payment device credentials visible thereon. Further, since these merchants have no means to discriminate payment devices that do have their credentials visible thereon, the merchants cannot monitor or remedy the situation. Furthermore, in many such environments, such as a transit service, the merchant has no means to communicate with the consumer at the point of service, as the terminal is unattended and/or the consumer has already left the terminal by the time the authorisation request is submitted. Thus, although the removal of visible credentials from contactless payment devices is designed to improve security of payment transactions, simplify their processing, and/or prevent their users from conducting certain types of transactions, e.g., e-commerce transactions, the actual effect is that users of such devices may not be able to enjoy services or goods that they should be able to enjoy and would have enjoyed if they used a more traditional payment device, such as a credit or debit card that has a PAN, a CVC2, and an expiry date printed or embossed thereon.

There is therefore a need to provide an improved method and/or system for processing transit payment transactions that enable users of payment devices that do not have one or more credentials visible thereon to use back-end services provided by transit agencies, including but not limited to accessing history transactions and disputing charges, even when such users do not know credentials associated with their payment devices. More generally, there is a need to provide a method and/or a system for processing payment transactions at unattended terminals that are adept to successfully process payment transactions initiated by a payment device that does not have one or more credentials visible thereon, whilst enabling a respective merchant to authenticate requests from a user of such a device subsequent to the payment transaction and to enable such users to access all services and goods available at the merchant in association with the payment transaction. There is a further need to enable issuers to prohibit use of certain payment devices for a certain type of transactions, without encroaching on user's ability to use the payment device for other types of transactions.

Summary of the Invention

The described embodiments of the invention provide for methods and systems for processing transactions initiated at unattended terminals by users who do not have access to the real credentials of user devices they use to initiate transactions.

Disclosed herein is a computer-implemented method for processing transactions associated with a first party, the method comprising:

receiving authorisation request data from a first party device concerning a transaction initiated at an unattended terminal of the first party device, the authorisation request data comprising real credentials of a user device used to initiate the transaction;

issuing one or more pseudo credentials for a user associated with the real credentials;

transmitting authorisation response data responsive to the authorisation request data through a payment system network toward the first party device, the authorisation response data comprising the one or more pseudo credentials; and

communicating the one or more pseudo credentials to the user.

Also disclosed is a non-transitory computer readable medium having stored instructions thereon which, when executed by at least one processor of a computer system, cause the computer system to carry out the method described above.

Also disclosed is a processing hub for processing a transaction initiated at an unattended terminal associated with a first party device, the processing hub comprising:

a memory for storing real credentials in association with pseudo credentials for a plurality of user devices, the memory storing instructions; and

at least one processor configured, when executing the instructions stored in the memory, to cause the processing hub to carry out the method described above.

Examples of processing systems, environments, and/or configurations that may be suitable for use with the embodiments described herein include, but are not limited to, embedded computer devices, personal computers, server computers (specific or cloud (virtual) servers), hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, mobile telephones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like. Hardware modules or apparatuses described in this disclosure include, but are not limited to, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGAs), dedicated or shared processors, and/or other hardware modules or apparatuses.

The order of execution or performance of the operations in the embodiments illustrated and described herein is not essential, unless otherwise specified. That is, the operations/steps may be performed in any order, unless otherwise specified, and embodiments may include additional or fewer operations/steps than those disclosed herein. For example, a particular selected order of steps of methods described in relation to FIGURES 3A to 6 may depend on preferences and/or technical specifications of the parties involved in the payment transaction processing. It is further contemplated that executing or performing a particular operation/step before, contemporaneously with, or after another operation is in accordance with the described embodiments.

While the invention has been described in terms of various specific embodiments, the skilled person would recognize that the invention can be practiced with modification within the spirit and scope of the claims.

The reference in this specification to any prior publication (or information derived from it), or to any matter which is known, is not, and should not be taken as an acknowledgment or admission or any form of suggestion that that prior publication (or information derived from it) or known matter forms part of the common general knowledge in the field of endeavour to which this specification relates.

