００へ送信する。

【００９４】

これにより、決済端末１００にネットワークデバイスを設けなくても、携帯端末２００を経由して決済端末１００と決済サーバ３００との間で決済データの送受信ができる。また、暗号化された決済データが送受信されるので、携帯端末２００において、暗号化された情報（例えば、端末ＩＤや決済金額）の改ざんを防止できる。従って、決済サーバと通信を行う専用のネットワークデバイスを有しない決済端末１００を利用して、安全かつ汎用的な決済方法を実現できる。更に、以下のような副次的な効果も奏される。

【００９５】

まず、決済端末１００にネットワークデバイスを設けないことにより、部品点数が減るので、決済端末１００のコストダウンを図れる。また、ネットワークデバイスを設けることによるプログラムコードの増加を防止でき、ソフトウェアの開発費を抑制できる。

【００９６】

また、決済端末１００の機能を単純化できるので、新しいサービスを導入する場合の設定作業を軽減できる。また、内部設定を変更する必要も無くなるので、決済端末１００の長期利用も可能になり、メンテナンスコストも低減できる。また、決済端末１００のメモリ量を制約としないので、将来にリッチかつ複雑なサービスが導入された場合にも対応しやすくなる。

【００９７】

また、購入者が決済端末１００で決済をする場合に、決済端末１００が設置される店舗への信用が１つの不安要素となる。例えば、出店のような数日間限りの店舗にて決済する場合には、クレジットカードを渡すことは購入者の心理的に難しい。これに対して、第１の実施形態に場合には、決済サーバ３００との接続は携帯端末２００が行うため、信頼したシステム内で決済処理を実現できる。

【００９８】

＜２．第２の実施形態＞

図１１を参照しながら、本開示の第２の実施形態に係る決済処理システム２０の概要について説明する。図１１は、本開示の第２の実施形態に係る決済処理システム２０の概要を説明するための図である。

【００９９】

第２の実施形態に係る決済処理システム２０は、前述した第１の実施形態に係る決済処理システム１０と同様な決済処理を行う。決済処理システム２０は、図１１に示すように、決済端末１００と、携帯端末２００と、決済サーバ３００と、ネットワーク４００と、を有する。以下では、第１の実施形態と同様な構成については、説明を省略する。

【０１００】

第１の実施形態ではサービスＩＤバリュー３５０（図１）が決済サーバ３００に接続されたデータベースに接続されていることとしたが、第２の実施形態では、携帯端末２００がサービスＩＤバリュー２０４を有する。すなわち、携帯端末２００が、決済可能なサービスのバリューを記憶するバリュー記憶部を有する。このため、決済サーバ３００は、携帯端末２００を経由して決済端末１００から受信した決済データのサービスＩＤに対応する、携帯端末２００に格納されたサービスＩＤバリュー２０４に対して、決済処理を実行する。このため、予め携帯端末２００に登録されたバリューに対してのみ決済処理が行われ、予期せぬバリューに対して決済処理が行わることを防止できる。

【０１０１】

第２の実施形態に係る決済処理システム２０においても、決済端末１００と決済サーバ３００との間で、携帯端末２００を経由して決済データを送受信する。このため、決済端末１００にネットワークデバイスを設けなくても、携帯端末２００を経由して決済端末１００と決済サーバ３００との間で決済データの送受信ができる。また、暗号化された決済データが送受信されるので、暗号化された情報の改ざんを防止できる。従って、決済

Petitioner Exhibit 1002-0930

かつ汎用的な決済方法を実現できる。

【０１０２】

＜３．第３の実施形態＞

図１２を参照しながら、本開示の第３の実施形態に係る決済処理システム３０の概要について説明する。図１１は、本開示の第３の実施形態に係る決済処理システム３０の概要を説明するための図である。

【０１０３】

第３の実施形態に係る決済処理システム３０は、前述した第１の実施形態に係る決済処理システム１０と同様な決済処理を行う。決済処理システム３０は、図１２に示すように、決済端末１００と、携帯端末２００と、決済サーバ３００と、ネットワーク４００と、ＩＣカード５００と、を有する。以下では、第１の実施形態と同様な構成については、説明を省略する。

【０１０４】

第１の実施形態ではサービスＩＤバリュー３５０（図１）が決済サーバ３００に接続されたデータベースに接続されていることとしたが、第３の実施形態では、ＩＣカード５００がサービスＩＤバリュー５１０を有する。すなわち、ＩＣカード５００が、決済可能なサービスのバリューを記憶するバリュー記憶部を有する。このため、決済サーバ３００は、携帯端末２００を経由して決済端末１００から受信した決済データのサービスＩＤに対応する、ＩＣカード５００に格納されたサービスＩＤバリュー５１０に対して、決済処理を実行する。このため、ユーザが所望のバリューを記憶したＩＣカード５００と携帯端末２００と通信させるだけで、多様なバリューに対する決済処理が可能となる。

