

CLAIMS:

1. An electronic payment system (EPS) (1000) for facilitating payment transactions between a plurality of users, said system comprising:
 - a main storage device (1002a) configured to store a set of pre-determined rules;
 - 5 • an operating processor (1002b) configured to cooperate with said main storage device (1002a) to receive and process said pre-determined rules to obtain a set of system operating commands;
 - a plurality of Payment Service Provider systems (PSPSs) configured to register users and further configured to be registered with said EPS (1000), each PSPS
 - 10 (1004) comprising:
 - a local storage device (1004a) configured to store user information data relating to users registered with said PSPS (1004),
 - at least one look up table (1004b) configured to facilitate matching data inputted by a customer, a user information data, and a registered
 - 15 user, and
 - a PSPS server (1004c);
 - a plurality of user devices, each user device (1006) associated with one of said registered users and registered as a part of user information data;
 - Payment Service Provider Application (PSPA) tools, each PSPA tool (1008)
 - 20 associated with and hosted by a PSPS server (1004c) of a PSPS (1004) registered with said EPS (1000), and having elements which are downloadable and storable in the user device (1006) of a registered user irrespective of the fact that the registered user is registered with the PSPS associated with said PSPA tool (1008) or not, each PSPA tool (1008) configured to facilitate generation and receipt of
 - 25 transactional data signals relating to payment requests from said registered users, and credit and/or debit accounts of said registered users based on said requests, said downloadable elements of each PSPA tool (1008) comprising:
 - a registering module (1008a) configured to permit registration of a user device (1006) with a registered PSPS (1004) associated with a
 - 30 PSPA tool (1008) in a one to one correspondence, and
 - a virtual payment address (VPA) creator module (1008b) configured to enable a registered user to create a unique VPA which includes identification of the PSPS in which the registered user is registered,

and further enable a user device (1006) to transmit said unique VPA to the local storage device (1004a) of the PSPS (1004) in which the user is registered, as part of the registered user's user information data;

5 and

- a Unified Payment Interface (UPI) (100) configured to facilitate registration of a PSPS (1004) with said EPS (1000), and further configured to facilitate controlled movement of transactional data signals selectively between PSPSs, to effect payment from one registered user to another registered user in same or different

10 PSPSs, said UPI (100) comprising:

- a settlement module (100a) configured to cooperate with said plurality of PSPSs to periodically collate credit and debit transactions, and generate net credit and debit instructions between said registered PSPSs.

15

2. The EPS (1000) as claimed in claim 1, wherein said UPI (100) further comprises:

- a receiver (100b) configured to receive transactional data signals relating to payment requests from the registered user devices via any of the PSPA tools, each request comprising a VPA of a first registered user, a VPA of a second registered
- 20 user, and a transaction amount;
- a parser (100c) configured to parse said transactional data signals to obtain parsed signals;
 - an extractor identifier (100d) configured to extract and identify, from the parsed signals, information relating to the PSPS of the first registered user and the PSPS
- 25 of the second registered user; and
- a transmitter (100e) configured to transmit said transactional data signals to the identified respective PSPSs, to facilitate credit from or debit to an account of the first registered user to or from an account of the second registered user, selectively based on content of the parsed data signals.

30

3. The EPS (1000) as claimed in claim 1, wherein each PSPS (1004) further comprises an authentication module configured to provide 2-factor authentication, said authentication module comprising:

- 5 • a first factor authenticator configured to accept a pre-registered unique number, form a user registered with said PSPS (1004), to validate and associate the registered user with a registered user device (1006) by matching the accepted pre-registered unique number with the registered user's user information data stored in said local storage device (1004a), thereby providing a first factor authentication, and
 - 10 • a second factor authenticator configured to accept a UPI PIN and/or biometrics input from the registered user to authenticate the registered user by matching the accepted PIN and/or biometrics input with said user information data, thereby providing a second factor authentication.
4. The EPS (1000) as claimed in claim 2, wherein said UPI (100) further comprises a transaction server for processing the transactional data signals, an authorization server for user authorization, and a UPI server to process a stored set of rules for identifying
- 15 registered PSPSs.
5. An electronic payment method for facilitating payment transactions between a plurality of users, said method comprising the following steps:
- 20 • storing, in a main storage device, a set of pre-determined rules;
 - processing, by an operating processor, said pre-determined rules to obtain a set of system operating commands;
 - registering users to a plurality of Payment Service Provider systems (PSPSs) configured to be registered with an electronic payment system (EPS) (1000), each PSPS comprising steps of:

 - 25 ○ storing, in a local storage device, user information data relating to users registered with said PSPS,
 - facilitating, by at least one look up table, matching data inputted by a customer, a user information data, and a registered user, and
 - providing a PSPS server;
 - 30 • associating each user device of a plurality of user devices with one of said registered users, and registering as a part of user information data;
 - associating and hosting, each Payment Service Provider Application (PSPA) tool of a plurality of PSPA tools, by a PSPS server of a PSPS registered with said

EPS, and having elements which are downloadable and storable in the user device of a registered user irrespective of the fact that the registered user is registered with the PSPS associated with said PSPA tool or not, and further facilitating, by each PSPA tool, generation and receipt of transactional data signals relating to payment requests from said registered users, and credit and/or debit accounts of said registered users based on said requests, said downloadable elements of each PSPA tool comprising steps of:

- permitting, by a registering module, registration of a user device with a registered PSPS associated with a PSPA tool in a one to one correspondence, and
- enabling, by a virtual payment address (VPA) creator module, a registered user to create a unique VPA which includes identification of the PSPS in which the registered user is registered, and further enabling a user device to transmit said unique VPA to the local storage device of the PSPS in which the user is registered, as part of the registered user's user information data;

and

- facilitating, by a Unified Payment Interface (UPI), registration of a PSPS with said EPS, and controlled movement of transactional data signals selectively between PSPSs to effect payment from one registered user to another registered user in same or different PSPSs, said UPI comprising steps of:
 - providing a settlement module configured to cooperate with said plurality of PSPSs to periodically collate credit and debit transactions, and generate net credit and debit instructions between said registered PSPSs.

6. The method as claimed in claim 5, wherein said UPI further comprises the following:

- receiving, by a receiver, transactional data signals relating to payment requests from the registered user devices via any of the PSPA tools, each request comprising a VPA of a first registered user, a VPA of a second registered user, and a transaction amount;
- parsing, by a parser, said transactional data signals to obtain parsed signals,

- extracting and identifying from the parsed signals, by an extractor identifier, information relating to the PSPS of the first registered user and the PSPS of the second registered user,
- transmitting, by a transmitter, said transactional data signals to the identified
5 respective PSPSs, to facilitate credit from or debit to an account of the first registered user to or from an account of the second registered user, selectively based on content of the parsed data signals.

7. The method as claimed in claim 5, wherein each PSPS further comprises the
10 following:

- providing 2-factor authentication, by an authentication module, said step of providing 2-factor authentication comprises the following steps:
 - accepting, by a first factor authenticator, a pre-registered unique
15 number from a user registered with said PSPS, to validate and associate the registered user with a registered user device, by matching the accepted pre-registered unique number with the registered user's user information data stored in said local storage device, thereby providing a first factor authentication, and

- accepting, by a second factor authenticator, a PIN and/or biometrics input from the registered user to authenticate the registered user by matching the accepted PIN and/or biometrics input with said user information data, thereby providing a second factor authentication.