

WHAT IS CLAIMED IS:

1. A consumer authentication and payment authorization method, comprising:
 - receiving, by a Proxy Service Manager Server computer, a consumer authentication request from a merchant device comprising consumer information from a consumer mobile device;
 - transmitting by the Proxy Service Manager Server computer, the consumer authentication request comprising the consumer information to an Authentication Service Manager Server computer;
 - receiving, by the Proxy Service Manager Server computer, from the Authentication Service Manager Server computer, a non-repudiable accountholder authentication value (“AAV”) token for transaction matching at an Issuer financial institution (FI);
 - generating, by the Proxy Service Manager Server computer, a payment authorization request that includes the AAV token in a Universal Card Authentication Field;
 - transmitting, by the Proxy Service Manager Server computer, the payment authorization request to an Acquirer financial institution (FI) Server computer;
 - receiving, by the Proxy Service Manager Server computer from the Acquirer FI, a payment authorization message signifying that the Issuer FI validated the AAV token; and
 - transmitting, by the Proxy Service Manager Server computer, the payment authorization message to the merchant device ~~to enable~~ing a merchant to complete a purchase transaction with a consumer.
2. The method of claim 1, further comprising, prior to transmitting the consumer authentication request, establishing a secure communications channel between the Proxy Service Manager Server computer and the Authentication Service Manager Server computer.
3. The method of claim 1, wherein the consumer authentication request comprises an alias or a surrogate factor.

4. The method of claim 3, further comprising, subsequent to transmitting the consumer authentication request:
- mapping, by the Authentication Service Manager Server computer, the alias or the surrogate factor to consumer account information;
- 5 validating the consumer account information;
- generating a non-repudiable AAV token; and
- transmitting, by the Authentication Service Manager Server computer, the non-repudiable AAV token to the Proxy Service Manager Server computer.
- 10 5. The method of claim 4, wherein validating the consumer's account information further comprises:
- retrieving a MS-ISDN number from a database storing consumer mobile device data;
- transmitting, by the Authentication Service Manager Server computer, a
- 15 challenge/response request to the MS-ISDN number;
- receiving an authentication response with cardholder credentials from the cardholder's mobile device; and
- validating the cardholder credentials.
- 20 6. The method of claim 1, further comprising, subsequent to transmitting the payment authorization request to an Acquirer FI Server computer:
- receiving, by the Proxy Service Manager Server computer, a payment authorization denied message; and
- transmitting the payment authorization denied message to a merchant device.

25

7. The method of claim 1, further comprising, prior to receiving the AAV token:
receiving, by the Proxy Service Manager Server computer, an authentication
failed message from the Authentication Service Manager Server computer; and
transmitting a cardholder authentication failure message to a merchant device.

5

8. The method of claim 1, wherein the consumer authentication request comprises
one of an account identifier of a consumer and a pre-authorized token.

9. The method of claim 1, wherein receiving the consumer authentication request
10 further comprises receiving merchant identification information.

10. The method of claim 9, wherein transmitting the payment authorization request to
an Acquirer FI Server computer further comprises transmitting the merchant
identification information.

15

11. The method of claim 10, further comprising receiving a payment authorization
denied message based on the merchant identification information.

12. A remote payments assurance system, comprising:
a Proxy Service Manager Server computer;
an Authentication Service Manager Server computer operably connected to the
Proxy Service Manager Server computer;
an Acquirer Financial Institution Server computer in communication with the
Proxy Service Manager Server computer;

a payment network operably connected to the Acquirer Financial Institution Server computer; and

an Issuer financial institution server computer operably connected to the payment network;

wherein the Proxy Service Manager Server computer receives a consumer authentication request from a merchant device, transmits the consumer authentication request to the Authentication Service Manager Server computer, receives a non-repudiable accountholder authentication value (“AAV”) token, generates a payment authorization request that includes the AAV token, transmits the payment authorization request to an Acquirer financial institution (FI) Server computer, receives a payment authorization message, and transmits the payment authorization message to the merchant device to enable a merchant to complete a purchase transaction with a consumer.