【０１０５】

ＩＣカード５００は、携帯端末２００と近距離通信（非接触通信）を行う。このため、携帯端末２００は、リーダ／ライタ機能を有する。なお、上記では、ＩＣカード５００が携帯端末２００に対して非接触通信を行うこととしたが、これに限定されない。例えば、ＩＣカード５００は携帯端末２００と接触通信を行うこととしても良い。また、ＩＣカード５００を例に挙げて説明したが、これに限定されず、サービスＩＤバリューを格納する機能を有する通信装置であれば形態を問わない。

【０１０６】

第３の実施形態に係る決済処理システム２０においても、決済端末１００と決済サーバ３００との間で、携帯端末２００を経由して決済データを送受信する。このため、決済端末１００にネットワークデバイスを設けなくても、携帯端末２００を経由して決済端末１００と決済サーバ３００との間で決済データの送受信ができる。また、暗号化された決済データが送受信されるので、暗号化された情報の改ざんを防止できる。従って、決済サーバと通信を行う専用のネットワークデバイスを有しない決済端末１００を利用して、安全かつ汎用的な決済方法を実現できる。

【０１０７】

＜４．ハードウェア構成例＞

上述した第１～第３の実施形態に係る決済処理システム１０、２０、３０による決済処理は、決済端末１００、携帯端末２００、及び決済サーバ３００が備えるハードウェア構成とソフトウェアとが協働することにより実現される。そして、決済端末１００、携帯端末２００、及び決済サーバ３００のハードウェア構成は同様であるので、以下では、図１３を参照しながら、携帯端末２００のハードウェア構成の一例について説明する。

【０１０８】

図１３は、第１～第３の実施形態に係る携帯端末２００のハードウェア構成の一例を示すブロック図である。図１３に示すように、携帯端末２００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）２６２と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）２６４と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２６６と、を有する。また、携帯端末２００は、入力装置２６８と、出力装置２７０と、[illegible]

Petitioner Exhibit 1002-0021

【０１０９】
ＣＰＵ２６２は、演算処理装置および制御装置として機能し、各種プログラムに従って携帯端末２００内の動作全般を制御する。また、ＣＰＵ２６２は、マイクロプロセッサであってもよい。ＲＯＭ２６４は、ＣＰＵ２６２が使用するプログラムや演算パラメータ等を記憶する。ＲＡＭ２６６は、ＣＰＵ２６２の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を一時記憶する。これらはＣＰＵバスなどから構成されるホストバスにより相互に接続されている。

【０１１０】
入力装置２６８は、マウス、キーボード、タッチパネル、ボタン、マイクロフォン、スイッチおよびレバーなどユーザが情報を入力するための入力手段と、ユーザによる入力に基づいて入力信号を生成し、ＣＰＵ２６２に出力する入力制御回路などから構成されている。携帯端末２００のユーザは、入力装置２６８を操作することにより、携帯端末２００に対して各種のデータを入力したり処理動作を指示したりすることができる。

【０１１１】
出力装置２７０は、例えば、液晶ディスプレイ（ＬＣＤ）装置、ＯＬＥＤ（Ｏｒｇａｎｉｃ Ｌｉｇｈｔ Ｅｍｉｔｔｉｎｇ Ｄｉｏｄｅ）装置およびランプなどの表示装置を含む。さらに、出力装置２７０は、スピーカおよびヘッドホンなどの音声出力装置を含む。例えば、表示装置は、生成された画像などを表示する。一方、音声出力装置は、音声データ等を音声に変換して出力する。

【０１１２】
ストレージ装置２７２は、携帯端末２００の記憶部の一例として構成されたデータ格納用の装置である。ストレージ装置２７２は、記憶媒体、記憶媒体にデータを記録する記録装置、記憶媒体からデータを読み出す読出し装置および記憶媒体に記録されたデータを削除する削除装置などを含んでもよい。このストレージ装置２７２は、ＣＰＵ２６２が実行するプログラムや各種データを格納する。

【０１１３】
ドライブ２７４は、記憶媒体用リーダライタであり、携帯端末２００に内蔵、あるいは外付けされる。ドライブ２７４は、装着されている磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリ等のリムーバブル記憶媒体６００に記録されている情報を読み出して、ＲＡＭ２６６に出力する。また、ドライブ２７４は、リムーバブル記憶媒体６００に情報を書き込むこともできる。

【０１１４】
通信装置２７６は、例えば、ネットワーク４００に接続するための通信デバイス等で構成された通信インタフェースである。また、通信装置２７６は、無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）対応通信装置であっても、ＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）対応通信装置であっても、有線による通信を行うワイヤー通信装置であってもよい。

