

CLAIMS

What is claimed is:

1. An identity verification system comprising:
 - a contactless card comprising a processor and memory, the contactless card associated with a first user; and
 - one or more applications comprising instructions for execution on one or more client devices, wherein:
 - a first application is configured to transmit, after entry of the contactless card into a communication field, identity data, the first application comprising instructions for execution on a first client device,
 - a second application is configured to receive a notification based on an identity verification process, the second application comprising instructions for execution on a second client device, the notification comprising:
 - a menu including shareable specified information about the first user; and
 - an option indicative of requested access to the shareable specified information about the first user, the option including a choice to accept or decline access to the shareable specified information about the first user; and
 - the first application is configured to receive the requested access to the shareable specified information about the first user based on selection of the option, and
 - the second application is configured to revoke the requested access to the shareable specified information about the first user from the menu based on evaluation of redacted

specified information from the shareable specified information and one or more permissions, the one or more permissions including at least one selected from the group of a geographic limitation, an approval list, a transaction type, and a frequency threshold.

2. The identity verification system of claim 1, wherein the second application is configured to perform a pre-verification process by requesting, prior to display of the notification, an authentication input of one or more login credentials.
3. The identity verification system of claim 1, wherein the second application is configured to modify at least one selected from the group of the shareable specified information about the first user and access to the shareable specified information about the first user.
4. The identity verification system of claim 1, further comprising a server, wherein the server is configured to:
 - perform the identity verification process,
 - determine an outcome based on the identity verification process, and
 - transmit the notification to the second application based on the outcome.
5. The identity verification system of claim 1, wherein the identity verification process comprises a comparison between the identity data and reference data.
6. The identity verification system of claim 1, wherein the selection of the option is associated with a predetermined time duration prior to a timeout of the requested access.
7. The identity verification system of claim 1, wherein the second application comprises instructions for execution on the second client device different than the first client device.

8. The identity verification system of claim 1, wherein the notification comprises a message that the first client device is in communication with the contactless card and is requesting access to the shareable specified information about the first user.

9. A method of identity verification comprising:

transmitting, after entry of a contactless card into a communication field, identity data by a first application comprising instructions for execution on a first client device;

receiving, based on an identity verification process of the identity data, a notification at a second application comprising instructions for execution on a second client device, the notification comprising:

a menu including shareable specified information about the first user; and

an option indicative of requested access to the shareable specified information about a first user, the option further including accept or decline access to the shareable specified information about the first user;

receiving, based on selection of the option, the requested access to the shareable specified information about the first user; and

revoking, by the second application, the requested access to the shareable specified information about the first user from the menu based on evaluation of redacted specified information from the shareable specified information and one or more permissions, the one or more permissions including at least one selected from the group of a geographic limitation, an approval list, a transaction type, and a frequency threshold.

10. The method of claim 9, further comprising performing a pre-verification process by requesting, prior to display of the notification, authentication input of one or more login credentials.
11. The method of claim 9, further comprising customizing at least one selected from the group of the shareable specified information about the first user and access to the shareable specified information about the first user.
12. The method of claim 9, further comprising:
 - performing the identity verification process,
 - determining an outcome based on the identity verification process, and
 - transmitting the notification to the second application based on the outcome.
13. The method of claim 9, wherein the identity verification process comprises a comparison between the identity data and reference data.
14. The method of claim 12, wherein the identity data includes at least one selected from the group of an account number, a password, a one-time passcode, and biometric information.
15. The method of claim 9, wherein selection of the option is associated with a predetermined time duration prior to a timeout of the requested access.
16. A computer readable non-transitory medium comprising compute-executable instructions that are executed on a processor and comprising the steps of:
 - transmitting, after entry of a contactless card into a communication field, identity data for identity verification by a first application comprising instructions for execution on a first client device;
 - performing an identity verification process on the transmitted identity data;

determining an outcome based on the identity verification process;

transmitting the notification to a second application based on the outcome, wherein second application comprises instructions for execution on a second client device different than the first client device;

customizing at least one selected from the group of shareable specified information about a first user and access to the shareable specified information about the first user;

receiving, based on the identity verification process of the identity data, a notification, the notification comprising:

a menu including the shareable specified information about the first user;

a message that the first application is in communication with the contactless card and is requesting access to the shareable specified information about the first user; and

an option associated with requested access to the shareable specified information about the first user;

receiving, based on selection of the option, the requested access to the shareable specified information about the first user; and

evaluating redacted specified information from the shareable specified information about the first user and one or more permissions are evaluated to determine whether to revoke access to the shareable specified information about the first user, the one or more permissions including at least one selected from the group of a geographic limitation, an approval list, a transaction type, and a frequency threshold.

17. The identity verification system of claim 5, wherein:

the identity data comprises a password and a one-time passcode,

the reference data comprises a reference password and a reference one-time passcode.

18. The identity verification system of claim 1, wherein:

the one or more permissions comprises the geographic limitation, and

the requested access is revoked if the first application is outside of a predetermined distance of the second device.

19. The method of claim 9, wherein

the one or more permissions comprises the transaction type, and

the requested access is revoked if the requested access does not match an approved transaction type .

20. The method of claim 9, wherein:

the one or more permissions comprises the frequency threshold, and

the requested access is revoked if selection of the option occurs more than a predetermined threshold within a given time.