

CLAIMS

1. A method of routing payments to non-card based entities using a card-based network, the method comprising:

assigning a pseudo-bank identification number (pseudo-BIN) to a payouts service provider supporting endpoints without financial card accounts;

assigning a pseudo-primary account number (pseudo-PAN) to the payouts service provider;

exposing a send payout application program interface (API) that receives a request to transfer funds to a recipient account of an account holder, wherein the send payout API comprises fields to communicate:

a payment amount;

a sending account; and

a recipient account;

parsing the request to determine the pseudo-PAN;

determining the payouts service provider based on the pseudo-PAN;

generating a look-ahead query to the payouts service provider using the pseudo-BIN associated with the pseudo-PAN;

receiving from the payouts service provider a response to the look-ahead query, the response including a recipient endpoint dataset;

assessing the recipient endpoint dataset to determine a success factor for fulfilling the request to transfer funds, wherein the success factor is based on the recipient endpoint dataset only;

comparing the success factor to a predetermined threshold;

responsive to the success factor exceeding the predetermined threshold, preparing a transaction payload including data from the recipient endpoint dataset; and

sending the transaction payload to the recipient account to execute the request to transfer funds.

2. The method of claim 1, further comprising exposing a received response application program interface (API) wherein the received response API comprises fields to communicate:

payouts that were returned; and
payouts that were rejected.

3. The method of claim 2, wherein the received response comprises a code which indicates one selected from a group comprising:

approved and completed successfully;
invalid transaction;
invalid amount;
invalid account number (no such number);
transaction not permitted to cardholder;
exceeds approval amount limit;
transaction does not fulfill requirement;
exceeds velocity limits;
transaction timeout;
transaction cannot be completed - violation of law;
duplicate transmission; and
invalid routing transit number.

4. The method of claim 2, wherein the received response comprises a code indicating a reason for a payout return including one selected from a group comprising:

- an account not found;
- a bank could not be located using bank information provided;
- a beneficiary name does not match an account owner's name;
- an amount is higher than a limit;
- an identification number provided to identify the beneficiary does not match an owner of the account;
- missing sender data;
- missing beneficiary data;
- returned due to regulatory reason;
- an account has been restricted;
- a recipient bank rejected the transfer;
- an account has been closed;
- a payment was not accepted by a recipient bank since it is not permitted as per a regulation or policy;
- a recipient bank returned the payment since it is a duplicate;
- a recipient did not accept the payment;
- no reason provided; and
- a payment was returned based on a good faith request from sending bank.

5. The method of claim 1, further comprising exposing a status notifications application program interface (API), wherein the status notifications API comprises a field to communicate interim status details.

6. The method of claim 5, wherein the status details include an indication that the transfer request has been received and is being processed, an indication that a payout has been sent to the recipient account, an indication that the transfer request is declined, an indication that the payout has been returned to the sending account, or an indication that the transfer request is pending additional information.
7. The method of claim 1, wherein the recipient endpoint dataset comprises onboarding data including identity information and a legal status of the recipient account holder.
8. The method of claim of 7, wherein the recipient endpoint dataset comprises anti-money laundering information.
9. The method of claim 7, wherein the recipient endpoint dataset comprises know your customer information.
10. The method of claim 1, wherein assessing the recipient endpoint dataset comprises identifying a closed account message in the dataset.
11. The method of claim 1, wherein assessing the recipient endpoint database comprises identifying a legal hold message in the database.
12. A computer-implemented method for routing payments to non-card based recipient endpoints using a card-based network, comprising:

assigning a pseudo-bank identification number (pseudo-BIN) to a payouts service provider supporting payouts to non-card based recipient endpoints without financial card accounts;

assigning a pseudo-primary account number (pseudo-PAN) to the payouts service provider;

exposing a first push application program interface (API) that receives a request to transfer funds to a recipient account, the recipient account being a non-card based endpoint associated with the payouts service provider, wherein the request to transfer funds includes fields to communicate:

a payment amount;

a sending account;

the recipient account; and

the pseudo-BIN and the pseudo-PAN;

pushing the request to transfer funds to a second push application program interface (API) associated with the payouts service provider;

receiving a response from the payouts service provider, the response including a recipient account dataset associated with the recipient account;

assessing the recipient account dataset to determine a success factor for fulfilling the request to transfer funds to the recipient account, wherein the success factor is based on the recipient account dataset only;

comparing the success factor to a predetermined threshold; and

executing the request to transfer funds responsive to the success factor exceeding the predetermined threshold.

13. The computer-implemented method of claim 12, wherein the recipient account dataset includes anti-money laundering information.

14. The computer-implemented method of claim 12, further comprising exposing the first push API that receives the response from the payouts service provider, wherein the response received from the payouts service provider comprises a response code indicating one or more of the following:

- approved and completed successfully;
- invalid transaction;
- invalid amount;
- invalid account number (no such number);
- transaction not permitted to recipient account;
- exceeds approval amount limit;
- exceeds velocity limits;
- transaction timeout;
- transaction cannot be completed – violation of law;
- duplicate transmission; and
- invalid routing transit number.

15. The computer-implemented method of claim 12, further comprising exposing a return application program interface (API) that receives a return request message from the payouts service provider when the payouts service provider cannot complete the request for funds transfer to the recipient account, the return request message including a request to return funds to the sending account and a reason for the return of funds to the sending account.

16. The computer-implemented method of claim 12, further comprising exposing a watchlist application program interface (API) that screens the sending account and the recipient account against global watchlists.

17. The computer-implemented method of claim 12, further comprising exposing a cancel payout application program interface (API) that receives a request to cancel the request to transfer funds to the recipient account.

18. A system for routing payments to non-card based recipient endpoints, comprising:

a requestor/payor;

a payouts service provider supporting payouts to non-card based recipient endpoints without financial card accounts; and

a transaction processor configured to execute computer-executable instructions for:

assigning a pseudo-bank identification number (pseudo-BIN) to the payouts service provider;

assigning a pseudo-primary account number (pseudo-PAN) to the payouts service provider;

exposing a first push application program interface (API) configured to receive a request to transfer funds to a recipient account from the requestor/payor, the recipient account being a non-card based endpoint associated with the payouts service provider, wherein the request to transfer funds includes fields to communicate:

a payment amount;
a sending account;
a recipient account; and
the pseudo-BIN and the pseudo-PAN;
pushing the request to transfer funds to a second push application
program interface (API) associated with the payouts service provider;
receiving a response from the payouts service provider, the response
including a recipient account dataset associated with the recipient account;
assessing the recipient account dataset to determine a success factor for
fulfilling the request to transfer funds, wherein the success factor is based on the
recipient account dataset only;
comparing the success factor to a predetermined threshold; and
executing the request to transfer funds responsive to the success factor
exceeding the predetermined threshold.

19. The system of claim 18, wherein the transaction processor is further configured to execute computer executable instructions for exposing a return application program interface (API) that receives a return request message from the payouts service provider when the payouts service provider cannot complete the request for funds transfer to the recipient account, the return request message including a request to return funds to the sending account and a reason for the return of funds to the sending account.

20. The system of claim 18, wherein the first push API is a single unified API that receives requests to transfer funds to both card-based and non-card based recipient endpoints.