Claims:

1. A computer-implemented method for processing transactions associated with a first party, the method comprising:

receiving authorisation request data from a first party device concerning a transaction initiated at an unattended terminal of the first party device, the authorisation request data comprising real credentials of a user device used to initiate the transaction;

issuing one or more pseudo credentials for a user associated with the real credentials;

transmitting authorisation response data responsive to the authorisation request data through a payment system network toward the first party device, the authorisation response data comprising the one or more pseudo credentials; and

communicating the one or more pseudo credentials to the user.

2. The method according to claim 1, wherein the one or more pseudo credentials are issued for the user to be used to query the first party concerning at least the transaction.

3 The method according to claim 1 or 2, wherein the one or more pseudo credentials are issued upon determining that the one or more pseudo credentials are required for the user device.

4. The method according to any one of claims 1 to 3, wherein the one or more pseudo credentials are determined to be required if one of more of the real credentials are not accessible to the user on the device.

5. The method according to one of claims 1 to 4, wherein the issuing of the one or more pseudo credentials comprises retrieving one or more pseudo credentials pre-generated prior to receiving the authorisation request data.

6. The method according to any of claims 1 to 4, further comprising:

generating the one or more pseudo credentials after receiving the authorisation request data.

7. The method according to any one of claims 1 to 6, further comprising:

storing the one or more pseudo credentials in association with the real credentials.

8. The method according to any one of claims 1 to 7, wherein the one or more pseudo credentials comprise at least one of a pseudo primary account number, a pseudo expiry

date, a pseudo card verification code, a pseudo name, a pseudo address, or one or more pseudo security codes.

9. The method according to any of claims 1 to 8, wherein communicating the one or more pseudo credentials to the user comprises at least one of:

sending an e-mail message comprising the one or more pseudo credentials to an e-mail address associated with the user;

sending a text message comprising the one or more pseudo credentials to a phone number associated with the user;

providing a computer-generated voice notification comprising the one or more pseudo credentials to the phone number associated with the user; or

making the one or more pseudo credentials available for access by the user via an application used by the user to access data concerning a user's account.

10. The method according to any one of claims 1 to 9, wherein the user device is a contactless device.

11. The method according to any one of claims 1 to 9, wherein the user device is one of: a payment card having no primary account number printed or embossed thereon, a key fob, a key tag, a sticker, a smartcard, or an NFC enabled mobile device.

12. The method according to any one of claims 1 to 11, wherein the method is performed by a third party that generates and maintains pseudo credentials at least on behalf of a second party associated with the user device.

13. The method according to claim 12, further comprising:

receiving an enquiry authorisation request data from the first party concerning the user device, the enquiry comprising the one or more pseudo credentials;

matching the one or more pseudo credentials to the real credentials of the user device;

updating the enquiry authorisation request data with the one or more pseudo credentials; and

transmitting the updated enquiry authorisation request data toward the second party.

14. The method according to claim 13, further comprising:

receiving, from the second party, an enquiry response data responsive to the updated enquiry authorisation request data;

updating the enquiry response data with the one or more pseudo credentials; and

transmitting the updated enquiry response data toward the first party.

15. The method according to any one of claims 12 to 14, wherein the second party is an issuer and the user device is a payment device issued by the issuer.

16. The method according to any one of claims 12 to 15, wherein the third party is a payment system network.

17. The method according to any of claims 1 to 15, further comprising:

receiving an enquiry from the first party concerning the user device, the enquiry comprising the one or more pseudo credentials; and

matching the one or more pseudo credentials to the real credentials.

18. The method according to any one of claims 1 to 17, wherein the one or more pseudo credentials are issued to replace one or more of the real credentials that are not accessible to the user on the user device.

19. The method according to any one of claims 1 to 18, wherein the transaction is a payment transaction, the first party is a merchant, the user device is a payment device, and the user is a customer of the merchant.

20. A non-transitory computer readable medium having stored instructions thereon which, when executed by at least one processor of a computer system, cause the computer system to carry out the method according to any of claims 1 to 19.

21. A processing hub for processing a transaction initiated at an unattended terminal associated with a first party device, the processing hub comprising:

a memory for storing real credentials in association with pseudo credentials for a plurality of user devices, the memory storing instructions; and

at least one processor configured, when executing the instructions stored in the memory, to cause the processing hub to carry out the method according to any of claims 1 to 19.