

What is claimed is:

1. A system, comprising
a non-transitory memory storing instructions;
a processor configured to execute the instructions to cause the system to perform operations comprising:
 - receiving, over a first wireless network connection, a request from a user device to generate a dynamic machine readable code;
 - retrieving, from a first source, user information associated with a user of the user device;
 - analyzing the user information and a device type of the user device to determine a first user information to include on the dynamic machine readable code;
 - detecting, a capture of the dynamic machine readable code; and
 - in response to the detecting, presenting a customized user interface based on the first user information embedded on the dynamic machine readable code.
2. The system of claim 1, wherein the first user information is embedded on the dynamic machine readable code using a middle tier application.
3. The system of claim 1, wherein the first user information includes at least one of a photo, an email, a date of birth, or an account number.
4. The system of claim 1, wherein the operations further comprise:
in response to the receiving the request retrieving, from a second source, the device type.
5. The system of claim 4, wherein the device type is a type of phone.
6. The system of claim 4, wherein the operations further comprise:
 - detecting, the capture of the dynamic machine readable code in conjunction with the device information; and
 - in response to the detecting, determining fraudulent activity is occurring.
7. The system of claim 6, wherein determining fraudulent activity includes identifying a device type captured does not match the first user information embedded in the dynamic

machine readable code.

8. The system of claim 1, wherein the customized user interface is based on a location of the capture of the dynamic machine readable code.

9. A method comprising:

receiving, over a first wireless network connection, a request from a user device to generate a dynamic machine readable code;

retrieving, from a first source, user information associated with a user of the user device;

analyzing the user information to determine a first user information to include on the dynamic machine readable code;

detecting, a capture of the dynamic machine readable code;

in response to the detecting, presenting a customized user interface based on the first user information embedded on the dynamic machine readable code;

detecting the capture of the dynamic machine readable code in conjunction with device information; and

based on the capture, determining fraudulent activity is occurring.

10. The method of claim 9, wherein the first user information is embedded on the dynamic machine readable code using a middle tier application.

11. The method of claim 9, wherein the first user information includes at least one of a photo, an email, a date of birth, or an account number.

12. The method of claim 11, wherein the device information includes a type of phone.

13. The method of claim 9, further comprising:

in response to the receiving the request retrieving, from a second source, the device information.

14. The method of claim 9, wherein the user information includes a device type of the user device.

15. The method of claim 9, wherein determining fraudulent activity includes identifying a device type captured does not match the first user information embedded in the dynamic machine readable code.

16. The method of claim 9, wherein the customized user interface is based on a location of the capture of the dynamic machine readable code.

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

receiving, over a first wireless network connection, a request from a user device to generate a dynamic machine readable code;

retrieving, from a first source, user information associated with a user of the user device;

analyzing the user information and a device type of the user device to determine a first user information to include on the dynamic machine readable code;

detecting, a capture of the dynamic machine readable code; and

in response to the detecting, presenting a customized user interface based on the first user information embedded on the dynamic machine readable code.

18. The non-transitory machine readable medium of claim 17, wherein the first user information is embedded on the dynamic machine readable code using a middle tier application.

19. The non-transitory machine readable medium of claim 17, wherein the first user information includes at least one of a photo, an email, a date of birth, or an account number.

20. The non-transitory machine readable medium of claim 17, wherein the operations further comprise:

in response to the receiving the request retrieving, from a second source, the device information.