WHAT IS CLAIMED IS:

1. A method of authenticating a user for a transaction, the method comprising:

receiving, at a server computer, a communication indicative of a communication device associated with the user entering a location within a virtual perimeter;

in response to receiving the communication and prior to receiving biometric data from the user, retrieving, via the server computer, a reference for accessing a biometric data model associated with the user, wherein the biometric data model is stored in a first database;

using the reference, ~~to access~~ retrieving the biometric data model stored in the first database and copying the biometric data model from the first database to a second database associated with the virtual perimeter;

receiving, at the server computer, the biometric data from the user;

retrieving the biometric data model from the second database;

comparing the received biometric data to the biometric data model; and

determining whether the user is authenticated for the transaction based at least in part on comparing the received biometric data to the biometric data model.

~~2. The method of claim 1, wherein the database is a first database, the method further comprising:~~

~~using the reference, copying the biometric data model from the first database to a second database, wherein the biometric data model being compared with the received biometric data is retrieved from the second database.~~

2~~3~~. The method of claim 1, wherein the comparing step further comprises determining a match score based at least in part on the comparison.

3~~4~~. The method of claim 1, wherein the virtual perimeter is established around a merchant location.

4~~5~~. The method of claim 1, wherein the reference is a pointer to a storage address within the first database.

5~~6~~. The method of claim 1, further comprising updating the biometric data model with the received biometric data.

6~~7~~. The method of claim 1, wherein the communication originates from the communication device.

7~~8~~. The method of claim 1, wherein the biometric data model is based on a plurality of biometric data previously received from the user.

8~~9~~. The method of claim 1, further comprising:

calculating a match score based at least in part on comparing the received biometric data to the biometric data model; and

approving or declining the transaction based on the match score.

9~~10~~. The method of claim 1, wherein the biometric data includes one or more of fingerprint data, facial recognition data, or voice data.

10~~11~~. A server computer comprising:

a processor; and

a non-transitory computer-readable storage medium, comprising code executable by the processor for implementing a method for authenticating a user for a transaction, the method comprising:

receiving, at the server computer, a communication indicative of a communication device associated the user entering a location within a virtual perimeter;

in response to receiving the communication and prior to receiving biometric data from the user, retrieving, via the server computer, a reference for accessing a biometric data model associated with the user, wherein the biometric data model is stored in a first database;

using the reference, ~~to access~~ retrieving the biometric data model stored in the first database and copying the biometric data model from the first database to a second database associated with the virtual perimeter;

receiving, at the server computer, the biometric data from the user;

retrieving the biometric data model from the second database;

comparing the received biometric data to the biometric data model; and

determining whether the user is authenticated for the transaction based at least in part on comparing the received biometric data to the biometric data model.

~~12. The server computer of claim 11, wherein the database is a first database, the method further comprising:~~

using the reference, copying the biometric data model from the first database to a second database, wherein the biometric data model being compared with the received biometric data is retrieved from the second database.

11~~13~~. The server computer of claim 10~~11~~, wherein the comparing step further comprises determining a match score based at least in part on the comparison.

12~~14~~. The server computer of claim 10~~11~~, wherein the virtual perimeter is established around a merchant location.

13~~15~~. The server computer of claim 10~~11~~, wherein the reference is a pointer to a storage address within the first database.

14~~16~~. The server computer of claim 10~~11~~, further comprising updating the biometric data model with the received biometric data~~.~~.

15~~17~~. The server computer of claim 10~~11~~, wherein the communication from the communication device.

16~~18~~. The server computer of claim 10~~11~~, wherein the biometric data model is based on a plurality of biometric data previously received from the user.

17~~19~~. The server computer of claim 10~~11~~, further comprising:

calculating a match score based at least in part on comparing the received biometric data to the biometric data model; and

approving or declining the transaction based on the match score.

18~~20~~. The server computer of claim 10~~11~~, wherein the biometric data includes one or more of fingerprint data, facial recognition data, or voice data.