Method (CVM) is used. This provides speed and convenience to users as they do not have to undertake a verification method.

Consumer Device Cardholder Verification Methods (CDCVMs) are increasingly being used for payment devices comprising a mobile device with a digital wallet. The use of CDCVMs generally allows the value of a payment transaction to be increased due to the security provided by verification. CDCVMs involve a user of the payment device verifying their identity on the payment device itself. During a payment transaction using CDCVM, no additional customer action is required on the POI or paper receipt to verify the customer, such as a signature or PIN. For example, the mobile device may be arranged to receive a PIN and/or comprise a biometric sensor for verifying the identity of a user. The payment device can then be used with a POI to undertake a payment transaction.

It is an aim of the present disclosure to address disadvantages associated with the prior art.

SUMMARY

In one aspect, the present disclosure provides a method for providing user authentication and user consent for a contactless transaction made with a mobile payment device, comprising: providing on the mobile payment device a digital wallet module, comprising: a communication module; a wallet processor; a consent risk manager module; and a payment application module; wherein the consent risk manager module is electronically coupled to the wallet processor and wherein the consent risk manager module further includes a decision module on the payment device, wherein the consent risk manager module provides authentication based on a consumer device cardholder verification method (CDCVM); a user authentication step, executed by the consent risk manager module, to verify that a user is entitled to use the payment device for a specific transaction; an implicit user consent step, determined by a decision module of the consent risk manager module, to verify that the user implicitly consents to the specific transaction, wherein: implicit consent is based on contextual information that is not directly related to providing explicit consent to the specific transaction, bypassing the need for any additional user action to indicate explicit consent, the user authentication step is discrete from the user consent step, the implicit user consent step is based on an order of events, and the events comprise correlating at least a plurality of user actions and behavioral

information, transaction context information, payment device information, terminal data, environmental information and proprietary check data; outputting, from the decision module to the payment application module, implicit consent data indicating that implicit consent for the specific transaction has been determined based on an analysis of the events; combining as CDCVM data the implicit consent data and authentication data associated with the CDCVM; and communicating, via the communication module and using an EMV data structure, the combined implicit consent data and CDCVM authentication data to an Issuer of an account associated with the mobile payment device.

In another aspect, the present disclosure provides a mobile payment device comprising a digital wallet module, the digital wallet module comprising: a wallet processor electronically coupled to a consent risk manager module and a payment application module, and a communication module, wherein the consent risk manager module further includes a decision module on the payment device, wherein the consent risk manager module provides authentication based on a consumer device cardholder verification method (CDCVM), the digital wallet module programmed to perform the following steps to provide user authentication and user consent for a contactless transaction made with the mobile payment device, the steps comprising: a user authentication step, executed by the consent risk manager module to verify that a user is entitled to use the payment device for a specific transaction and; an implicit user consent step, determined by a decision module of the consent risk manager module, to verify that the user implicitly consents to the specific transaction, wherein: implicit consent is based on contextual information that is not directly related to providing explicit consent to the specific transaction, bypassing the need for any additional user action to indicate explicit consent, the user authentication step is discrete from the user consent step, the implicit user consent step is based on an order of events, and the events comprise correlating at least a plurality of user actions and behavioral information, transaction context information, payment device information, terminal data, environmental information and proprietary check data; an output from the decision module to the payment application module, implicit consent data indicating that implicit consent for the specific transaction has been determined based on an analysis of the events; a combination of the implicit consent data and authentication data associated with the CDCVM as CDCVM data; and communication, via the communication module and using an EMV data structure, the

combined implicit consent data and CDCVM authentication data to an Issuer of an account associated with the mobile payment device.

According to one aspect of the present disclosure, there is provided a method for providing user authentication and user consent for a transaction made with a payment device, the method comprising a user authentication step to verify that a user is entitled to use the payment device and a user consent step to verify that the user consents to the transaction, wherein the user authentication step is discrete from the user consent step. The user authentication step may comprise a consumer device cardholder verification method (CDCVM). This user authentication step may be taken outside a transaction context, but may persist into a transaction context. The user consent step may be an explicit user consent made within a transaction process. The user consent may in embodiments be an implicit user consent inferred from user or device actions or user or device context. According to yet another aspect of the present disclosure, there is provided a payment device, the payment device comprising a processor programmed to perform the following steps to provide user authentication and user consent for a transaction made with the payment device, the steps comprising a user authentication step to verify that a user is entitled to use the payment device and; a user consent step to verify that the user consents to the transaction, wherein the user authentication step is discrete from the user consent step. In various embodiments, there is provided apparatus adapted to perform the methods described above are also provided.

