WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a first server computer, authentication data for a user from a user device, the authentication data including user identification data that identifies the user;

determining, by the first server computer, a biometric identifier, as a random number or string of characters that does not reveal information about the user, to be associated with the authentication data;

storing, by the first server computer, the biometric identifier in association with the user identification data in a database of the first server computer;

transmitting, by the first server computer, the biometric identifier to a second server computer along with a first encrypted biometric template associated with the user, the second server computer storing the biometric identifier in association with the first encrypted biometric template;

in response to receiving, by the first server computer from the user device, a biometric identifier request message comprising the user identification data and a request for the biometric identifier, transmitting, by the first server computer to the user device, the biometric identifier retrieved by the first server computer from the database based on the user identification data, wherein the second server computer subsequently receives a second encrypted biometric template and the biometric identifier from the user device, identifies the first encrypted biometric template using the biometric identifier, and generates an encrypted match value data file by comparing the first encrypted biometric template and the second encrypted biometric template;

receiving, by the first server computer, the encrypted match value data file;

decrypting, by the first server computer, the encrypted match value data file to determine a decrypted match value data file; and

determining, by the first server computer from the decrypted match value data file, a match likelihood value.

2. The method of claim 1, wherein the first server computer is an enrollment server computer and the second server computer is a match server computer.

3. The method of claim 1, wherein the second encrypted biometric template is received by the second server computer in relation to a transaction to be completed by the user.

4. The method of claim 1, wherein the match likelihood value represents a likelihood that the first encrypted biometric template and the second encrypted biometric template are generated from the same user.

5. The method of claim 1, wherein the match likelihood value is represented as a numeric value.

6. The method of claim 1, further comprising comparing the match likelihood value to an acceptable risk threshold value to determine whether the user is authenticated.

7. The method of claim 1, wherein each of the first encrypted biometric template and the second encrypted biometric template are encrypted using a public key associated with the first server computer.

8. The method of claim 7, wherein the encrypted match value data file is decrypted using a private key associated with the first server computer.

9. The method of claim 1, further comprising transmitting, by the first server computer, the biometric identifier to the user device.

10. The method of claim 1, further comprising providing an indication to the second server computer as to whether or not the first encrypted biometric template matches the second encrypted biometric template based on the match likelihood value.

11. A server computer comprising:

a processor; and

a non-transitory computer-readable storage medium having code embodied thereon, the code being configured to cause the processor to:

receive authentication data for a user from a user device, the authentication data including user identification data that identifies the user;

determine a biometric identifier, as a random number or string of characters that does not reveal information about the user, to be associated with the authentication data;

store the biometric identifier in association with the user identification data in a database of the server computer;

transmit the biometric identifier to a second server computer along with a first encrypted biometric template associated with the user, the second server computer storing the biometric identifier in association with the first encrypted biometric template;

in response to receiving, from the user device, a biometric identifier request message comprising the user identification data and a request for the biometric identifier, transmit, to the user device, the biometric identifier retrieved from the database based on the user identification data, wherein the second server computer subsequently receives a second encrypted biometric template and the biometric identifier from the user device, identifies the first encrypted biometric template using the biometric identifier, and generates an encrypted match value data file by comparing the first encrypted biometric template and the second encrypted biometric template;

receive the encrypted match value data file;

decrypt the encrypted match value data file to determine a decrypted match value data file; and

determine, from the decrypted match value data file, a match likelihood value.

12. The server computer of claim 11, wherein the second server computer is prevented from accessing plaintext data within the first encrypted biometric template.

13. The server computer of claim 11, wherein the first encrypted biometric template and the second encrypted biometric template are both encrypted using a public key associate with the server computer and using the same encryption technique.

14. The server computer of claim 13, wherein the same encryption technique comprises a homomorphic encryption technique.

15. The server computer of claim 11, wherein the encrypted match value data file comprises an indication of a similarity between the first encrypted biometric template and the second encrypted biometric template.

16. The server computer of claim 15, wherein the decrypted match value data file comprises an indication of a similarity between a first decrypted biometric template and a second decrypted biometric template.

17. The server computer of claim 16, wherein the match likelihood value is determined based on the indication of the similarity between the first decrypted biometric template and the second decrypted biometric template.

18. The server computer of claim 11, wherein the biometric identifier is transmitted to the second server computer via a secure channel.

19. A method comprising:

receiving, at a match server from a service provider computer, a plurality of encrypted enrollment biometric templates and a plurality of biometric identifiers, respectively, wherein the plurality of biometric identifiers correspond to a plurality of users, respectively, each of the plurality of biometric identifiers comprising a random number or string of characters that does not reveal information about a corresponding user and is stored in a database of the service provider computer in association with user identification data identifying a respective user of the plurality of users;

receiving, by the match server from an access device, an encrypted authentication biometric template and a first biometric identifier in a transaction, the encrypted authentication

biometric template and the first biometric identifier corresponding to a first user operating a user device among the plurality of users;

determining, by the match server using the first biometric identifier, an encrypted enrollment biometric template corresponding to the first biometric identifier from the plurality of encrypted enrollment biometric templates;

generating, by the match server, an encrypted match result data file by comparing the encrypted authentication biometric template to the encrypted enrollment biometric template;

transmitting, by the match server to the service provider computer, the encrypted match result data file, wherein the service provider computer decrypts the encrypted match result data file and determines, from a decrypted match value data file, a match result;

receiving, by the match server from the service provider computer, the match result;

determining, by the match server, if the match result exceeds a threshold; and

based on the match result exceeding the threshold, initiating the transaction using account information associated with the first biometric identifier,

wherein, prior to the match server receiving from the access device the encrypted authentication biometric template and the first biometric identifier, the user device sends to the service provider computer a biometric identifier request message comprising first user identification data identifying the first user and a request for the first biometric identifier, obtains the first biometric identifier from the service provider computer based on first user identification data, and sends the first biometric identifier to the access device.

20. A computing device comprising:

a processor; and

a non-transitory computer-readable storage medium having code embodied thereon, the code being configured to cause the processor to:

receive, from a service provider computer, a plurality of encrypted enrollment biometric templates and a plurality of biometric identifiers, respectively, wherein the plurality of biometric identifiers correspond to a plurality of users, respectively, each of the plurality of biometric identifiers comprising a random number or string of characters that does not reveal information about a corresponding user and is stored in a database of the

service provider computer in association with user identification data identifying a respective user of the plurality of users;

receive, from an access device, an encrypted authentication biometric template and a first biometric identifier in a transaction, the encrypted authentication biometric template and the first biometric identifier corresponding to a first user operating a user device among the plurality of users;

determine, using the first biometric identifier, an encrypted enrollment biometric template corresponding to the first biometric identifier from the plurality of encrypted enrollment biometric templates;

generate an encrypted match result data file by comparing the encrypted authentication biometric template to the encrypted enrollment biometric template;

transmit, to the service provider computer, the encrypted match result data file, wherein the service provider computer decrypts the encrypted match result data file and determines, from a decrypted match value data file, a match result;

receive, from the service provider computer, the match result;

determine if the match result exceeds a threshold; and

based on the match result exceeding the threshold, initiate the transaction using account information associated with the first biometric identifier,

wherein, prior to the computing device receiving from the access device the encrypted authentication biometric template and the first biometric identifier, the user device sends to the service provider computer a biometric identifier request message comprising first user identification data identifying the first user and a request for the first biometric identifier, obtains the first biometric identifier from the service provider computer based on first user identification data, and sends the first biometric identifier to the access device.