【０１１５】
近距離通信装置２７８は、外部装置と近距離通信（例えば、ＮＦＣ通信）を行う装置である。近距離通信装置２７８は、例えば、通信アンテナにより外部装置のリーダ／ライタから送信された搬送波を受信し、内臓のＩＣチップにおける処理の処理結果に基づく応答信号を送信する。通信アンテナは、例えば、所定のインダクタンスをもつコイル（インダクタ）と、所定の静電容量をもつキャパシタとからなる共振回路で構成される。ＩＣチップは、受信された搬送波に基づいて搬送波信号を復調して処理し、負荷変調により応答信号を通信アンテナから送信させる。

【０１１６】
以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更

Petitioner Exhibit 1002-0932

術的範囲に属するものと了解される。

【０１１７】

上記の実施形態では、通信装置としてスマートフォンを例に挙げて説明したが、これに限定されない。例えば、通信装置は、近距離通信と無線通信を有すれば、ＰＤＡ、ゲーム機、電子辞書、ノートパソコン等であっても良い。

【０１１８】

また、上記の実施形態では、近距離通信としてＮＦＣ（Near Field Communication）通信を例に挙げて説明したが、これに限定されない。例えば、近距離通信は、Bluetoothであっても良い。また、上記では、通信装置（携帯端末２００）が、決済サーバと無線通信を行うこととしたが、これに限定されない。例えば、通信装置（携帯端末２００）が、決済サーバと有線通信を行って、決済データを送受信しても良い。

【０１１９】

また、上記の実施形態のフローチャートに示されたステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的に又は個別的に実行される処理をも含む。また時系列的に処理されるステップでも、場合によっては適宜順序を変更することが可能であることは言うまでもない。

【０１２０】

本明細書において説明した情報処理装置による処理は、ソフトウェア、ハードウェア、及びソフトウェアとハードウェアとの組合せのいずれを用いて実現されてもよい。ソフトウェアを構成するプログラムは、例えば、各装置の内部又は外部に設けられる記憶媒体に予め格納される。そして、各プログラムは、例えば、実行時にＲＡＭ（Random Access Memory）に読み込まれ、ＣＰＵなどのプロセッサにより実行される。

【０１２１】

なお、以下のような構成も本開示の技術的範囲に属する。

（１）

決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理システムであって、

前記決済端末は、

前記決済金額情報を暗号化した第１決済データを生成する決済データ生成部と、

生成された前記第１決済データを、近距離通信により前記通信装置へ送信する端末通信部と、

を備え、

前記通信装置は、

前記近距離通信により前記決済端末から前記第１決済データを受信する第１装置通信部と、

前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する第２装置通信部と、

を備え、

前記決済サーバは、

前記ネットワークを介して前記通信装置から前記第２決済データを受信するサーバ通信部と、

前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行する決済処理部と、

を備え、

前記サーバ通信部は、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信し、

前記第１装置通信部は、前記第２装置通信部により前記決済サーバから受信した決済後の前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末

Petitioner Exhibit 1002-0933

決済処理システム。

（２）

前記通信装置は、前記第１装置通信部により受信した前記第１決済データを用いて、前記決済サーバへ送信する前記第２決済データを生成する装置データ処理部を更に備え、

前記第２装置通信部は、前記装置データ処理部により生成された前記第２決済データを前記決済サーバへ送信する、

前記（１）に記載の決済処理システム。

（３）

前記決済端末から前記通信装置へ送信される前記第１決済データには、決済可能な複数のサービスのリスト情報が暗号化されずに含まれ、

前記装置データ処理部は、前記リスト情報を、前記決済サーバによる決済対象の一のサービス情報に置換することで、前記第２決済データを生成する、

前記（２）に記載の決済処理システム。

（４）

前記装置データ処理部は、生成する前記第２決済データに、前記決済サーバで処理される装置付加情報を暗号化せずに付加し、

前記決済サーバは、前記通信装置から受信した前記第２決済データに基づく決済処理の際に、前記装置付加情報に対応する処理を行う、

前記（２）又は（３）に記載の決済処理システム。

（５）

前記通信装置は、前記第２装置通信部により受信した決済後の前記第３決済データを用いて、前記決済端末へ送信する前記第４決済データを生成する装置データ処理部を更に備え、

前記第１装置通信部は、前記装置データ処理部により生成された前記第４決済データを前記決済端末へ送信する、

前記（１）～（４）のいずれか１項に記載の決済処理システム。

（６）

前記装置データ処理部は、生成する前記第４決済データに、前記決済端末で処理される装置付加情報を暗号化せずに付加し、

前記決済端末は、前記通信装置から受信した前記第４決済データの前記装置付加情報に対応する処理を行う、

前記（５）に記載の決済処理システム。

（７）

前記決済サーバから前記通信装置へ送信される前記第３決済データには、前記通信装置で処理されるサーバ付加情報が暗号化せずに含まれ、

前記通信装置は、前記決済サーバから受信した前記第３決済データの前記サーバ付加情報に対応する処理を行う、

前記（１）～（６）のいずれか１項に記載の決済処理システム。

（８）

前記決済端末から前記通信装置へ送信される前記第１決済データには、前記通信装置で処理される端末付加情報が暗号化せずに含まれ、

前記通信装置は、前記決済端末から受信した前記第１決済データの前記端末付加情報に対応する処理を行う、

前記（１）～（７）のいずれか１項に記載の決済処理システム。

（９）

決済可能なサービスのバリューを記憶するバリュー記憶部が、前記決済サーバに接続され、

前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの[illegible]