Within the scope of this application it is expressly intended that the various aspects, embodiments, examples and alternatives set out in the preceding paragraphs, in the claims and/or in the following description and drawings, and in particular the individual features thereof, may be taken independently or in any combination. That is, all embodiments and/or features of any embodiment can be combined in any way and/or combination, unless such features are incompatible. The

CLAIMS

1. A method for providing user authentication and user consent for a contactless transaction made with a mobile payment device, comprising:

providing on the mobile payment device a digital wallet module, comprising:

a communication module;

a wallet processor;

a consent risk manager module; and

a payment application module;

wherein the consent risk manager module is electronically coupled to the wallet processor and wherein the consent risk manager module further includes a decision module on the payment device, wherein the consent risk manager module provides authentication based on a consumer device cardholder verification method (CDCVM);

a user authentication step, executed by the consent risk manager module, to verify that a user is entitled to use the payment device for a specific transaction;

an implicit user consent step, determined by a decision module of the consent risk manager module, to verify that the user implicitly consents to the specific transaction, wherein:

implicit consent is based on contextual information that is not directly related to providing explicit consent to the specific transaction, bypassing the need for any additional user action to indicate explicit consent,

the user authentication step is discrete from the user consent step,

the implicit user consent step is based on an order of events, and

the events comprise correlating at least a plurality of user actions and behavioral

information, transaction context information, payment device information, terminal data, environmental information and proprietary check data;

outputting, from the decision module to the payment application module, implicit consent data indicating that implicit consent for the specific transaction has been determined based on an analysis of the events;

combining as CDCVM data the implicit consent data and authentication data associated with the CDCVM; and

communicating, via the communication module and using an EMV data structure, the combined implicit consent data and CDCVM authentication data to an Issuer of an account associated with the mobile payment device.

2. The method of claim 1, wherein the user authentication step is taken outside a transaction context, but persists into a transaction context.

3. The method of claim 1, wherein the user consent step is an explicit user consent made within a transaction process.

4. The method of claim 1, wherein the user consent is an implicit user consent inferred from user or device actions or user or device context.

5. The method of claim 1, wherein results of the user authentication step and the user consent step are provided within a transaction.

6. The method of claim 5, wherein the results of the user consent step comprise a type of consent.

7. The method of claim 5, wherein the results of the user consent step comprise a rating of the user consent step.

8. The method of claim 5, wherein the results of the user authentication step comprise a type of user authentication used.

9. The method of claim 5, wherein the results of the user consent step comprise a rating of the user authentication step.

10. The method of claim 5, wherein the results of the user authentication step and the user consent step are transmitted as magnetic stripe track data.

11. The method of claim 10, further comprising encoding the results of the user authentication step and the user consent step into a coded value before transmission in the transaction.

12. A mobile payment device comprising a digital wallet module, the digital wallet module comprising: a wallet processor electronically coupled to a consent risk manager module and a payment application module, and a communication module, wherein the consent risk manager module further includes a decision module on the payment device, wherein the consent risk manager module provides authentication based on a consumer device cardholder verification method (CDCVM), the digital wallet module programmed to perform the following steps to provide user authentication and user consent for a contactless transaction made with the mobile payment device, the steps comprising:

a user authentication step, executed by the consent risk manager module to verify that a user is entitled to use the payment device for a specific transaction and;

an implicit user consent step, determined by a decision module of the consent risk manager module, to verify that the user implicitly consents to the specific transaction, wherein:

implicit consent is based on contextual information that is not directly related to providing explicit consent to the specific transaction, bypassing the need for any additional user action to indicate explicit consent,

the user authentication step is discrete from the user consent step,

the implicit user consent step is based on an order of events, and

the events comprise correlating at least a plurality of user actions and behavioral

information, transaction context information, payment device information, terminal data, environmental information and proprietary check data;

an output from the decision module to the payment application module, implicit consent data indicating that implicit consent for the specific transaction has been determined based on an analysis of the events;

a combination of the implicit consent data and authentication data associated with the CDCVM as CDCVM data; and

communication, via the communication module and using an EMV data structure, the combined implicit consent data and CDCVM authentication data to an Issuer of an account associated with the mobile payment device.

13. The payment device of claim 12, wherein the payment device is adapted to provide results of the user authentication step and the user consent step within a transaction.