometrics server computer in response to the authenticity assessment request and based on the at least a portion of the transaction data; and

generate, based on the authenticity assessment response, an authentication response message configured to authenticate or decline the transaction.

8. The system of claim 7, wherein the server computer is further programmed and/or configured to embed a behavioral biometrics service in the merchant webpage or the mobile application based on a first uniform resource locator (URL) and a second URL, wherein the first URL points to a domain of the issuer system and the second URL points to a domain of the behavioral biometrics server computer.

9. The system of claim 8, wherein the server computer is further programmed and/or configured to, in response to the authenticity assessment response indicating a lack of authenticity of the user and/or the payment device, communicate an alert to at least one of the merchant webpage, the mobile application, and the issuer system.

10. The system of claim 7, wherein the server computer is further programmed and/or configured to communicate the authentication response message to the issuer system associated with the issuer of the payment device, the authentication response message configured to authenticate or decline the transaction when evaluated by the issuer system in combination with a user response to the second factor authentication process.

11. The system of claim 7, wherein the authentication assessment response is based on behavioral biometrics signals associated with the payment device and/or user that are collected, prior to the transaction being initiated, by the behavioral biometrics server computer in a separate communication channel to a transaction processing network of the server computer.

12. The system of claim 7, wherein the server computer is further programmed and/or configured to configure the authentication response message to authenticate or decline the transaction based on a comparison of the authenticity assessment response to a predetermined threshold provided by the merchant system.

13. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

receive an authorization request message from a merchant system, the authorization request message associated with a transaction between the merchant system and a payment device, the authorization request message initiated by a user of the payment device through a merchant webpage or mobile application, and the authorization request message comprising transaction data;

determine that an additional security authentication should be applied to the authorization request message, based on the payment device being associated with an issuer that has specified that behavioral biometrics should be employed as a secondary form of authentication;

in response to determining that the additional security authentication should be applied, and before the authorization request message is transmitted to an issuer system of the issuer, communicate an authenticity assessment request to a behavioral biometrics server computer that is associated with a transaction service provider system and independent of the issuer system, the authenticity assessment request communicated to the behavioral biometrics server computer while the user is responding to a second factor authentication process in the merchant webpage or the mobile application, and the authenticity assessment request comprising at least a portion of the transaction data;

receive, from the behavioral biometrics server computer, an authenticity assessment response generated by the behavioral biometrics server computer in response to the authenticity assessment request and based on the at least a portion of the transaction data; and

generate, based on the authenticity assessment response, an authentication response message configured to authenticate or decline the transaction.

14. The computer program product of claim 13, wherein the program instructions further cause the at least one processor to embed a behavioral biometrics service in the merchant webpage or the mobile application based on a first URL and a second URL, wherein the first uniform resource locator (URL) points to a domain of the issuer system and the second URL points to a domain of the behavioral biometrics server computer.

15. The computer program product of claim 14, wherein the program instructions further cause the at least one processor to, in response to the authenticity assessment response indicating a lack of authenticity of the user and/or the payment device, communicate an alert to at least one of the merchant webpage, the mobile application, and the issuer system.

16. The computer program product of claim 13, wherein the program instructions further cause the at least one processor to communicate the authentication response message to the issuer system associated with the issuer of the payment device, the authentication response message configured to authenticate or decline the transaction when evaluated by the issuer system in combination with a user response to the second factor authentication process.

17. The computer program product of claim 13, wherein the authentication assessment response is based on behavioral biometrics signals associated with the payment device and/or user that are collected, prior to the transaction being initiated, by the behavioral biometrics server computer in a separate communication channel to a transaction processing network of the server computer.