CLAIMS

What is claimed is:

1. A system for authenticating a user associated with a plurality of user devices using a plurality of types of authentication information, the system comprising: an electronic computing device including an electronic processor, the electronic processor configured to:

receive, from a user device executing an application, a request to access sensitive information, wherein the user device is associated with a user profile;

send, to the user device, a request for a first accuracy measurement for a first type of authentication information;

upon receipt of the first accuracy measurement, determine whether the first accuracy measurement indicates that the accuracy of the first type of authentication information is below a predetermined threshold associated with the user device;

when the accuracy of the first type of authentication information is below the predetermined threshold, send to the user device a request for a second accuracy measurement for a second type of authentication information;

upon receipt of the second accuracy measurement, determine whether the second accuracy measurement indicates that the accuracy of the second type of authentication information is above or equal to the predetermined threshold associated with the user device; and

when the accuracy of the second type of authentication information is above or equal to the predetermined threshold, authenticate the user and lower the predetermined threshold for each user device associated with the user profile.

2. The system according to claim 1, wherein the electronic processor is further configured to:

record, for the user profile, an anomaly associated with the first type of the authentication information;

receive, from a second user device associated with the user profile, a request to access sensitive information subsequent to recording the anomaly; and

send, to the second user device, a request for a third accuracy measurement for a type of authentication information different than the first type of authentication information.

3. The system according to claim 1, the electronic processor further configured to:

subsequent to lowering the predetermined threshold for each user device associated with the user profile, receive, from a second user device associated with the user profile, a request to access sensitive information;

send, to the second user device, a request for a third accuracy measurement for the first type of authentication information, the second type of authentication information, or other type of authentication information; and

when the third accuracy measurement is above or equal to the predetermined threshold, authenticate the user.

4. The system according to claim 1, wherein the authentication information is one selected from the group consisting of a biometric identifier, public key infrastructure certificate, a one-time password, and a username and password.

5. The system according to claim 1, wherein the electronic processor is further configured to:

revert the lowered predetermined threshold for each user device associated with the user profile to the predetermined threshold, after a predetermined amount of time has passed.

6. The system according to claim 1, wherein a memory of the electronic computing device includes a mapping of a plurality of applications to types of authentication information and each of the plurality of applications is mapped to one or more types of authentication information that the application accepts as authentication for the user.

7. The system according to claim 1, wherein the electronic processor is further configured to:

receive a request to add a second user device to the user profile; and

in response to receiving the request to add a second user device to the user profile, store, in the user profile included in a memory of the electronic computing device, a unique identifier for the second user device, types of authentication information accepted by the second user device, and a predetermined threshold associated with the second user device.

8. The system according to claim 7, wherein the request to add the second user device to the user profile is received when an application allowing access to sensitive information associated with the user is installed in the second user device.

9. A method of authenticating a user associated with a plurality of user devices using a plurality of types of authentication information, the method comprising:

generating, with a user device, a request to access sensitive information, wherein the user device is associated with a user profile;

requesting, with the user device, a first type of authentication information;

upon receipt of the first type of authentication information, determining whether the accuracy of the first type of authentication information is below a predetermined threshold associated with the user device;

when the accuracy of the first type of authentication information is above or equal to the predetermined threshold, authenticating, with the user device, the user and sending, to an electronic computing device, a notification of successful authentication;

when the accuracy of the first type of authentication information is below the predetermined threshold, requesting, with the user device, a second type of authentication information;

upon receipt of the second type of authentication information, determining whether the accuracy of the second type of authentication information is above or equal to the predetermined threshold associated with the user device;

when the accuracy of the second type of authentication information is above or equal to the predetermined threshold, authenticating, with the user device, the user and sending, to the electronic computing device, a notification of successful authentication and an unsuccessful authentication attempt using the first type of authentication information; and

upon receipt by the electronic computing device of a notification of successful authentication, for each of the plurality of user devices associated with the user profile, lower the predetermined threshold.