Petitioner Exhibit 1002-0934

前記（１）～（８）のいずれか１項に記載の決済処理システム。

（１０）

決済可能なサービスのバリューを記憶するバリュー記憶部が、前記通信装置に設けられ、

前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの前記バリューに対して決済処理を行う、

前記（１）～（８）のいずれか１項に記載の決済処理システム。

（１１）

決済可能なサービスのバリューを記憶するバリュー記憶部が、前記通信装置と近距離通信する外部装置に設けられ、

前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの前記バリューに対して決済処理を行う、

前記（１）～（８）のいずれか１項に記載の決済処理システム。

（１２）

決済処理を実行する決済処理システムにおいて、通信装置を経由して決済サーバとの間で、少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う、前記決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末であって、

前記決済金額情報を暗号化した第１決済データを生成する決済データ生成部と、

生成された前記第１決済データを、近距離通信により前記通信装置へ送信する端末通信部と、

を備え、

前記端末通信部は、前記第１決済データに基づく第２決済データを前記通信装置から受信した前記決済サーバが前記第２決済データを復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データに基づく第４決済データを前記近距離通信により前記通信装置から受信する、

決済端末。

（１３）

決済処理を実行する決済処理システムにおいて、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバとの間で、少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う通信装置であって、

前記決済端末において前記決済金額情報を暗号化して生成された第１決済データを、近距離通信により前記決済端末から受信する第１装置通信部と、

前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する第２装置通信部と、

を備え、

前記第２装置通信部は、送信した前記第２決済データを前記決済サーバが復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記決済サーバから受信し、

前記第１装置通信部は、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信する、

通信装置。

（１４）

決済処理を実行する決済処理システムにおいて、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末との間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う決済サーバであって、

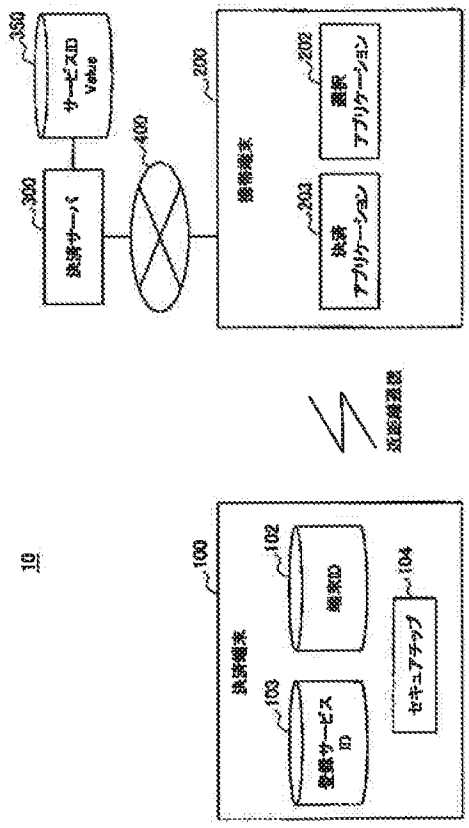
Petitioner Exhibit 1002-0935

く第２決済データを、ネットワークを介して前記通信装置から受信するサーバ通信部と、
前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行する決済処理部と、
を備え、
前記サーバ通信部は、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信する、
決済サーバ。
（１５）
決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理方法であって、
前記決済端末が、前記決済金額情報を暗号化した第１決済データを生成することと、
前記決済端末が、生成された前記第１決済データを、近距離通信により前記通信装置へ送信することと、
前記通信装置が、前記近距離通信により前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信することと、
前記決済サーバが、前記ネットワークを介して前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行することと、
前記決済サーバが、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信することと、
前記通信装置が、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信することと、
を含む決済処理方法。
（１６）
決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理方法であって、
前記通信装置が、前記決済端末において前記決済金額情報を暗号化して生成された第１決済データを、近距離通信により前記決済端末から受信することと、
前記通信装置が、前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信することと、
前記通信装置が、送信した前記第２決済データを前記決済サーバが復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記決済サーバから受信することと、
前記通信装置が、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信することと、
を含む決済処理方法。
【符号の説明】
【０１２２】
１０、２０、３０　決済処理システム
１００　決済端末
１１８　近距離通信部
１２０　決済データ生成部
１２２　署名検証部
２００　携帯端末
２１８　近距離通信部
２２０　無線通信部
２２２　決済データ処理部
３００　決済サーバ
３１０　無線通信部

