CLAIMS

1. A system (100) for authorizing electronic transactions over a network, said system (100) comprising: ~~a data processing and storage unit (102) and at least one computing device (104) co-operating with said data processing and storage unit (102) over a network (118), wherein~~

- ~~said~~ a computing device (104) ~~is~~ associated with at least one user, wherein the user is associated with an identification code, said computing device (104) prompts for an input of at least one ~~authentication code~~ biometric feature from the user and facilitates generation of a notification if ~~authentication code~~ said biometric input is verified and transmits said notification along with said identification code to a data processing and storage unit (102) through a network (118);
- said data processing and storage unit (102) associated with at least one entity (106), wherein said data processing and storage unit (102) includes a processing unit (108) and a repository (110) coupled to said processing unit (108)~~, wherein said processing unit (108)~~ that receives at least one notification and said identification code from a user associated with a computing device (104) for at least one entity and stores said notification in said repository (~~108~~ 110) for the user; and
- said processing unit (108) ~~compares~~ comparing details of an actual transaction with the stored notification in said repository (110) for the user and ~~authorizes~~ authorizing a transaction in the event that said transaction is within the bounds of said notification and sends a confirmation message to the user;

wherein said authentication code biometric input is verified by comparing with a biometric reference that is pre-stored in a memory (114) of the computing device (104) during user registration.

~~2. The system (100) as claimed in claim 1, wherein said authentication code is at least one code selected from the group consisting of a biometric reference, a secret code, a single factor authentication code, and a multifactor authentication code.~~

~~3.~~2. The system (100) as claimed in claim ~~2~~ 1, wherein said biometric feature is selected from the group consisting of a voice print, a fingerprint, a retinal image, an iris image, and a facial image.

~~4.~~3. The system (100) as claimed in claim 1, wherein said notification is a preemption message to notify said entity of a transaction.

~~5.~~4. The system (100) as claimed in claim 1, wherein said notification comprises information including specific / range based values pertaining to a transaction, monetary value / range bound monetary value for a transaction, currency details, credentials and geographical data of entities involved in the transaction, and time-limit associated with said notification.

~~6.~~5. The system (100) as claimed in claim 1, wherein said notification is generated for transactions at events including prior to initiation of a transaction, at initiation of a transaction, during a transaction and before completion of a transaction.

~~7.~~6. The system (100) as claimed in claim 1, wherein said computing device (104) transmits said notification to said data storage and processing unit (102) using communication techniques including Interactive Voice response, Touch Tone response, voice over data, and voice call.

~~8.~~7. The system (100) as claimed in claim 1, wherein said processing unit (108) sends a confirmation of delivery to said computing device (104) upon receiving said notification.

~~9.~~8. The system (100) as claimed in claim 1, wherein said processing unit (108) validates the authenticity of said notification and said identification code before storing in said repository (110).

~~10.~~9. The system (100) as claimed in claim 1, wherein said processing unit (108) updates the status of said notification on completion of an actual transaction, wherein said status includes details selected from the group consisting of the entity against which the notification is used; balance amount available in the notification and expiration details of the notification.

~~11.~~10. The system (100) as claimed in claim 1, wherein said processing unit (108) updates status of said transaction on completion of an actual transaction, wherein said status is selected from the group consisting of hold, cleared and posted.

~~12.~~11. The system (100) as claimed in claim 1, wherein ~~said computing device (104) facilitates registration of a user, wherein~~ said registration includes facilitating selection of at least one account associated with at least one entity; accepting ~~a sample authentication code~~ said biometric reference from the user; ~~prompting the user to select a preferred storage location for said sample authentication code for future verification~~ storing said biometric reference in the memory (114) of said computing device (104); and assigning an identification code to the user~~, wherein said preferred storage location includes in a memory (114) included in said computing device (104), said repository (110) of said data processing and storage unit (102) and a third party storage and verification service accessible to said computing device (104) and said data processing and storage unit (102)~~.

