MOBILE DEVICE FRAUD DETECTION WITHOUT RESORT TO A NETWORK

~~SELF-AUTHENTICATION~~

Field of the Invention:

The present invention is directed to the use of mobile devices in offline transactions, and, more particularly, to a system, method and device for self-authentication of transactions.

Description of the Related Art:

Mobile devices nowadays are in widespread use. The mobile devices of today have many uses other than plain conversation and messaging. One of the emerging fields of use for the mobile devices is for transactions such as purchasing an item.

The improved ability of mobile devices provides enhanced web capabilities (e.g. internet) and applications. The user interface has improved and thus created a platform for applications, innovative initiatives and new opportunities.
In the context of financial transactions, the mobile device can be used in many processes, when payments by which (m-payments) are one category of financial transactions implemented by the mobile platform, along with financial services (m-services) and trade (m-commerce).

It is customary to distinguish between several key procedures wherein a mobile device is involved in financial transactions:

Mobile payment – a fee, set by the transfer of money in exchange for a product or service, wherein the mobile device is involved in both the initiation and the approval of the payment. The payer can be present at the point of sale or "in movement" ("on the way") and the infrastructure that supports the payment can change.

CLAIMS

1. A mobile payment device comprising:
   a memory for storing a file containing a behavioral pattern of a customer;
   a model for storing a software element for decrypting said file.
2. The mobile payment device of claim 1 wherein said file containing a behavioral pattern of a customer is updated in real time to reflect the customer behavior.
3. The mobile payment device of claim 1 wherein said model is rejecting or approving a transaction of said customer.
4. The mobile payment device of claim 3 wherein said rejecting or approving is based on calculating the probability for fraud based on the behavioral pattern and the transaction's details.
5. The mobile payment device of claim 3 or 4 wherein if said model is rejecting said transaction, said customer will be asked to enter identification means for approving the transaction.
6. The mobile payment device of claim 5 wherein said identification means comprise password, biometric characteristic of the customer, or a combination thereof.
7. The mobile payment device of any one of the previous claims wherein said mobile payment device is a cellular phone or credit card.
8. The mobile payment device of any one of the previous claims wherein said approving of the transaction is being done offline.
9. The mobile payment device of claim 1 further comprising:
   a location receiver;
   a validity token storage place;
   transaction history storage place.
10. The mobile payment device of claim 9 wherein the payment functionality of said mobile payment device will be halted if a valid validity token was not received.
11. The mobile payment device of claim 9 wherein the entire functionality of said mobile payment device will be halted if a valid validity token was not received.

12. A method for self-authentication using a mobile payment device, said method comprising:
storing in a memory of the mobile payment device a file containing a behavioral pattern of a customer;
storing in a model of the mobile payment device a software element for decrypting said file.
13. The method claim 12 wherein said file containing a behavioral pattern of a customer is updated to reflect the customer behavior.
14. The method of claim 12 further comprising rejecting or approving a transaction of said customer by said model.
15. The method of claim 14 wherein said rejecting or approving is based on calculating the probability for fraud based on the behavioral pattern and the transaction's details.
16. The method of claim 14 or 15 further comprising asking said customer to enter identification means if said model is rejecting said transaction.
17. The method of claim 16 wherein said identification means comprise password, biometric characteristic of the customer, or a combination thereof.
18. The method of any one of claims 12 to 17 wherein said mobile payment device is a cellular phone or credit card.
19. The method of any one of the previous claims wherein said approving of the transaction is being done offline.
20. A system for self-authentication of a transaction, comprising:
A server, said server computing a behavioral pattern of a customer;
A mobile payment device , said mobile payment device computing whether the transaction can receive authorization, based on the behavioral pattern received from the server in the mobile payment device.
21. A method of self-authentication of a transaction comprising the steps of:
sending behavioral data of a customer by an issuer to a server;
computing by the server a behavioral pattern of the customer;
sending the behavioral pattern to a mobile payment device;
receiving at the mobile payment device from a point of sale details of a

transaction;

computing by the mobile payment device whether the transaction can receive authorization, based on the behavioral pattern received in the mobile payment device;

requesting said customer by the mobile payment device to enter identification means if said computing by the mobile payment device resulted that the transaction did not receive authorization;

verifying the identification means by the mobile payment device;

denying the transaction by the mobile payment device if said verifying fails;

sending transaction data to a clearing house if either said computing by the mobile payment device whether the transaction can receive authorization or said verifying the identification means resulted in a positive outcome;

sending the transaction data to an issuer.

22. The method of claim 21 wherein the steps of computing by the mobile payment device whether the transaction can receive authorization and requesting said customer by the mobile payment device to enter identification means further comprise:

initiating communication between the mobile payment device and the point of sale (POS);

transferring the details of the transaction from the POS to the mobile payment device;

approving or denying the transaction by a model in the mobile payment device;

asking the customer to enter identification means if the transaction was denied;

sending an update from the mobile payment device to the server about said approving or denying the transaction by the model.

