CLAIMS

WHAT IS CLAIMED IS:

1. A user device system comprising:

a biometric capture device;

a non-transitory memory; and

one or more hardware processors coupled to the non-transitory memory and configured to read instructions from the non-transitory memory to cause the user device system to perform operations comprising:

receiving image data of a fingerprint captured by the biometric capture device;

detecting, at a time of capture of the image data, an increased heart rate of a user associated with the user device system using one of the biometric capture device of the user device system or an additional biometric device wirelessly connected to the user device system;

determining fingerprint input data of the fingerprint that comprises an orientation of the fingerprint and a length of time the fingerprint is on the user device system using at least in part the image data;

determining an electronic transaction processed using an account associated with the user device system through an application of the user device system;

determining, based on the increased heart rate and the fingerprint input data of the fingerprint, whether to display a balance and a financial information for the account on a user interface associated with displaying the electronic transaction through the application;

determining an interface display configuration for the user interface displayed by the user device system based on the determining whether to display the balance and the financial information;

outputting the user interface based on the interface display configuration;

detecting a computing action associated with the balance and the financial information that is executed in the application using the user interface;

determining that the computing action indicates fraud based on the increased heart rate and the fingerprint input data; and

marking the computing action for reversal based on the determining that the computing action indicates fraud.

2. The user device system of claim 1, wherein prior to determining the interface display configuration, the operations further comprise:

determining that the orientation of the fingerprint is within a range of orientations,

wherein the interface display configuration provides full data access to the balance and the financial information through the user interface based on the determination that the orientation is within the range.

3. The user device system of claim 1, wherein prior to determining the interface display configuration, the operations further comprise:

determining that the orientation of the fingerprint is outside of a range of orientations,

wherein the interface display configuration provides partial data access to the balance and the financial information through the user interface based on the determination that the orientation is outside the range.

4. The user device system of claim 1, wherein prior to determining the interface display configuration, the operations further comprise:

determining that the orientation of the fingerprint is within a range of orientations,

wherein the interface display configuration prevents access to the balance and the financial information through the user interface based on the determination that the orientation is within the range.

5. The user device system of claim 4, wherein the user device system is associated with a second user device system, and wherein the operations further comprise:

transmitting an alert to the second user device system based on the orientation of the fingerprint being within the range.

6. The user device system of claim 1, wherein prior to the determining the interface display configuration, the operations further comprise:

connecting to a wearable computing device associated with the user of the user device system; and

determining user data for the user using the wearable computing device,

wherein the interface display configuration is further determined based on the user data.

7. The user device system of claim 1, wherein prior to the determining the interface display configuration, the operations further comprise:

determining a pressure of the fingerprint applied to the biometric capture device,

wherein the interface display configuration is further determined based on the pressure.

8. The user device system of claim 1, wherein prior to determining the orientation of the fingerprint, the operations further comprise:

generating a map of the fingerprint using the image data; and

comparing the map of the fingerprint to stored fingerprint data associated with the user of the user device system,

wherein the orientation is determined based on the comparing.

9. The user device system of claim 8, wherein the map of the fingerprint comprises curvature information of ridges and grooves of the fingerprint, and wherein the orientation is determined based on the curvature information.

10. The user device system of claim 1, wherein prior to the determining the interface display configuration, the operations further comprise:

detecting voice data using a microphone of the user device system,

wherein the interface display configuration is further determined based on the voice data.

11. The user device system of claim 10, wherein the voice data comprises a voice command, and wherein the determining the interface display configuration comprises:

identifying a requested action for the interface display configuration based on the voice command,

wherein the user interface is output based on the requested action.

12. The user device system of claim 1, wherein the biometric capture device comprises one of a home screen button having an image capture device, a touch screen interface of the user device system, or an ultrasonic capture device.

13. A method comprising:

receiving, by a device, an access request to access an application on the device;

in response to receiving the access request, capturing a first image of a first fingerprint using an input component of the device;

detecting, at a time of the capturing the first image, an increased heart rate of a user associated with the device using one of the input component of the device or a biometric device wirelessly connected to the device;

determining fingerprint input data of the first fingerprint that comprises a placement of the first fingerprint on the input component based on the first image and a length of time of the first fingerprint on the input component;

determining an electronic transaction processed using an account associated with the device through the application of the device;

determining, based on the increased heart rate and the fingerprint input data of the first fingerprint, whether to display a balance and a financial information for the account on a user interface associated with displaying the electronic transaction through the application;

determining data accessibility within the application based on the determining whether to display the balance and the financial information;

outputting data within the application based on the data accessibility and the user interface;

detecting a computing action associated with the balance and the financial information that is executed in the application using the user interface;

determining that the computing action indicates fraud based on the increased heart rate and the fingerprint input data; and

marking the computing action for reversal based on the determining that the computing action indicates fraud.

14. The method of claim 13, wherein the data within the application comprises false application data, and wherein the computing action comprises a request to process the electronic transaction within the application, and wherein the method further comprises:

alerting an entity associated with the application.

15. The method of claim 13, further comprising:

capturing a second image of a second fingerprint on the device within a predetermined time of capturing the first image;

determining that the second fingerprint is unknown to the device; and

locking at least one of the application or the device based on the determining that the second fingerprint is unknown.

16. The method of claim 13, wherein prior to determining the data accessibility, the method further comprises:

in response to detecting the first fingerprint, activating at least one of an additional device component of the device or a connected device to the device; and

capturing additional data associated with the device using the at least one of the additional device component or the connected device,

wherein the data accessibility is further determined based on the additional data.

17. The method of claim 16, wherein the additional data comprises at least one of a location of the device, an image, voice data, a pressure applied to the device, or a perspiration amount of the user, and wherein the additional device component or the connected device comprises a GPS locator, a camera, a microphone, a pressure sensor, a touch screen interface, or a wearable computing device.

18. A non-transitory machine-readable medium having stored thereon machine-readable instructions executable to cause a machine to perform operations comprising:

receiving, by a mobile phone device, an unlock request to unlock the mobile phone device;

capturing fingerprint data with the unlock request using a biometric input component of the mobile phone device;

detecting, at a time of the capturing the fingerprint data, an increased heart rate of a user associated with the mobile phone device using one of the biometric input component of the mobile phone device or a biometric device wirelessly connected to the mobile phone device;

determining fingerprint input data of the fingerprint that comprises an orientation of the fingerprint and a length of time of the fingerprint on the mobile phone device during the unlock request based at least in part on the fingerprint data;

determining an electronic transaction processed using an account associated with the mobile phone device through an application of the mobile phone device;

determining, based on the increased heart rate and the fingerprint input data of the fingerprint, whether to display a balance and a financial information for the account on a user interface associated with displaying the electronic transaction through the application;

outputting content on the mobile phone device based on the determining whether to display the balance and the financial information;

detecting a computing action associated with the balance and the financial information that is executed in the application using the user interface;

determining that the computing action indicates fraud based on the increased heart rate and the fingerprint input data; and

marking the computing action for reversal based on the determining that the computing action indicates fraud.

19. The non-transitory machine-readable medium of claim 18, wherein the operations further comprise:

determining a first device within a first distance from the mobile phone device; and

transmitting a communication to the first device based on the computing action.

20. The non-transitory machine-readable medium of claim 19, wherein the first device comprises one of a plurality of devices associated with a group of users designated by a user of the mobile phone device or by a service provider associated with the mobile phone device.