What is claimed is:

1. A non-transitory computer-readable medium storing instructions that, when executed by a processor, cause the processor to:

receive a request from a validation server, the request associated with a user account associated with a user;

perform a first validation action by authenticating, on a computing device, an identity of the user;

perform a second validation action by receiving, via a short-range communication protocol, a scan of a code from a physical token;

based on the first validation action and the second validation action, generating a validation response package identifying the user and the code retrieved from the physical token; and

transmitting the response package to the validation server.

2. The medium of claim 1, wherein the short-range communication protocol is a near field communication (NFC) protocol.

3. The medium of claim 1, wherein the code is a counter stored on the physical token that is incremented each time the code is read from the physical token.

4. The medium of claim 1, wherein the physical token is computing hardware physically incorporated into a credit card.

5. The medium of claim 1, wherein authenticating the identity of the user comprises logging the user into the user account on an application running on the computing device.

6. The medium of claim 1, further storing instructions for:

receiving an escalated validation request in response to transmitting the response package; receiving a photograph from a camera of the computing device; and generating a response to the escalated validation request, the response including the photograph.

7. The medium of claim 6, wherein the escalated validation request is a request for a photograph of identification associated with the user.

8. A method comprising:

receiving a request to confirm an intent of a user to execute a transaction associated with a service; receiving a cumulative value from a physical token associated with the user;

accessing a log, the log mapping users of the service to last-known values of respective physical tokens of the users;

retrieving, from the log, the last-known value of the physical token associated with the user;

identifying a window of acceptable values around the last-known value of the physical token;

determining that the cumulative value received from the physical token is within the window of acceptable values; and

causing the transaction to be executed when the cumulative value is within the window.

9. The method of claim 8, wherein the physical token is credit card.

10. The method of claim 8, wherein the window is a single value.

11. The method of claim 8, wherein the window is a range of values

12. The method of claim 11, wherein the range is a dynamic range, and further comprising modifying the window based on user profile information that indicates an estimated rate at which the cumulative value is unintentionally incremented.

13. The method of claim 8, further comprising computing a risk value associated with the transaction.

14. The method of claim 13, wherein a size of the window varies according to the risk value.

15. A system comprising:

A validation server configured to transmit a request to authenticate a user associated with a user account; and

a client device configured to receive information derived from a scan of a code from a physical token, wherein

the validation server is further configured to authenticate the information, the authenticating comprising comparing the code received from the physical token to a corresponding code stored at the validation server, wherein the authenticating is performed at least in part based on a risk assessment.

16. The apparatus of claim 15, wherein the authenticating comprises failing an initial authentication procedure and transmitting a request for further authentication.

17. The apparatus of claim 16, wherein the validation server is further configured to determine that the further authentication has failed, and increase a level of risk associated with the risk assessment in response to the failure.

18. The apparatus of claim 16, wherein the validation server is further configured to determine that the further authentication has succeeded, and maintain or decrease a level of risk associated with the risk assessment in response to the success.

19. The apparatus of claim 15, wherein the authenticating comprises passing an initial authentication procedure and decreasing a level of risk associated with the risk assessment in response to the success.

~~20. The apparatus of claim 15, wherein the validation server is further configured to determine adjust the risk assessment based on information determined during the authenticating.~~

1. A non-transitory computer-readable medium storing instructions that, when executed by a processor, cause the processor to:

receive, by a computing device, a request from a validation server, the request associated with a user account associated with a user;

perform a first validation action by authenticating a username and password of the user to gain access to an application on the computing device, on a computing device, an identity of the user;

perform, by the application on the computing device, a second validation action, wherein the second validation action comprises ~~by~~ receiving, via a short-range communication protocol, a code from a contactless card;

generate, by the application on the computing device, a validation response package identifying the user and the code retrieved from the physical token; and

communicate, by the application on the computing device, the response package to the validation server.

2. The medium of claim 1, wherein the short-range communication protocol is a near field communication (NFC) protocol.

3. The medium of claim 1, wherein the code is a counter stored on the physical token that is incremented each time the code is read from the contactless card.

