

CLAIMS

What is claimed is:

1. A method for provisioning funding card numbers to third party wallets, comprising:
 - in an information processing apparatus comprising at least one computer processor:
 - authenticating a customer using an electronic device;
 - redirecting the customer to a third-party website;
 - receiving, from the third-party website and via a first API, a request for funding primary account numbers (FPANs) associated with the customer;
 - providing the third-party website with a plurality of FPAN identifiers for FPANs associated with the customer;
 - receiving, from the third-party website and via a second API, a request for a FPAN associated with a selected FPAN identifier;
 - encrypting the FPAN associated with the selected FPAN identifier;
 - and
 - communicating the encrypted FPAN to the third-party website.
2. The method of claim 1, further comprising:
 - providing the third-party website with an authentication token and a session key during the redirect.
3. The method of claim 1, wherein the FPAN identifiers each comprise fewer than all digits of the FPAN.
4. The method of claim 1, wherein the FPAN identifiers are encrypted

5. The method of claim 1, wherein the step of encrypting the FPAN associated with the selected FPAN identifier comprises:

encrypting FPAN data associated with the selected FPAN identifier, wherein the FPAN data comprises the FPAN and at least one of an expiration date and a billing zip code.

6. The method of claim 1, wherein the third party decrypts the encrypted FPAN and stores the FPAN.

7. A method for provisioning funding card numbers to third party wallets, comprising:

in an issuer backend comprising at least one computer processor:

authenticating a customer using an electronic device accessing the issue backend using a computer program;

receiving, from the customer, a request to provision a FPAN to a third party;

launching a frame in the computer program with a website for the third party, wherein the customer logs in to the website for the third party using the frame and the third-party website generates a session identifier for a session with the customer;

receiving, from the third-party website, the session identifier;

encrypting the FPAN; and

communicating the encrypted FPAN to the third-party website.

8. The method of claim 7, wherein the computer program comprises a computer application or a website.

9. The method of claim 8, wherein the frame comprises a lightbox.

10. The method of claim 7, further comprising:
validating the session identifier.
11. The method of claim 10, wherein the validation comprises
OAUTH or SiteMinder validation.
12. The method of claim 7, wherein the step of encrypting the FPAN
comprises:
encrypting FPAN data associated with the FPAN, wherein the FPAN data
comprises the FPAN and at least one of an expiration date and a billing zip
code.
13. The method of claim 12, wherein the third party decrypts the
encrypted FPAN and stores the FPAN.
14. A method for provisioning funding card numbers to third party
wallets, comprising:
in an information processing apparatus comprising at least one computer
processor:
receiving, from a third-party website and on behalf of a customer,
an authentication request for the customer;
generating an access token;
generating a symmetric key using the access token;
receiving, from the third-party website and via a first API, a
request for funding primary account numbers (FPANs) associated with
the customer and an authentication token;
providing the third-party website with a plurality of FPAN
identifiers for FPANs associated with the customer;

receiving, from the third-party website and via a second API, a request for a FPAN associated with a selected FPAN identifier and the authentication token;;

encrypting the FPAN associated with the selected FPAN identifier with the symmetric key; and

communicating the encrypted FPAN to the third-party website.

15. The method of claim 14, wherein the FPAN identifiers each comprise fewer than all digits of the FPAN.

16. The method of claim 14, wherein the FPAN identifiers are encrypted

17. The method of claim 14, wherein the step of encrypting the FPAN associated with the selected FPAN identifier comprises:

encrypting FPAN data associated with the selected FPAN identifier, wherein the FPAN data comprises the FPAN and at least one of an expiration date and a billing zip code.

18. The method of claim 14, wherein the third party decrypts the encrypted FPAN using the symmetric key and stores the FPAN.

19. The method of claim 14, wherein the authentication token comprises an OAUTH token.