- 10 | 13. A consumer authentication and payment authorization method, comprising:
- receiving, by a Proxy Service Manager Server computer from a merchant device, a consumer authentication request comprising a consumer identifier and a pre-authorization token obtained from a consumer mobile device;
- transmitting, by the Proxy Service Manager Server computer, the consumer authentication request to an Authentication Service Manager Server computer;
- receiving, by the Proxy Service Manager Server computer, a non-repudiable accountholder authentication value (“AAV”) token for transaction matching at an Issuer financial institution (FI);
- generating, by the Proxy Service Manager Server computer, a payment authorization request that includes the AAV token in a Universal Card Authentication Field;
- transmitting, by the Proxy Service Manager Server computer, the payment authorization request to an Acquirer financial institution (FI) Server computer;
- receiving, by the Proxy Service Manager Server computer, a payment authorization message signifying that the Issuer FI validated the AAV token; and
- 20 |

transmitting, by the Proxy Service Manager Server computer, the payment authorization message to the merchant device ~~to enable~~ing a merchant to complete a purchase transaction with a consumer.

5 14. The method of claim 13, further comprising, prior to transmitting the consumer authentication request, establishing a secure communications channel between the Proxy Service Manager Server computer and the Authentication Service Manager Server computer.

10 15. The method of claim 13, wherein the consumer authentication request comprises an alias or a surrogate factor.

16. The method of claim 13, further comprising, prior to receiving the AAV token:
receiving, by the Proxy Service Manager Server computer, an authentication
15 failure message; and
transmitting the authentication failure message to a merchant device.

17. The method of claim 13, further comprising, subsequent to transmitting the payment authorization request to an Acquirer FI Server computer:
20 receiving a payment authorization denied message; and
transmitting the payment authorization denied message to a merchant device.

18. The method of claim 1, wherein receiving the consumer authentication request further comprises receiving merchant identification information.

19. The method of claim 18, wherein transmitting the payment authorization request to an Acquirer FI Server computer further comprises transmitting the merchant identification information.
- 5 20. The method of claim 19, further comprising receiving a payment authorization denied message based on the merchant identification information.
21. A remote payments assurance system, comprising:
- a Proxy Service Manager Server computer;
 - an Authentication Service Manager Server computer operably connected to the Proxy Service Manager Server computer;
 - an Acquirer Financial Institution (FI) Server computer in communication with the Proxy Service Manager Server computer;
 - a payment network operably connected to the Acquirer Financial Institution Server computer; and
 - an Issuer financial institution server computer operably connected to the payment network;
- wherein the Proxy Service Manager Server computer receives a consumer authentication request comprising a consumer identifier and a pre-authorization token,
- 10 transmits the consumer authentication request to the Authentication Service Manager Server computer, receives a non-repudiable accountholder authentication value (“AAV”) token, generates a payment authorization request that includes the AAV token, transmits the payment authorization request to the Acquirer FI Server computer, receives a payment authorization message, and transmits the payment authorization message to the
- 15 merchant device to enable a merchant to complete a purchase transaction with a consumer.

22. A consumer authentication method, comprising:
- receiving, by an Authentication Service Manager Server computer from a Proxy Service Manager computer, a consumer identifier;
- matching, by the Authentication Service Manager Server computer, the consumer identifier to data stored in a database;
- transmitting, by the Authentication Service Manager Server computer, a challenge/response request to a consumer device;
- receiving, by the Authentication Service Manager Server computer, a correct response to the challenge/response request from the consumer device;
- generating, by the Authentication Service Manager Server computer, a unique and non-repudiable AAV token; and
- transmitting, by the Authentication Service Manager Server computer, the non-repudiable AAV token to a Proxy Service Manager Server computer.
23. The method of claim 22, wherein matching the consumer identifier to data stored in a database further comprises retrieving a MS-ISDN number from a database storing consumer mobile device data.
24. The method of claim 23, wherein transmitting the challenge/response request comprises transmitting the challenge/response request to the MS-ISDN number.
25. The method of claim 22, further comprising, subsequent to receiving the consumer identifier:
- failing to match the consumer identifier to data stored in the database; and
- transmitting an authentication failure message to the Proxy Service Manager Server computer.
26. The method of claim 22, wherein the consumer identifier comprises one of an alias or a surrogate factor.

27. A remote payments assurance system, comprising:
- a Proxy Service Manager Server computer;
 - an Authentication Service Manager Server computer operably connected to the Proxy Service Manager Server computer;
 - 5 an Acquirer Financial Institution (FI) Server computer in communication with the Proxy Service Manager Server computer;
 - a payment network operably connected to the Acquirer FI Server computer; and
 - an Issuer FI server computer operably connected to the payment network;
- wherein the Authentication Service Manager Server computer receives a
- 10 consumer identifier, matches the consumer identifier to data stored in a database, transmits a challenge/response request to a consumer device, receives a correct response from the consumer device, generates a non-repudiable AAV token, and transmits the non-repudiable AAV token to the Proxy Service Manager Server computer.