10. The method according to claim 9, the method further comprising:

generating, with a second user device associated with the user profile, a request to access sensitive information subsequent to receiving the lowered predetermined threshold from the electronic computing device;

requesting, with the second user device, the first type of authentication information or another type of authentication information; and

when the accuracy of the first type of authentication information or another type of authentication information is above or equal to the predetermined threshold, authenticating, with the second user device, the user.

11. The method according to claim 9, the method further comprising:

when the accuracy of the second type of authentication information is above or equal to the predetermined threshold, recording, with the electronic computing device, an anomaly associated with the first type of the authentication information; and

sending, with the electronic computing device, a notification of the anomaly associated with the first type of authentication information to each of the plurality of user devices associated with the user profile.

12. The method according to claim 11, the method further comprising:

generating, with a second user device associated with the user profile, a request to access sensitive information subsequent to receiving the notification of the anomaly associated with the first type of authentication information; and

requesting, with the second user device, a type of authentication information different than the first type of authentication information.

13. The method according to claim 9, the method further comprising:

reverting the lowered predetermined threshold for each of the plurality of user devices associated with the user profile to the predetermined threshold, after a predetermined amount of time has passed.

14. The method according to claim 9, the method further comprising:

receiving, with the electronic computing device, a request to add a second user device to the user profile; and

in response to receiving the request to add a second user device to the user profile, storing, in the user profile included in a memory of the electronic computing device, a unique identifier for the second user device, types of authentication information accepted by the second user device, and a predetermined threshold associated with the second user device.

15. A non-transitory computer-readable medium with computer-executable instructions stored thereon executed by an electronic processor to perform the method of authenticating a user associated with a plurality of user devices using a plurality of types of authentication information, comprising:

receiving, from a user device executing an application, a request to access sensitive information wherein the user device is associated with a user profile;

sending, to the user device, a request for a first type of authentication information;

upon receipt of the first accuracy measurement the first type of authentication information, determining a first accuracy measurement for the first type of authentication information;

determining whether the first accuracy measurement indicates that the accuracy of the first type of authentication information is below a predetermined threshold associated with the user device;

when the accuracy of the first type of authentication information is below the predetermined threshold, sending to the user device a request for a second accuracy measurement for a second type of authentication information;

upon receipt of the second accuracy measurement, determining whether the second accuracy measurement indicates that the accuracy of the second type of authentication information is above or equal to the predetermined threshold associated with the user device;

when the accuracy of the second type of authentication information is above or equal to the predetermined threshold, authenticating the user and lowering the predetermined threshold for each user device associated with the user profile.

16. The non-transitory computer-readable medium according to claim 15, the method further comprising:

recording, for the user profile, an anomaly for the first type of authentication information;

receiving, from a second user device associated with the user profile, a request to access sensitive information subsequent to recording the anomaly; and

sending to the second user device a request for a type of authentication information different than the first type of authentication information.

17. The non-transitory computer-readable medium according to claim 15, the method further comprising:

subsequent to lowering the predetermined threshold associated with the user device, receiving, from a second user device associated with the user profile, a request to access sensitive information;

sending to the second user device a request for a third accuracy measurement for the first type of authentication information, the second type of authentication information, or another type of authentication information;

determining a third accuracy measurement for the first type of authentication information, second type of authentication type of authentication information, or other type of authentication information;

determining whether the third accuracy measurement is above or equal to the lowered predetermined threshold associated with the second user device; and

when the third accuracy measurement of the first type of authentication information is above or equal to the predetermined threshold, authenticating the user.

18. The non-transitory computer-readable medium according to claim 15, the method further comprising:

reverting the lowered predetermined threshold for each user device associated with the user profile to the predetermined threshold, after a predetermined amount of time has passed.

19. The non-transitory computer-readable medium according to claim 15, the method further comprising:

receiving a request to add a second user device to the user profile; and

in response to receiving the request to add a second user device to the user profile, storing, in the user profile included in a memory of the electronic computing device, a unique identifier for the second user device, types of authentication information accepted by the second user device, and a predetermined threshold associated with the second user device.

20. The non-transitory computer-readable medium according to claim 15, wherein the predetermined threshold is a value, the first type of authentication information is a facial image, and the second type of authentication information is an audio clip of a voice.