4. The medium of claim 1, wherein the contactless card comprising, a debit card, a rewards card, or a credit card.

5. The medium of claim 1, further storing instructions to cause the processor to receive and process an escalated validation request, the escalated validation request comprising a requested validation action.

6. The medium of claim 5, wherein the requested validation action comprises a request to provide a security question, and the medium further storing instructions to cause the processor to:

present, via the application and on a display of the computing device, the security question;

receive, by the application, a response to the security question; and

communicate, by the application, the response to the validation server.

7. The medium of claim 5, wherein the requested validation action comprises a request to provide a biometric input, and the medium further storing instructions to cause the processor to:

receive, by the application and via a biometric device of the computing device, the biometric input; and

communicate, by the application, the biometric input to the validation server.

8. The medium of claim 5, wherein the requested validation action comprises a request to provide a photograph, and the medium further storing instructions to cause the processor to:

receive, by the application, the photograph from a camera of the computing device;

generate, by the application, a response to the escalated validation request, the response including the photograph; and

communicate, by the application, the response to the validation server.

9. The medium of claim 8, wherein the photograph is a picture of an identification associated with the user.

10. A computer-implemented method, comprising:

processing, by a computing device, a request from a validation server, the request associated with a user account associated with a user;

performing, by the computing device, a first validation action on the computing device, the first validation action comprising validating a username and a password associated with the user to access an application, and executing the application in response to validating the username and the password;

performing, by the application on the computing device, a second validation action, the second validation action comprising presenting a prompt to provide a physical token within a short-range communication range of the computing device, and receiving a code from the physical token based on a short-range communication protocol;

generating, by the application on ~~by~~ the computing device, a validation response package identifying the user and the code receiving from the physical token; and

sending, by the application on the computing device, the response package to the validation server.

11. The computer-implemented method of claim 10, wherein the code is a counter stored on the physical token that is incremented each time the code is read from the physical token.

12. The computer-implemented method of claim 10, comprising receiving an escalated validation request, the escalated validation request comprising a requested validation action.

13. The computer-implemented method of claim 12 wherein the requested validation action comprises a request to provide a security question, and the method comprising:

presenting, by the application on a display of the computing device, the security question;

receiving, by the application, a response to the security question; and

sending, by the application, the response to the validation server.

14. The computer-implemented method of claim 12 claim 13, wherein the requested validation action comprises a request to provide a biometric input, and the method comprising:

receiving, by the application via a biometric device of the computing device, the biometric input; and

transmitting, by the application, the biometric input to the validation server.

15. The computer-implemented method of claim 12 claim 13, wherein the requested validation action comprises a request to provide a photograph, and the method comprising:

receiving, by the application, the photograph from a camera of the computing device;

generating, by the application, a response to the escalated validation request, the response including the photograph; and

transmit by the application, the response to the validation server.

16. An apparatus, comprising:

a memory storing instructions for one or more applications; and

a hardware processor circuit configured to execute the instructions to:

receive, by a first application of the one or more applications, a request from a validation server, the request associated with a user account associated with a user;

perform, by the first application of the one or more applications a first validation action on a computing device based on an identity of the user, the first validation action comprising the processor to validate a username and a password of the user to continue to execute the first application;

perform, by the first application, a second validation action by presenting a prompt to provide a physical token within a short-range communication range of the computing device, and scanning a code from the physical token based on a short-range communication protocol;

generate, by the first application, a validation response package identifying the user and the code retrieved from the physical token; and

send, by the first application, the response package to the validation server.

17. The apparatus of claim 16, the processor to:

receive an escalated validation request to answer a security question;

present, on a display, the security question;

receive a response to the security question; and

send the response to the validation server.

18. The apparatus of claim 16, the processor to:

receive an escalated validation request to provide a biometric input;

receive, via a biometric device, the biometric input; and

send the biometric input to the validation server.

19. The apparatus of claim 16, the processor to:

receive an escalated validation request to provide a photograph;

receive the photograph from a camera;

generate a response to the escalated validation request, the response including the photograph; and

send the response to the validation server.