CLAIMS

1. A strong authentication process for an online purchase transaction, comprising:

receiving, by a cloud-based authentication service computer system from a user mobile device, a user authentication request in association with an online purchase transaction, the user authentication request comprising user biometric data, user mobile device identification data comprising at least one of the make of the mobile device and the model number of the mobile device, and purchase transaction data that includes entity identification data of an entity and a transaction amount indicating a type of purchase transaction;

determining, by a mobile transaction application running on the cloud-based authentication service computer system, based on the user biometric data and on at least a portion of the purchase transaction data that the user and the entity involved in the online purchase transaction are both enrolled in a cloud-based authentication service;

identifying, by the mobile transaction application running on the cloud-based authentication service computer system, a user data structure comprising a user profile pre-stored by the cloud-based authentication service computer system, the user profile associated with the entity involved in the online purchase transaction based on the data submitted with the user authentication request;

determining, by the mobile transaction application running on the cloud-based authentication service computer system, that the received user authentication data and user mobile device identification data matches data stored in the user profile;

determining, by the mobile transaction application running on the cloud-based authentication service computer system, that user authentication rules, device authentication rules and business rules of the entity stored in the user profile associated with the type of purchase transaction are satisfied by at least a portion of the data submitted with the user authentication request; and

transmitting, by mobile transaction application running on the cloud-based authentication service computer system to an entity computer, a positive user authentication message indicating authentication of the user and authentication of the user mobile device.

2. The method of claim 1, further comprising, subsequent to receiving the user authentication request:

determining, by a mobile transaction application running on the cloud-based authentication service computer system, that the user involved in the online purchase transaction is not enrolled in a cloud-based authentication service; and

transmitting, by a mobile transaction application, an enrollment message to the user mobile device.

3. The method of claim 1, further comprising, subsequent to receiving the user authentication request:

determining, by a mobile transaction application running on the cloud-based authentication service computer system, that the entity involved in the online purchase transaction is not enrolled in a cloud-based authentication service; and

transmitting, by a mobile transaction application, an enrollment message to an entity computer.

4. The method of claim 1, further comprising, subsequent to identifying the user data structure and the user profile:

determining, by the mobile transaction application, that at least one of the received user authentication data and user mobile device identification data does not match data stored in the user profile; and

transmitting, by the mobile transaction application to an entity computer, a negative user authentication message indicating that at least one of the user and the user mobile device has not been validated.

5. The method of claim 1, further comprising, subsequent to identifying the user profile:

determining, by the mobile transaction application, that at least one requirement of the entity has not been satisfied with regard to the online purchase transaction; and

transmitting, by the mobile transaction application to an entity computer, a negative user authentication message indicating that at least one requirement of the entity has not been satisfied.

6. The method of claim 1, wherein the entity is a merchant.

7. The method of claim 1, wherein the user biometric data comprises at least one of photographic data, facial data, fingerprint data and voice data.

8. A strong authentication system comprising:

at least one user mobile device comprising at least one authenticator; and

a cloud-based computer system in communication with the at least one user mobile device, the cloud-based computer system comprising a cloud-based processor operably connected to a storage device, wherein the storage device includes a mobile transaction application including instructions configured to cause the cloud-based processor to:

receive a user authentication request in association with an online purchase transaction from a user mobile device, the user authentication request comprising user biometric data, user mobile device identification data comprising at least one of the make of the mobile device and the model number of the mobile device, and purchase transaction data that includes entity identification data of an entity and a transaction amount indicating a type of purchase transaction;

determine, based on the user biometric data and on at least a portion of the purchase transaction data, that the user and the entity involved in the online purchase transaction are both enrolled in a cloud-based authentication service;

identify a user data structure comprising a user profile pre-stored by the cloud-based computer system, the user profile associated with the entity involved in the online purchase transaction based on the data submitted with the user authentication request;

determine that the received user authentication data and user mobile device identification data matches data stored in the user profile;

determine that user authentication rules, device authentication rules and business rules of the entity stored in the user profile associated with the type of purchase transaction are satisfied by at least a portion of the data submitted with the user authentication request; and

transmit a positive user authentication message to an entity computer, the positive user authentication message indicating authentication of the user and authentication of the user mobile device.

9. The system of claim 8, wherein the at least one authenticator comprises at least one of a digital camera, a fingerprint reader, a biochemical sensor, and a microphone.

10. The system of claim 8, wherein the mobile transaction application includes, subsequent to the instructions for receiving the user authentication request, further instructions configured to cause the cloud-based processor to:

determine that the user involved in the online purchase transaction is not enrolled in a cloud-based authentication service; and

transmit an enrollment message to the user mobile device.

11. The system of claim 8, wherein the mobile transaction application includes, subsequent to the instructions for receiving the user authentication request, further instructions configured to cause the cloud-based processor to:

determine that the entity involved in the online purchase transaction is not enrolled in a cloud-based authentication service; and

transmit an enrollment message to an entity computer.

12. The system of claim 8, wherein the mobile transaction application includes, subsequent to the instructions for identifying the user data structure and the user profile, further instructions configured to cause the cloud-based processor to:

determine that at least one of the received user authentication data and user mobile device identification data does not match data stored in the user profile; and

transmit a negative user authentication message to an entity computer, the negative authentication message indicating that at least one of the user and the user mobile device has not been validated.

13. The system of claim 8, wherein the mobile transaction application includes, subsequent to the instructions for identifying the user profile, further instructions configured to cause the cloud-based processor to:

determine that at least one requirement of the entity has not been satisfied with regard to the online purchase transaction; and

transmit a negative user authentication message indicating that at least one requirement of the entity has not been satisfied.