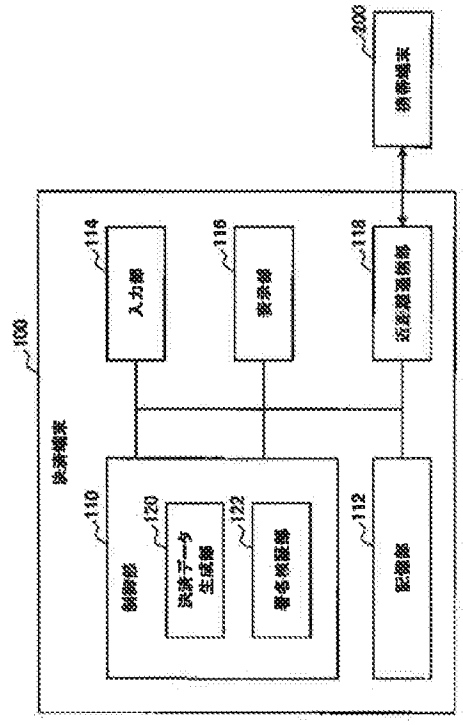
Petitioner Exhibit 1002-0936

３２０　署名検証部
３２２　決済処理部
３２４　決済データ処理部
４００　ネットワーク
５００　ＩＣカード

【図１】

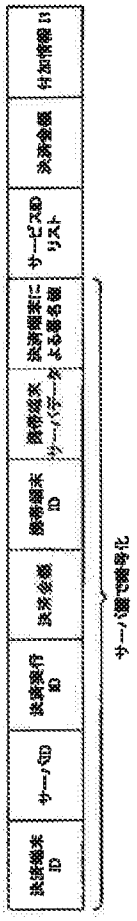


【図２】

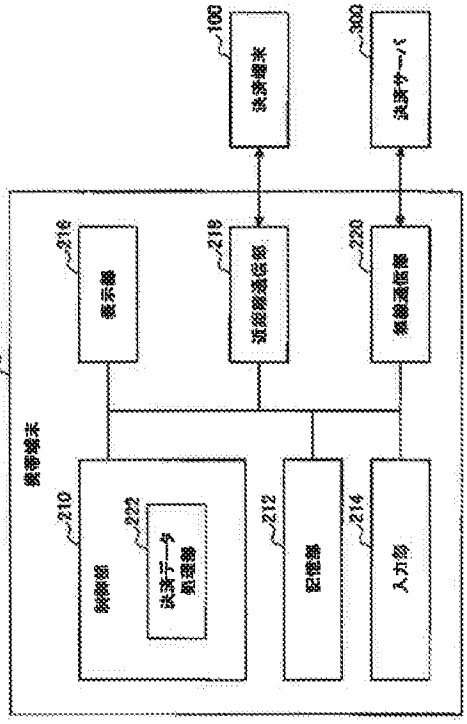


Petitioner Exhibit 1002-0937

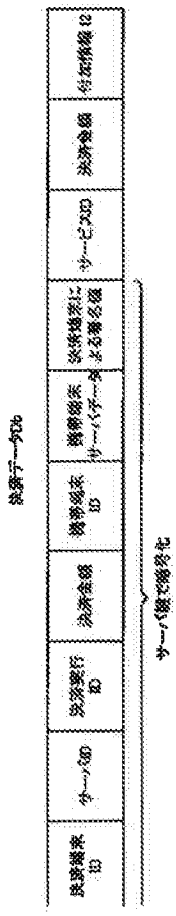
【図３】



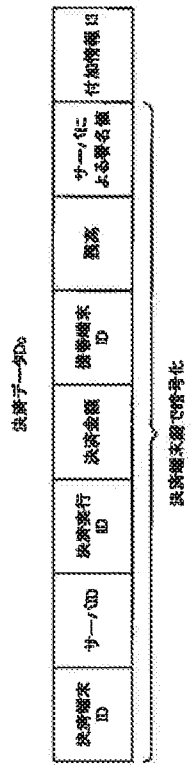
【図４】



【図５】

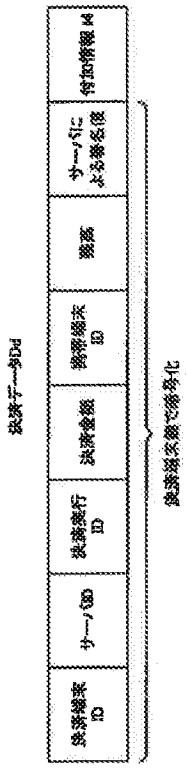


【図６】

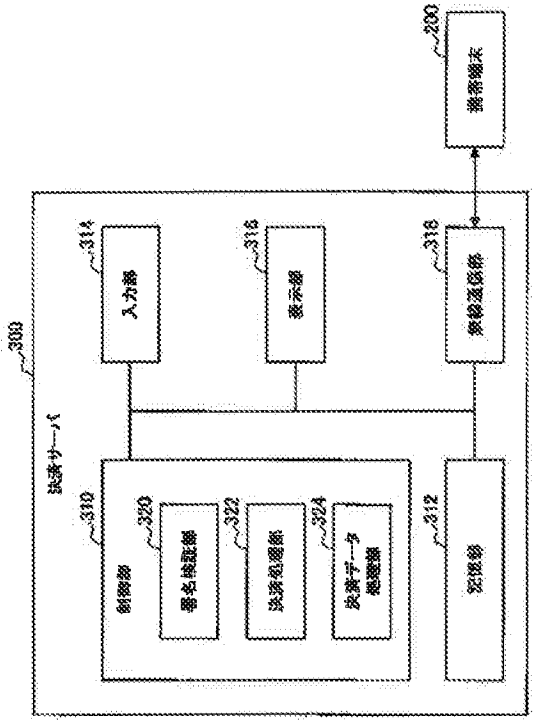


Petitioner Exhibit 1002-0938

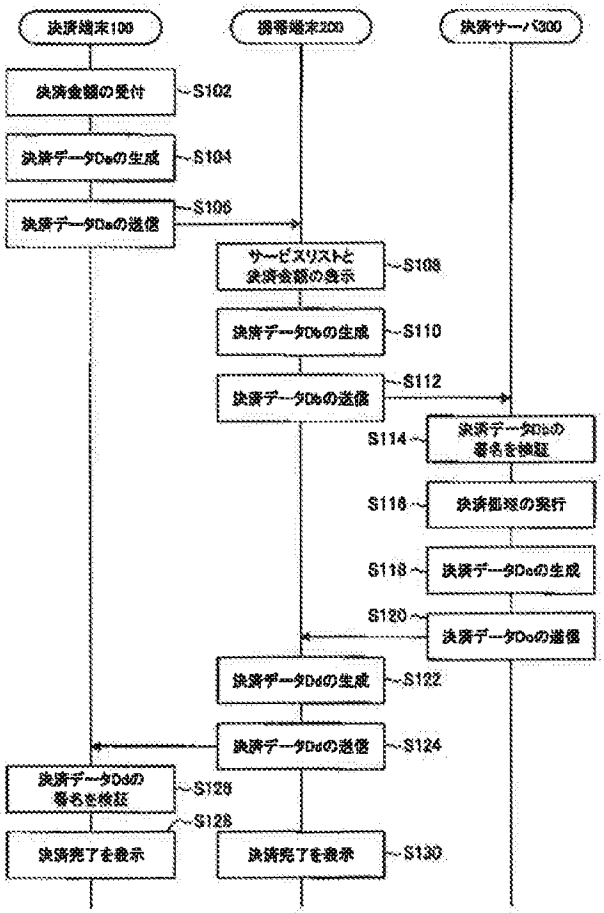
【図７】



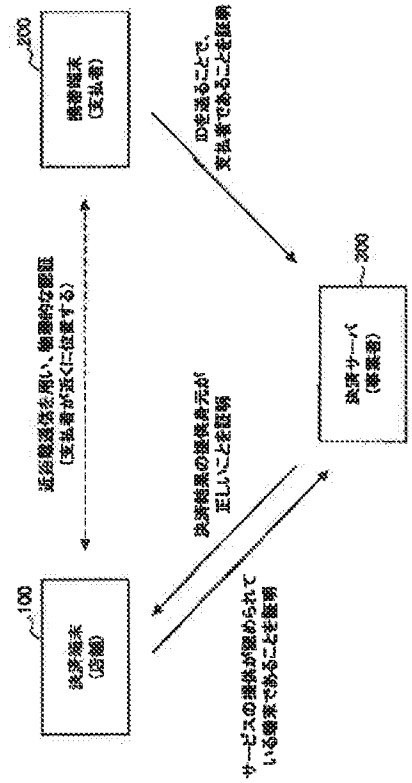
【図８】



【図９】

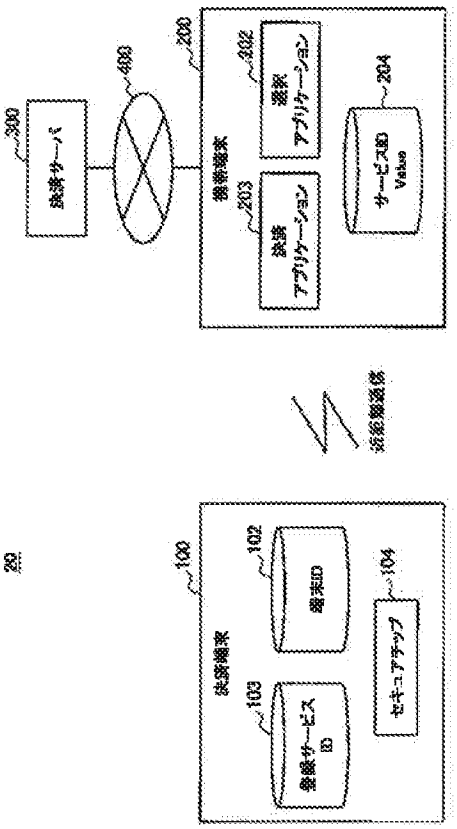


