CLAIMS:

1. An authentication/verification server for authenticating and verifying users of an online service, the authentication/verification server comprising:

a memory storing computer readable instructions; and

processing circuitry configured to execute the computer readable instructions to cause the authentication/verification server to:

receive a network request from a client server associated with the online service in response to a user access attempt of the online service associated with a user, the network request including message recipient information for a mobile-terminated (MT) short message service (SMS) message and a unique one-time password or pin (OTP) code associated with the user,

calculate at least one first signature based on the network request and a shared secret key, the shared secret key being a cryptographic key shared with the client server, the at least one first signature associated with the user,

transmit a network response to the client server, the network response causing the client server to determine a device type of at least one user device associated with the user and transmit a call-to-action (CTA) message to the at least one user device associated with the user based on the determined device type,

determine whether a mobile-originated (MO) SMS message corresponding to the CTA message was received within a desired response time period, and

based on results of the determination of whether the MO SMS message corresponding to the CTA message was received within the desired response time period, determine a status of the user access attempt.

2. The authentication/verification server of claim 1, wherein the user access attempt corresponds to at least one of:

a user account creation attempt on the online service, a user account log-in attempt on the online service, a transaction attempt on the online service, a new user device log-in attempt on the online service, a log-in attempt at a new geographical location, a password reset with the online service, a new support request with the online

service, adding or editing personal account information with the online service, or any combinations thereof.

3. The authentication/verification server of claim 1, wherein the message recipient information includes at least one of:

a mobile phone number associated with the user, a PTSN phone number associated with the user, a virtual phone number associated with the user, a proxy phone number associated with the authentication/verification server, a proxy phone number associated with the client server, or any combinations thereof.

4. The authentication/verification server of claim 1, wherein the authentication/verification server is further caused to:

receive the MO SMS message from the at least one user device via the authentication/verification server, or receive the MO SMS message from the at least one user device via the client server;

determine the status of the user access attempt based on contents of the received MO SMS message, the calculated at least one first signature, and the desired response time period; and

transmit the determined status of the user access attempt to the client server.

5. The authentication/verification server of claim 4, wherein

the MO SMS message includes a second signature; and

the authentication/verification server is further caused to determine the status of the user access attempt by:

determining whether the MO SMS message is received before expiration of the desired response time period,

determining whether the second signature matches at least one of the calculated at least one first signature associated with the user, and

determining whether the matching first signature was calculated during the desired response time period.

6. The authentication/verification server of claim 1, wherein the authentication/verification server is further caused to:

perform a home location register (HLR) lookup on a phone number associated with the at least one user device to determine an International Mobile Subscriber Identity (IMSI) number associated with the phone number;

determine fraud potential information associated with the user access attempt based on the determined IMSI number; and

transmit the determined fraud potential information to the client server.

7. The authentication/verification server of claim 1, wherein

the network response includes at least one communication account identifying information associated with the authentication/verification server or the client server, the at least one communication account identifying information being at least one of:

a local phone number, a national phone number, an international phone number, a toll-free phone number, a mobile phone number, a short code, a long code, a network specific number, or any combinations thereof.

8. The authentication/verification server of claim 1, wherein

the at least one user device includes at least a mobile phone device associated with the user; and

the authentication/verification server is further caused to,

generate the MT SMS message in response to the received network request, the MT SMS message including the OTP code associated with the user and the message recipient information, the message recipient information being a phone number associated with the mobile phone device; and

transmit the MT SMS message to the mobile phone device associated with the user in response to an expiration of the desired response time period or a determined status of the user access attempt indicating failure.

9. The authentication/verification server of claim 8, wherein the authentication/verification server is further caused to:

cancel transmission of the MT SMS message to the mobile phone device in response to the determined status of the user access attempt indicating success prior to the expiration of the desired response time period.

10. The authentication/verification server of claim 1, wherein the authentication/verification server is further caused to calculate the at least one first signature by:

generating a unique keyed-hash using a desired hashing algorithm on at least the OTP code, and the shared secret key.

11. The authentication/verification server of claim 1, wherein

the network request includes a message body; and

the authentication/verification server is further caused to calculate the at least one first signature by:

generating a unique keyed-hash using a desired hashing algorithm on the message body included in the network request and the shared secret key.

12. A client server associated with an online service, the client server comprising:

a memory storing computer readable instructions; and

processing circuitry configured to execute the computer readable instructions to cause the client server to:

receive a user access attempt from a primary user device associated with a user, the user access attempt including at least a phone number associated with the user,

generate a unique one-time password or pin (OTP) code associated with the user,

transmit a network request to an authentication/verification server, the network request including message recipient information for a mobile-terminated (MT) short message service (SMS) message and the OTP code, the network request causing the authentication/verification server to calculate at least one first signature associated with the user based on the network request and a shared secret key, the shared secret key being a cryptographic key shared with the authentication/verification server,

receive a network response from the authentication/verification server,

determine a device type of the primary user device,

generate a call-to-action (CTA) message for the user based on the determined device type, and

transmit the CTA message to the primary user device.

