

CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:
 - receiving a payment request associated with a customer, wherein the payment request is associated with an end agent that requires a payment associated with the customer, and wherein information used to access the payment is not directly accessible by the end agent;
 - transmitting an authorization request to obtain authorization for the payment, wherein when the authorization request is received at a computing device associated with the customer, the authorization request is used to prompt the customer for authorization data and the information used to access the payment;
 - receiving the authorization data and the information;
 - using the authorization data and the information to obtain the payment, wherein when the authorization data and the information are received at a processing service, the processing service uses the authorization data and the information to retrieve the payment; and
 - providing a transaction code, wherein when the transaction code is received by the end agent, the end agent uses the transaction code to obtain the payment without directly accessing the information.
2. The computer-implemented method of claim 1, wherein the payment request is received as a result of a determination that the computing device associated with the customer is capable of providing the authorization data using rich messaging.
3. The computer-implemented method of claim 1, wherein the information specifies a payment method.
4. The computer-implemented method of claim 1, wherein the authorization data includes biometric information associated with the customer.

5. The computer-implemented method of claim 1, further comprising providing a digital receipt corresponding to the transaction, wherein when the digital receipt is received at the computing device associated with the customer, the digital receipt is presented to the customer.
6. The computer-implemented method of claim 1, wherein the authorization request is encrypted using a cryptographic key, wherein the authorization request is decryptable by the computing device associated with the customer.
7. The computer-implemented method of claim 1, wherein:
the authorization data and the information is encrypted using a cryptographic key of the computing device associated with the customer; and
the method further comprises decrypting the authorization data and the information.
8. A system, comprising:
one or more processors; and
memory storing thereon instructions that, as a result of being executed by the one or more processors, cause the system to:
receive a payment request associated with a customer, wherein the payment request is associated with an end agent that requires a payment associated with the customer, and wherein information used to access the payment is not directly accessible by the end agent;
transmit an authorization request to obtain authorization for the payment, wherein when the authorization request is received at a computing device associated with the customer, the authorization request is used to prompt the customer for authorization data and the information used to access the payment;
receive the authorization data and the information;
use the authorization data and the information to obtain the payment, wherein when the authorization data and the information are received at a processing service, the processing service uses the authorization data and the information to retrieve the payment; and

provide a transaction code, wherein when the transaction code is received by the end agent, the end agent uses the transaction code to obtain the payment without directly accessing the information.

9. The system of claim 8, wherein the instructions further cause the system to:
transmit a query to obtain configuration information of the computing device; and
use the configuration information of the computing device to determine that the computing device is capable of providing the authorization data using rich messaging.
10. The system of claim 8, wherein the information specifies a payment method.
11. The system of claim 8, wherein the authorization request is encrypted using a cryptographic key, wherein the second request is decryptable by the computing device associated with the customer.
12. The system of claim 8, wherein the instructions further cause the system to transmit a digital receipt corresponding to the transaction, wherein when the digital receipt is received at the computing device associated with the customer, the digital receipt is presented to the customer.
13. The system of claim 8, wherein the authorization data includes biometric information associated with the customer.
14. The system of claim 8, wherein the communications session is a voice call between the customer and the agent.
15. A non-transitory, computer-readable storage medium storing thereon executable instructions that, as a result of being executed by one or more processors of a computer system, cause the computer system to:

receive a payment request associated with a customer, wherein the payment request is associated with an end agent that requires a payment associated with the customer, and wherein information used to access the payment is not directly accessible by the end agent;

transmit an authorization request to obtain authorization for the payment, wherein when the authorization request is received at a computing device associated with the customer, the authorization request is used to prompt the customer for authorization data and the information used to access the payment;

receive the authorization data and the information;

use the authorization data and the information to obtain the payment, wherein when the authorization data and the information are received at a processing service, the processing service uses the authorization data and the information to retrieve the payment; and

provide a transaction code, wherein when the transaction code is received by the end agent, the end agent uses the transaction code to obtain the payment without directly accessing the information.

16. The non-transitory, computer-readable medium of claim 15, wherein the payment request is received as a result of a determination that the computing device associated with the customer is capable of providing the authorization data using rich messaging.

17. The non-transitory, computer-readable storage medium of claim 15, wherein the authorization request is encrypted using a cryptographic key, wherein the authorization request is decryptable by the computing device associated with the customer.

18. The non-transitory, computer-readable storage medium of claim 15, wherein the executable instructions further cause the computer system to provide a digital receipt corresponding to the transaction, wherein when the digital receipt is received at the computing device associated with the customer, the digital receipt is presented to the customer.

19. The non-transitory, computer-readable storage medium of claim 15, wherein the authorization data includes biometric information associated with the customer.

20. The non-transitory, computer-readable storage medium of claim 15, wherein the authorization data includes biometric information associated with the customer.