【図１０】

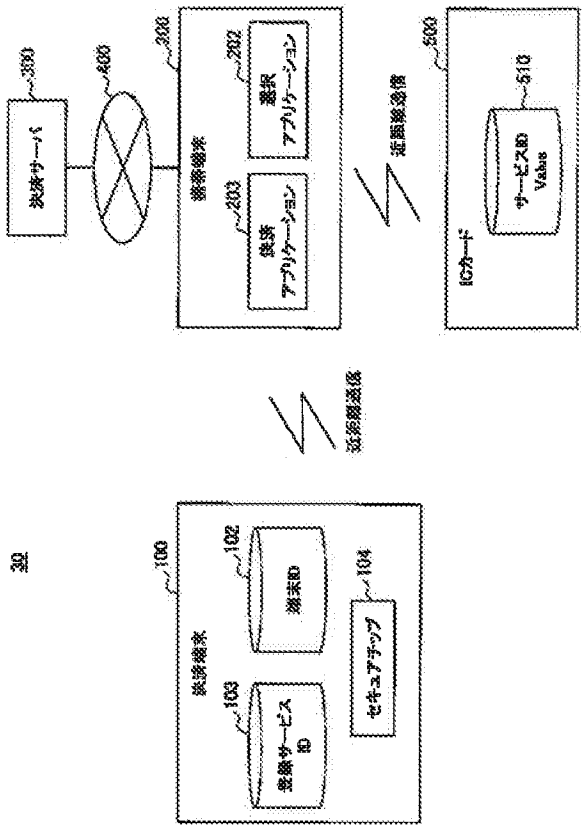


Petitioner Exhibit 1002-0939

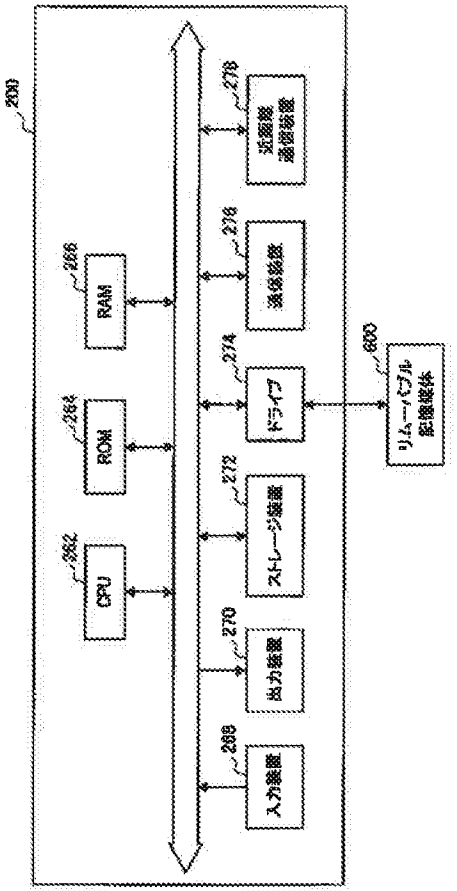
【図１１】



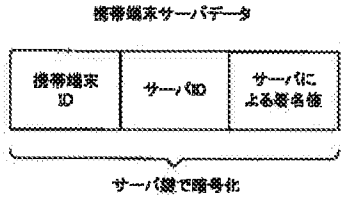
【図１２】



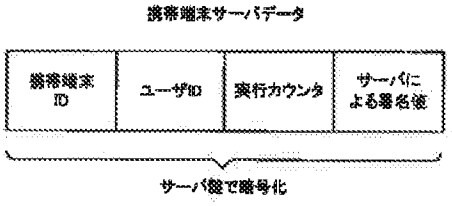
【図１３】



【図１４】



【図１５】



Petitioner Exhibit 1002-0940

【手続補正書】
【提出日】平成27年2月5日(2015.2.5)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理システムであって、
前記決済端末は、
前記決済金額情報を暗号化した第１決済データを生成する決済データ生成部と、
生成された前記第１決済データを、近距離通信により前記通信装置へ送信する端末通信部と、
を備え、
前記通信装置は、
前記近距離通信により前記決済端末から前記第１決済データを受信する第１装置通信部と、
前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する第２装置通信部と、
を備え、
前記決済サーバは、
前記ネットワークを介して前記通信装置から前記第２決済データを受信するサーバ通信部と、
前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行する決済処理部と、
を備え、
前記サーバ通信部は、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信し、
前記第１装置通信部は、前記第２装置通信部により前記決済サーバから受信した決済後の前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信する、
決済処理システム。
【請求項２】
前記通信装置は、前記第１装置通信部により受信した前記第１決済データを用いて、前記決済サーバへ送信する前記第２決済データを生成する装置データ処理部を更に備え、
前記第２装置通信部は、前記装置データ処理部により生成された前記第２決済データを前記決済サーバへ送信する、
請求項１に記載の決済処理システム。
【請求項３】
前記決済端末から前記通信装置へ送信される前記第１決済データには、決済可能な複数のサービスのリスト情報が暗号化されずに含まれ、
前記装置データ処理部は、前記リスト情報を、前記決済サーバによる決済対象の一のサービス情報に置換することで、前記第２決済データを生成する、
請求項２に記載の決済処理システム。
【請求項４】
前記装置データ処理部は、生成する前記第２決済データに、前記決済端末の識別