~~13. The system (100) as claimed in claim 1, wherein said computing device (104) verifies said authentication code with a sample stored therein to allow transmission of said notification to said data processing and storage unit (102).~~

~~14. The system (100) as claimed in claim 1, wherein said computing device (104) transmits said authentication code to said data processing and storage unit (102), wherein said repository (110) stores a sample of said authentication code and said processing unit (108) verifies said authentication code with said sample and transmits verification result to said computing device (104).~~

~~15. The system (100) as claimed in claim 1 and 10, wherein said computing device (104) transmits said authentication code to said third party storage and verification service, wherein said third party storage and verification server verifies said authentication code with an authentication code sample stored therein and transmits verification result to said computing device (104).~~

~~16.~~12. The system (100) as claimed in claim 1, wherein said processing unit (108) generates a reverse notification for a user associated with said computing device (104) in the event that no stored notification is retrieved from said repository (110) for an actual transaction.

~~17.~~13. The system (100) as claimed in claim ~~16~~ 12, wherein said processing unit (108) transmits said reverse notification to ~~a~~ said computing device (104) using communication channels selected from the group consisting of short message service (SMS), multimedia messaging service (MMS), direct messaging protocol and Email.

~~18.~~14. The system (100) as claimed in claim ~~17~~ 13, wherein said computing device prompts a user to provide ~~an authentication code~~ a biometric feature for verification to approve a reverse transaction.

~~19.~~15. A computing device (104), said computing device (104) comprising: a processor (112); a memory (114) co-operating with the processor (112) and a data capturing unit (116) co-operating with said memory (114) and said processor (112),
wherein said memory (114) hosting a transaction application that when executed by said processor (112) performs operations including: prompting for an input of at least one ~~authentication code~~ biometric input from a user using said data capturing unit (116); facilitating generation of a notification if ~~authentication code~~ said biometric input is verified; transmitting said notification for authorizing ~~a~~ an actual transaction; and receiving a confirmation and ~~status~~ statuses of the transaction and said notification on completion of ~~an~~ said actual transaction, wherein said notification is a preemption message to notify said entity of ~~a~~ said actual transaction~~.~~;
wherein said biometric input is verified by comparing with a biometric reference stored in said memory (114); and
wherein said biometric reference is further comprising of biometric reference selected from the group consisting of a voice print, a fingerprint, a retinal image, an iris image, and a facial image.

~~20.~~16. The computing device (104) of claim ~~19~~ 15, wherein said processor (112) initiates an interface for said transaction application, wherein said interface is at least for: initiating a

prompt to a user to login to the transaction application; registering at least one account associated with at least one entity with said transaction application; input of at least one ~~authentication code~~ biometric input from the user through said data capturing unit (116); selecting storage preference of said authentication code; capturing at

least one ~~authentication code~~ biometric input from the user via said data capturing unit (116); and verifying said ~~authentication code~~ biometric input to confirm registration.

~~21.~~17. The computing device (104) of claim ~~19~~ 15, wherein said interface is at least for: initiating a prompt to a user for selecting at least one entity for generation of a notification; composing a notification by entering information including credentials and geographical data of the parties involved in the transaction, specific or range based value for the transaction and time-limit associated with the notification; performing ~~authentication code~~ biometric input verification; scrambling and compressing the composed notification for transmission on successful verification of the ~~authentication code~~ biometric input; and displaying a notification delivery confirmation to the user.

~~22.~~18. The computing device (104) of claim ~~19~~ 16, wherein said interface is at least for: checking the status of the notification including if the notification has been received by the entity; the entity against which the notification is used; balance amount available in the notification and expiration details of the notification.

~~23. The computing device (104) of claim 19, wherein said authentication code is at least one code selected from the group consisting of a biometric sample, a secret code, a single factor authentication code, and a multifactor authentication code.~~

~~24.~~19. The computing device (104) of claim ~~19~~ 15, wherein said data capturing unit (116) is at least one device selected from the group consisting of a microphone, a biometric scanner and a biometric sensor.