13. The client server of claim 12, wherein the phone number associated with the user is at least one of:

a mobile phone number associated with the user, a PTSN phone number associated with the user, a virtual phone number associated with the user, a proxy phone number associated with the authentication/verification server, a proxy phone number associated with the client server, or any combinations thereof.

14. The client server of claim 12, wherein the transmitting of the CTA message causes the primary user device to display the CTA message to the user for a desired response time period.

15. The client server of claim 14, wherein

the network response includes at least one communication account identifying information associated with the authentication/verification server or the client server;

in response to the device type of the primary user device being a mobile phone device, the CTA message includes a clickable CTA;

in response to the device type of the primary user device being a non-mobile phone device, the CTA message includes a scannable CTA, the scannable CTA being at least one of a barcode or quick response (QR) code; and

the clickable CTA and the scannable CTA are both configured to cause the mobile phone device to automatically compose a mobile-originated (MO) SMS message, the automatically composing the MO SMS message including,

pre-populating a message recipient field of the MO SMS message with the at least one communication account identifying information associated with the authentication/verification server or the client server, and

pre-populating a message body of the MO SMS message with the calculated at least one first signature associated with the user.

16. The client server of claim 15, wherein the client server is further caused to:

receive the MO SMS message from the primary user device or a secondary user device; and

forward the MO SMS message to the authentication/verification server.

17. The client server of claim 15, wherein the client server is further caused to:

receive a user access attempt status message from the authentication/verification server, the user access attempt status message indicating a determined status of the user access attempt.

18. The client server of claim 17, wherein the client server is further caused to:

transmit a message to the primary user device in response to expiration of the desired response time period or the determined status of the user access attempt indicating failure, the message prompting the user to enter the OTP code;

receive a user input from the primary user device; and

determine the user access attempt status based on the received user input and the OTP code associated with the user.

19. The client server of claim 15, wherein the at least one communication account identifying information associated with the authentication/verification server or the client server is at least one of:

a local phone number, a national phone number, an international phone number, a toll-free phone number, a mobile phone number, a short code, a long code, a network specific number, or any combinations thereof.

20. The client server of claim 12, wherein the client server is further caused to:

receive fraud potential information associated with the user access attempt from the authentication/verification server, the fraud potential information determined based on an International Mobile Subscriber Identity (IMSI) number associated with the phone number associated with the user received from a home location register (HLR) lookup performed on the phone number associated with the user; and

determine a user access attempt status based on the received fraud potential information.

21. The client server of claim 12, wherein the user access attempt corresponds to at least one of:

a user account creation attempt on the online service, a user account log-in attempt on the online service, a transaction attempt on the online service, a new user device log-in attempt on the online service, a log-in attempt at a new geographical location, a password reset with the online service, a new support request with the online service, adding or editing personal account information with the online service, or any combinations thereof.

22. A user device associated with a user accessing an online service, the user device comprising:

a memory storing computer readable instructions; and

processing circuitry configured to execute the computer readable instructions to cause the user device to:

transmit a user access attempt to a client server associated with the online service, the user access attempt including at least a phone number associated with the user, the user access attempt causing the client server to,

generate a unique one-time password or pin (OTP) code associated with the user,

transmit a network request to an authentication/verification server, the network request including message recipient information for a mobile-terminated (MT) short message service (SMS) message and the OTP code,

receive a network response from the authentication/verification server in response to the network request, and

determine a device type of the user device,

receive a call-to-action (CTA) message from the client server, the CTA message generated based on the determined device type, and

display the CTA message to the user for a desired response time period.

23. The user device of claim 22, wherein the user device is further caused to:

receive a user input engaging the CTA message;

automatically compose a mobile originated (MO) short message service (SMS) message in response to the user input, the automatically composing the MO SMS message including pre-populating a message recipient field of the MO SMS message with at least one communication account identifying information associated with the

authentication/verification server or associated with the client server, and pre-populating a message body of the MO SMS message with at least one signature associated with the user calculated by the client server;

transmit the MO SMS message to the at least one communication account identifying information associated with the authentication/verification server or the client server; and

receive a user access attempt status message corresponding to the user access attempt from the client server in response to the transmitted MO SMS message.

24. The user device of claim 23, wherein the user device is further caused to:

receive a mobile-terminated (MT) SMS message from the authentication/verification server in response to an expiration of the desired response time period or the user access attempt status message indicating failure of the user access attempt, the MT SMS message prompting the user to enter the unique one-time password or pin (OTP) code;

receive a second user input from the user in response to the MT SMS message; and

transmit a user response message to the client server, the user response message including the second user input.

25. The user device of claim 23, wherein the at least one communication account identifying information associated with the authentication/verification server or the client server is at least one of:

a local phone number, a national phone number, an international phone number, a toll-free phone number, a mobile phone number, a short code, a long code, a network specific number, or any combinations thereof.