CLAIMS

We Claim:

1. A computer-implemented method for performing security protection of association between a user device and a user, comprising:

receiving, by a processor of a computing system, from a service provider through a first communication path between the service provider and the computing system, a notification that an identifier of a user device has been activated in the user device to be associated with a user identifier to replace an existing identifier of the user device associated with the user identifier, wherein the identifier of the user device is a hardware based network identifier including a subscriber identify module (SIM) card or a media access control (MAC) address of the user device, and the user identifier includes a phone number or an email address to identify a user to the service provider, wherein the notification is sent to the computing system to determine whether an attacker is attempting to gain control over the user identifier by transferring the user identifier to another user device under control of the attacker to cause security information related to the user to be sent to that other user device, wherein user authentication via a phone or IoT one-time password (OTP) is not allowed until the user is authenticated as a valid user;

storing, in a storage device coupled to the processor, the user identifier of the user to indicate that the existing identifier of the user device associated with the user identifier has been changed;

receiving, by the processor, from the user device through a second communication path between the user device and the computing system, a request for information associated with the user identifier to be sent to the user device associated with the identifier of the user device;

searching the storage device to look up the user identifier; and

verifying the identifier of the user device has been activated by the user by an additional authentication of the user through a third communication path between the user and the computing system, when the user identifier is found in the storage device, wherein the user authentication via the third communication path protects against an attacker from attempting to use the user device from performing an account take over (ATO) of that user.

2. The computer-implemented method of claim 1, wherein verifying the identifier of the user device has been activated by the user by the additional authentication of the user includes:

sending, to the user through the third communication path between the user and the computing system, a request for authentication information different from the user identifier of the user;

receiving, from the user, a response message to the request for authentication information; and

authenticating the user based on the response message and a set of rules.

3. The computer-implemented method of claim 1, further comprising:

sending, to the user device associated with the identifier of the user device through the second communication path, after verifying the identifier of the user device has been activated by the user is successful, the requested information associated with the user identifier.

4. The computer-implemented method of claim 1, further comprising:

updating the storage to associate the identifier of the user device with the user identifier.

5. The computer-implemented method of claim 1, wherein the request for information associated with the user identifier to be sent to the user device includes a request for one time password (OTP) for the user.

6. The computer-implemented method of claim 1, wherein the request for information associated with the user identifier to be sent to the user device is received through an application software operating on the user device, and the information associated with the user identifier is for operating the application software by the user.

7. The computer-implemented method of claim 1, wherein the user device includes a wireless phone, a cellular phone, a satellite phone, a VoIP phone, a smart

phone, a laptop, a tablet, a personal computer, a point of sale (POS) terminal, a transaction terminal, or a handheld computer.

8. The computer-implemented method of claim 1, wherein the service provider includes a phone service provider or an internet service provider.

9. The computer-implemented method of claim 2, wherein sending to the user the request for authentication information different from the user identifier of the user includes sending the request to the user through the third communication path that is different from the second communication path.

10. The computer-implemented method of claim 2, wherein the authentication information includes information the user knows, information the user has, information about what the user is, information about where the user is, or information about what the user does.

11. The computer-implemented method of claim 2, wherein the set of rules for authenticating the user based on the response message includes a rule about a limit on a number of requests for information associated with the user identifier to be sent to the user device associated with the identifier of the user device, a rule about a limit on a number of identifiers of user devices associated with the user identifier, a rule about a limit on a number of user identifiers associated with the identifier of the user device, a rule about a restriction on providers of the user devices, or a rule providing an authentication scheme corresponding to the identifier of the user device.