~~25.~~20. The computing device (104) of claim ~~19~~ 15, wherein said computing device (104) receives a reverse notification for verification of details of an actual transaction, if said notification is not transmitted before said actual transaction.

~~26.~~21. The computing device (104) of claim ~~25~~ 20, wherein said computing device performs ~~authentication code~~ biometric input verification for a user in response to said reverse notification to facilitate a verified user to approve a transaction.

~~27.~~22. A method for authorizing electronic transactions over a network, said method comprising the following steps:

- verifying at least one ~~authentication code~~ biometric input associated with a user;
- facilitating a verified user to generate a notification for conducting a transaction using a computing device;
- transmitting said notification along with an identification code to a data storage and processing unit;
- storing said notification corresponding to said identification code for a validated user in a repository at the data storage and processing unit;
- verifying an actual transaction based on the notification for a user at the data storage and processing unit;
- authorizing said actual transaction in the event that said actual transaction is within the bounds of said notification; and
- sending a confirmation message to the user;

wherein the step of verifying at least one biometric input associated with a user includes accepting a biometric input selected from the group consisting of a voice print, a fingerprint, a retinal image, an iris image, and a facial image, and comparing said biometric input with a biometric reference stored in a memory of said computing device.

~~28. The method as claimed in claim 27, wherein the step of verifying at least one authentication code associated with a user includes accepting an authentication code selected from the group consisting of a biometric sample, a secret code, a single factor authentication code, and a multifactor authentication code.~~

~~29.~~23. The method as claimed in claim ~~27~~ 22, wherein the step of facilitating a verified user to generate a notification includes prompting the verified user to enter credentials and geographical data of parties participating in the transaction; specific or range based value for the transaction; time-limit associated with the notification; and compressing and scrambling the composed notification for transmission.

~~30.~~24. The method as claimed in claim ~~27~~ 22, wherein the step of storing said notification corresponding to said identification code includes sending a delivery receipt confirmation

message back to the computing device for displaying to the corresponding user.

~~31.~~25. The method as claimed in claim ~~27~~ 22, wherein the step of verifying an actual transaction based on the notification includes the following steps:

- comparing the details of the notification with the details of the actual transaction to verify if actual transaction is within the bounds of said notification; and
- marking the notification as used / partly used in the repository and updating the status of the transaction.

~~32.~~26. The method as claimed in claim ~~27~~ 22, wherein the step of verifying an actual transaction includes:

- generating a reverse notification at the data processing and storage unit in the event that no stored notification is retrieved;
- transmitting said reverse notification to a user on the corresponding computing device;
- conducting ~~authentication code~~ biometric input verification for the user; and
- enabling the user to approve a transaction if the ~~authentication code~~ biometric input is verified.

~~33.~~27. The method as claimed in claim ~~27~~ 22, wherein the method includes registration of users for facilitating authorization of transactions, ~~the method~~ said registration comprising the following steps:

- prompting a user to select at least one account associated with at least one entity;
- prompting for input of at least one ~~sample authentication code~~ biometric reference from the user;
- ~~prompting the user to select at least one storage preference of said sample authentication code, wherein said storage preference is selected from the group consisting of in a memory included in the computing device, in the repository of the data processing and storage unit, and a third party storage and verification server accessible to the computing device and the data processing and storage unit.~~ Storing said biometric reference in the memory of said computer device.
- ~~capturing at least one authentication code from the user; and~~

- verifying said authentication code with said sample to confirm registration and assign and identification code to the user.

34. The method as claimed in claim 27 and 33, wherein the step of verifying at least one authentication code associated with a user includes verifying said authentication code with a sample stored in the computing device.

35. The method as claimed in claim 27 and 33, wherein the step of verifying at least one authentication code associated with a user includes verifying said authentication code with a sample stored in the repository of the data processing and storage unit and transmitting the verification result to the computing device.

36. The method as claimed in claim 27 and 33, wherein the step of verifying at least one authentication code associated with a user includes verifying said authentication code with a sample stored in a third party storage and verification server and transmitting the verification result to the computing device.