23. The method of claim 22 wherein the step of initiating communication between the mobile payment device and the point of sale (POS) further comprises validating by the POS a validity token stored in the mobile payment device.

24. The method of claim 23 wherein the update from the mobile payment device to the server further comprises the location of the mobile payment device.

25. The method of claim 24 further comprising updating by the server the behavioral pattern of the customer based on said location and said approving or denying the transaction by the model.
26. The method of claim 21 or 22 further comprising blocking the customer from performing further transactions by not sending a valid validity token from the server to the mobile payment device, if said transaction was not approved.
27. A method for tracking merchant fraud, comprising:
keeping track in a mobile payment device of transactions of a customer;
interrogating said mobile payment device if a certain transaction took place.
28. The method of claim 27, further comprising:
receiving transaction data from a merchant by an issuer;
sending a request for transaction validation by said issuer to a server;
sending a request for transaction details by said server to said mobile payment device;
sending said transaction details or a response that said transaction details are not available by said mobile payment device to said server;
validating, by said server, said transaction and said merchant if said transaction details were available;
sending result of said validating to the issuer by said server.

CLAIMS

1. A non-transitory computer readable medium including instructions that, when executed by at least one processor, cause the at least one processor to perform operations comprising:

receiving, on a mobile payment device, transaction data associated with a requested financial transaction;

accessing behavioral information stored locally on the mobile payment device;

comparing information in the transaction data with the behavioral information on the mobile payment device without resort to a mobile network, such that the comparing is capable of occurring when the mobile payment device is outside of a network coverage area; and

determining, based on the comparing on the mobile payment device, whether to authorize the requested financial transaction.

2. The non-transitory computer readable medium of claim 1, wherein determining whether to authorize occurs on the mobile payment device, without contacting a remote server.

3. The non-transitory computer readable medium of claim 1, wherein the behavioral information comprises a behavioral pattern.

4. The non-transitory computer readable medium of claim 1, wherein the operations further comprise receiving, from a remote server, and storing, on the mobile payment device before the requested financial transaction, the behavioral information.

5. The non-transitory computer readable medium of claim 1, wherein the behavioral information stored locally on the mobile payment device includes behavioral information of a user of the mobile payment device as well as behavioral information of other users.

6. The non-transitory computer readable medium of claim 5, wherein the other users are determined to have behavioral information similar to that of the user.

7. The non-transitory computer readable medium of claim 5, wherein the other users are determined to have behavioral information associated with fraudulent behavior.

8. The non-transitory computer readable medium of claim 1, wherein the operations further comprise communicating an approval signal from the mobile payment device to a point of sale terminal after a determination is made to authorize the requested financial transaction.

9. The non-transitory computer readable medium of claim 1, wherein the comparing on the mobile payment device produces a likelihood that the requested financial transaction is fraudulent.

10. The non-transitory computer readable medium of claim 9, wherein the instructions further comprise prompting the user to provide identification information if the likelihood exceeds a threshold.

11. A computer-implemented method for processing requested financial transactions comprising:

receiving, on a mobile payment device, transaction data associated with a requested financial transaction;

accessing behavioral information stored locally on the mobile payment device;

comparing information in the transaction data with the behavioral information on the mobile payment device without resort to a mobile network, such that the comparing is capable of occurring when the mobile payment device is outside of a network coverage area; and

determining, based on the comparing on the mobile payment device, whether to authorize the requested financial transaction.

12. The computer-implemented method of claim 11, wherein determining whether to authorize occurs on the mobile payment device, without contacting a remote server.

13. The computer-implemented method of claim 11, wherein the behavioral information comprises a behavioral pattern.

14. The computer-implemented method of claim 11, further comprising receiving, from a remote server, and storing, on the mobile payment device before the requested financial transaction, the behavioral information.

15. The computer-implemented method of claim 11, wherein the behavioral information stored locally on the mobile payment device includes behavioral information of a user of the mobile payment device as well as behavioral information of other users.

16. The computer-implemented method of claim 15, wherein the other users are determined to have behavioral information similar to that of the user.

17. The computer-implemented method of claim 15, wherein the other users are determined to have behavioral information associated with fraudulent behavior.

18. The computer-implemented method of claim 11, further comprising communicating an approval signal from the mobile payment device to a point of sale terminal after a determination is made to authorize the requested financial transaction.

19. The computer-implemented method of claim 11, wherein the comparing on the mobile payment device produces a likelihood that the requested financial transaction is fraudulent.

20. The computer-implemented method of claim 19, further comprising prompting the user to provide identification information if the likelihood exceeds a threshold.