12. A computing system for performing security protection of association between a user device and a user, comprising:

one or more processors configured to receive from a service provider through a first communication path between the service provider and the computing system, a notification that an identifier of the user device has been activated in the user device to be associated with a user identifier and to replace an existing identifier of the user device associated with the user identifier, wherein the identifier of the user device is a hardware based network identifier including a subscriber identity module

(SIM) card or a media access control (MAC) address of the user device, and the user identifier includes a phone number or an email address to identify the user by the service provider, wherein the notification is sent to the computing system to determine whether an attacker is attempting to gain control over the user identifier by transferring the user identifier to another user device under control of the attacker to cause security information related to the user to be sent to that other user device, wherein user authentication via a phone or IoT one-time password (OTP) is not allowed until the user is authenticated as a valid user;

a storage device coupled to the one or more processors, wherein the storage device is configured to store the user identifier of the user to indicate that the existing identifier of the user device associated with the user identifier has been changed;

an application software to be operated by the one or more processors, wherein the application software is to receive from the user device through a second communication path between the user device and the computing system, a request for information associated with the user identifier to be sent to the user device associated with the identifier of the user device, and the information associated with the user identifier is for operating the application software by the user; and

an authentication module to be operated by the one or more processors, wherein the authentication module is to:

search the storage device to look up the user identifier;

send, to the user through a third communication path between the user and the computing system, when the user identifier is found in the storage device, a request for authentication information different from the user identifier of the user;

receive, from the user, a response message to the request for authentication information; and

authenticate the user based on the response message and a set of rules, wherein the user authentication via the third communication path protects against an attacker from attempting to use the user device from performing an account take over (ATO) of that user.

13. The computing system of claim 12, wherein the application software is further to send, to the user device associated with the identifier of the user device through the second communication path, after authenticating the user based on the

response message is successful, the requested information associated with the user identifier.

14. The computing system of claim 12, wherein the authentication module is further to update the storage to associate the identifier of the user device with the user identifier.

15. The computing system of claim 12, wherein the third communication path is different from the second communication path.

16. The computing system of claim 12, wherein the request for information associated with the user identifier to be sent to the user device includes a request for one time password (OTP) for the user.

17. An executable software product stored on a non-transitory computer-readable medium containing program instructions that cause a processor of a computing system to perform security protection of association between a user device and a user, in response to execution of the instructions by the processor, to:

receive, from a service provider through a first communication path between the service provider and the computing system, a notification that an identifier of a user device has been activated in the user device to be associated with a user identifier and to replace an existing identifier of the user device associated with the user identifier, wherein the identifier of the user device is a hardware based network identifier including a subscriber identity module (SIM) card or a media access control (MAC) address of the user device, and the user identifier includes a phone number or an email address to identify the user to the service provider, wherein the notification is sent to the computing system to determine whether an attacker is attempting to gain control over the user identifier by transferring the user identifier to another user device under control of the attacker to cause security information related to the user to be sent to that other user device, wherein user authentication via a phone or IoT one-time password (OTP) is not allowed until the user is authenticated as a valid user;

store, in a storage device coupled to the processor, the user identifier of the user to indicate that the existing identifier of the user device associated with the user identifier has been changed;

receive, by the processor, from the user device through a second communication path between the user device and the computing system, a request for information associated with the user identifier to be sent to the user device associated with the identifier of the user device;

search the storage device to look up the user identifier;

send, to the user through a third communication path between the user and the computing system, when the user identifier is found in the storage device, a request for authentication information different from the user identifier of the user;

receive, from the user, a response message to the request for authentication information; and

authenticate the user based on the response message and a set of rules, wherein the user authentication via the third communication path protects against an attacker from attempting to use the user device from performing an account take over (ATO) of that user.

18. The executable software product of claim 17, wherein the program instructions further cause the processor to:

send, to the user device associated with the identifier of the user device through the second communication path, after authenticating the user based on the response message is successful, the requested information associated with the user identifier; and

update the storage to associate the identifier of the user device with the user identifier.

19. The executable software product of claim 17, wherein the third communication path is different from the second communication path, and

the request for information associated with the user identifier to be sent to the user device includes a request for one time password (OTP) for the user.