Claims

1. A computer-implemented method for cardless use of an automated teller machine (ATM) by a user, the method implemented using a computer system comprising a server, the server including at least one processor in communication with a database, the database storing a user profile of the user and stored ATM information, the stored ATM information identifying a plurality of ATMs, the method comprising:

receiving, by the server from a user device of the user, a request to log on to a computer application, the request including at least one security feature submitted by the user;

granting, by the server, access by the user device to the computer application in response to verifying that the submitted at least one security feature matches at least one profile security feature stored in the user profile;

receiving, by the server, ATM information submitted by the user device via the computer application, the ATM information identifying a candidate ATM, wherein the candidate ATM is not associated in the database with the user profile;

identifying, by the server, the candidate ATM by comparing the submitted ATM information to the stored ATM information;

receiving, by the server from the user device of the user, a control element indicating a request for a cardless service type of a plurality of cardless service types to be accessed at the candidate ATM;

determining, by the server, that the user is authorized to access the cardless service type of the plurality of cardless service types at the candidate ATM based on the control element;

generating and transmitting, by the server to the user device, a first onetime password (OTP) for the user to enter at the candidate ATM in response to determining that the user is authorized to access the cardless service type of the plurality of cardless service types at the candidate ATM;

receiving, by the server, a second OTP entered into ~~the candidate~~an ATM;

verifying, by the server, that the first OTP matches the second OTP and that the ATM into which the second OTP was entered matches the candidate ATM; and

in response to the verification, authorizing, by the server, access by the user to at least one service associated with the cardless service type of the plurality of cardless service types available through the candidate ATM, without use of a card.

2. The method according to Claim 1, wherein the at least one security feature includes at least one of a password, a PIN, or a biometric.

3. The method according to Claim 1, wherein the ATM information includes at least one of geolocation information of a user device associated with the user, an ATM ID code, a building name, a street name, a post code, a barcode, or a QR code.

4. The method according to Claim 1, wherein verifying that the first OTP ~~entered into the candidate ATM~~ matches the second OTP entered into the ATM further comprises comparing the first OTP to the second OTP within the database.

5. The method according to Claim 1, further comprising:

determining, by the server, that the user is authorized to access the at least one service available through the candidate ATM, without use of a card; and

instructing, by the server, the candidate ATM to provide access to the user to the at least one service.

6. The method according to Claim 1, further comprising:

receiving, by the server from the user device via the computer application, a request to access at least another cardless service type of the plurality of cardless service types available through the candidate ATM;

determining, by the server, that the user is not authorized to access the at least another cardless service type of the plurality of cardless service types without use of a card; and

instructing the candidate ATM, by the server, to refuse access to the user to the at least another cardless service type of the plurality of service types.

7. A computer system for cardless use of an automated teller machine (ATM) by a user, the computer system comprising a server, the server including at least one processor in communication with a database, the database storing a user profile of the user and stored ATM information, the stored ATM information identifying a plurality of ATMs, the computer system configured to:

receive, from a user device of the user, a request to log on to a computer application, the request including at least one security feature submitted by the user;

grant access by the user device to the computer application in response to verifying that the submitted at least one security feature matches at least one profile security feature stored in the user profile;

receive ATM information submitted by the user device via the computer application, the ATM information identifying a candidate ATM, wherein the candidate ATM is not associated in the database with the user profile;

identify the candidate ATM by comparing the submitted ATM information to the stored ATM information;

receive, from the user device of the user, a control element indicating a request for a cardless service type of a plurality of cardless service types to be accessed at the candidate ATM;

determine that the user is authorized to access the cardless service type of the plurality of cardless service types at the candidate ATM based on the control element;

generate and transmit, to the user device, a first one-time password (OTP) for the user to enter at the candidate ATM; receive a second OTP entered into ~~the candidate~~an ATM in response to determining that the user is authorized to access the cardless service type of the plurality of cardless service types at the candidate ATM;

verify that the first OTP matches the second OTP and that the ATM into which the second OTP was entered matches the candidate ATM; and

in response to the verification, authorize access by the user to at least one service associated with the cardless service type of the plurality of cardless service types available through the candidate ATM, without use of a card.

8. The computer system according to Claim 7, wherein the at least one security feature includes at least one of a password, a PIN, or a biometric.

9. The computer system according to Claim 7, wherein the ATM information includes at least one of geolocation information of a user device associated with the user, an ATM ID code, a building name, a street name, a post code, a barcode, or a QR code.

10. The computer system according to Claim 7, wherein verifying that the first OTP ~~entered into the candidate ATM~~ matches the second OTP entered into the ATM further comprises comparing the first OTP to the second OTP within the database.

11. The computer system according to Claim 7, further configured to:

determine that the user is authorized to access the at least one service available through the candidate ATM, without use of a card; and

instruct the candidate ATM to provide access to the user to the at least one service.

12. The computer system according to Claim 7, further configured to:

receive, from the user device via the computer application, a request to access at least another cardless service type of the plurality of cardless service types available through the candidate ATM;

determine that the user is not authorized to access the at least another cardless service type of the plurality of cardless service types without use of a card; and

instruct the candidate ATM to refuse access to the user to the at least another cardless service type of the plurality of cardless service types.

13. At least one non-transitory computer-readable storage media having computer-executable instructions embodied thereon for cardless use of an automated teller machine (ATM) by a user, wherein when executed by at least one processor, the processor at a server of a computer system and in communication with a database, the database storing a user profile of the user and stored ATM information, the stored ATM information identifying a plurality of ATMs, the computer-executable instructions cause the processor to:

receive, from a user device of the user, a request to log on to a computer application, the request including at least one security feature submitted by the user;

grant access by the user device to the computer application in response to verifying that the submitted at least one security feature matches at least one profile security feature stored in the user profile;

receive ATM information submitted by the user device via the computer application, the ATM information identifying a candidate ATM, wherein the candidate ATM is not associated in the database with the user profile;

identify the candidate ATM by comparing the submitted ATM information to the stored ATM information;

receive, from the user device of the user, a control element indicating a request for a cardless service type of a plurality of cardless service types to be accessed at the candidate ATM;

determine that the user is authorized to access the cardless service type of the plurality of cardless service types at the candidate ATM based on the control element;

generate and transmit, to the user device, a first one-time password (OTP) for the user to enter at the candidate ATM in response to determining that the user is authorized to access the cardless service type of plurality of cardless service types at the candidate ATM;

receive a second OTP entered into ~~the candidate~~an ATM;

verify that the first OTP matches the second OTP and that the ATM into which the second OTP was entered matches the candidate ATM; and

in response to the verification, authorize access by the user to at least one service associated with the cardless service type of the plurality of cardless service types available through the candidate ATM, without use of a card.

14. The at least one computer-readable storage media according to Claim 13, wherein the at least one security feature includes at least one of a password, a PIN, or a biometric.

15. The at least one computer-readable storage media according to Claim 13, wherein the ATM information includes at least one of geolocation information of a user device associated with the user, an ATM ID code, a building name, a street name, a post code, a barcode, or a QR code.

16. The at least one computer-readable storage media according to Claim 13, wherein verifying that the first OTP ~~entered into the candidate ATM~~ matches the second OTP entered into the ATM further comprises comparing the first OTP to the second OTP within the database.

17. The at least one computer-readable storage media according to Claim 13, wherein the computer-executable instructions further cause the processor to:

determine that the user is authorized to access the at least one cardless service type of the plurality of cardless service types available through the candidate ATM, without use of a card; and

instruct the candidate ATM to provide access to the user to the at least one cardless service type of the plurality of cardless service types.