WHAT IS CLAIMED IS:

1. A method comprising:

prompting, by an access device, a user to enter an access code, the access code determined by a validation computer, the access code associated with an account number corresponding to a user device associated with the user, the validation computer configured to determine an expiration time period for the access code, the expiration time period of a certain length based on one or more policies, the one or more policies including one or more of a number of access code requests previously transmitted by the user device compared to a certain time period, a location of the user device, or a threshold period, the validation computer transmitting the access code and the expiration time period for the access code to the user device upon receiving a request for the access code from the user device;

receiving, by the access device, the access code from the user;

transmitting, by the access device, the access code to the ~~a~~ validation computer, that ~~which~~ validates the access code and the expiration time period for the access code;

receiving, by the access device, an access identifier or access token from the validation computer in response to validating the access code;

transmitting, by the access device, an authorization request message including the access identifier or the access token to an authorizing computer; and

receiving, by the access device, an authorization response message from the authorizing computer.

2. The method of claim 1, wherein the access device is an ATM.

3. The method of claim 1, further comprising, after receiving the access identifier or the access token: prompting, by the access device, the user for a personal identifier comprising a PIN.

4. The method of claim 3, wherein the authorization request message includes the access identifier or the access token and the personal identifier.

5. The method of claim 1, further comprising:

generating a notification indicating a result of authorization by the authorizing computer; and

transmitting the notification to a user device associated with the user.

~~6. The method of claim 5, wherein the notification includes the access code and a geographic location of the access device associated with the authorization.~~

6~~7~~. The method of claim 1, wherein the authorizing computer maintains information including an account number associated with the user, a type

of transaction, a monetary amount of the transaction, and a personal identifier of the user.

78. An access device comprising:

a processor;

a wireless communication device coupled to the processor; and

a memory element including instructions that, when executed with the processor, cause the system to at least:

prompt a user for an access code, the access code determined by a validation computer, the access code associated with an account number corresponding to a user device associated with the user, the validation computer configured to determine an expiration time period for the access code, the expiration time period of a certain length based on one or more policies, the one or more policies including one or more of a number of access code requests previously transmitted by the user device compared to a certain time period, a location of the user device, or a threshold period, the validation computer transmitting the access code and the expiration time period for the access code to the user device upon receiving a request for the access code from the user device;

receive the access code from the user;

transmit the access code to the validation computer that validates the access code and the expiration time period for the access code for validation;

receive an access identifier or access token in response to validating the access code by the validation computer;

transmit an authorization request message including the access identifier or the access token to an authorizing computer; and

receive, from the authorizing computer, an authorization response message.

89. The access device of claim 78, wherein the instructions when executed with the processor further cause the system to at least after receiving the access identifier or the access token: prompting, by the access device, the user for a personal identifier comprising a PIN.

9~~10~~. A computer-implemented method comprising:

receiving, by a validation computer and from a first user device, a request for an access code;

determining, by the validation computer, the access code associated with an account number corresponding to the first user device;

determining, by the validation computer, an expiration time period for the access code, the expiration time period of a certain length based on one or more policies, the one or more policies including one or more of a number of access code requests previously transmitted by the first user device compared to a certain time period, a location of the first user device, or a threshold period;

transmitting, by the validation computer, the access code and the expiration time period for the access code to the first user device;

receiving, by the validation computer and from an access device, the access code;

validating, by the validation computer, the access code based at least in part on the access code associated with the request and the expiration time period for the access code;

generating, by the validation computer, a message that includes the account number associated with the access code in accordance with a determination that the access code is validated, the validation computer maintaining information that identifies a delivery channel preference for the access code, the delivery channel preferences specified by a user associated with the first user device and including an email or an application push notification; and

transmitting, by the validation computer, the message to the access device using the delivery channel preference.

~~11. The computer-implemented method of claim 10, wherein determining the access code further includes determining an expiration time period associated with the access code.~~

1012. The computer-implemented method of claim 911, wherein the expiration time period is specified by the a user associated with the first user device.

~~13. The computer-implemented method of claim 11, wherein the expiration time period is transmitted with the access code to the first user device in response to the request for the access code.~~

1114. The computer-implemented method of claim 910, further comprising determining one or more geographic locations for access devices that are configured to utilize the access code.

1215. The computer-implemented method of claim 1114, further comprising updating a user interface of the first user device to display the one or more geographic locations for the access devices in response to the request for the access code.

1316. The computer-implemented method of claim 910, wherein determining the access code associated with the account number is in response to the a user authenticating with the first user device prior to requesting the access code.

~~17. The computer-implemented method of claim 10, wherein the validating computer maintains information that identifies a delivery channel preference for the access code.~~

14~~18~~. The computer-implemented method of claim 9~~10~~, wherein the validation computer and the access device communicate by invoking an application

programming interface call that uses mutual secure socket layer authentication and channel encryption.

1519. The computer-implemented method of claim 910, further comprising:

receiving, by the validation computer, the access code from a second user device;

validating, by the validation computer, the access code based at least in part on the access code associated with the request;

generating, by the validation computer, the a message that includes the account number associated with the access code in accordance with a determination that the access code is validated; and

transmitting, by the validation computer, the message to the access device.

1620. The computer-implemented method of claim 1519, further comprising:

generating, by the validation computer, a notification indicating that the access code has been used by the second user device; and

transmitting, by the validation computer, the notification to the first user device.