Petitioner Exhibit 1002-0941

前記決済サーバは、前記通信装置から受信した前記第２決済データに基づく決済処理の際に、前記装置付加情報に対応する処理を行う、
請求項２又は３に記載の決済処理システム。
【請求項５】
前記通信装置は、前記第２装置通信部により受信した決済後の前記第３決済データを用いて、前記決済端末へ送信する前記第４決済データを生成する装置データ処理部を更に備え、
前記第１装置通信部は、前記装置データ処理部により生成された前記第４決済データを前記決済端末へ送信する、
請求項１～４のいずれか１項に記載の決済処理システム。
【請求項６】
前記装置データ処理部は、生成する前記第４決済データに、前記決済端末で処理される装置付加情報を暗号化せずに付加し、
前記決済端末は、前記通信装置から受信した前記第４決済データの前記装置付加情報に対応する処理を行う、
請求項５に記載の決済処理システム。
【請求項７】
前記決済サーバから前記通信装置へ送信される前記第３決済データには、前記通信装置で処理されるサーバ付加情報が暗号化せずに含まれ、
前記通信装置は、前記決済サーバから受信した前記第３決済データの前記サーバ付加情報に対応する処理を行う、
請求項１～６のいずれか１項に記載の決済処理システム。
【請求項８】
前記決済端末から前記通信装置へ送信される前記第１決済データには、前記通信装置で処理される端末付加情報が暗号化せずに含まれ、
前記通信装置は、前記決済端末から受信した前記第１決済データの前記端末付加情報に対応する処理を行う、
請求項１～７のいずれか１項に記載の決済処理システム。
【請求項９】
決済可能なサービスのバリューを記憶するバリュー記憶部が、前記決済サーバに接続され、
前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの前記バリューに対して決済処理を行う、
請求項１～８のいずれか１項に記載の決済処理システム。
【請求項１０】
決済可能なサービスのバリューを記憶するバリュー記憶部が、前記通信装置に設けられ、
前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの前記バリューに対して決済処理を行う、
請求項１～８のいずれか１項に記載の決済処理システム。
【請求項１１】
決済可能なサービスのバリューを記憶するバリュー記憶部が、前記通信装置と近距離通信する外部装置に設けられ、
前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの前記バリューに対して決済処理を行う、
請求項１～８のいずれか１項に記載の決済処理システム。

Petitioner Exhibit 1002-0942

決済処理を実行する決済処理システムにおいて、通信装置を経由して決済サーバとの間で、少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う、前記決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末であって、

前記決済金額情報を暗号化した第１決済データを生成する決済データ生成部と、

生成された前記第１決済データを、近距離通信により前記通信装置へ送信する端末通信部と、

を備え、

前記端末通信部は、前記第１決済データに基づく第２決済データを前記通信装置から受信した前記決済サーバが前記第２決済データを復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データに基づく第４決済データを前記近距離通信により前記通信装置から受信する、

決済端末。

【請求項１３】

決済処理を実行する決済処理システムにおいて、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバとの間で、少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う通信装置であって、

前記決済端末において前記決済金額情報を暗号化して生成された第１決済データを、近距離通信により前記決済端末から受信する第１装置通信部と、

前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する第２装置通信部と、

を備え、

前記第２装置通信部は、送信した前記第２決済データを前記決済サーバが復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記決済サーバから受信し、

前記第１装置通信部は、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信する、

通信装置。

【請求項１４】

決済処理を実行する決済処理システムにおいて、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末との間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う決済サーバであって、

前記決済端末において前記決済金額情報を暗号化して生成された第１決済データに基づく第２決済データを、ネットワークを介して前記通信装置から受信するサーバ通信部と、

前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行する決済処理部と、

を備え、

前記サーバ通信部は、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信する、

決済サーバ。

【請求項１５】

決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理方法であって、

前記決済端末が、前記決済金額情報を暗号化した第１決済データを生成することと、

前記決済端末が、生成された前記第１決済データを、近距離通信により前記通信装置へ送信することと、

前記通信装置が、前記近距離通信により前記決済端末から受信した前記第１決済データ

Petitioner Exhibit 1002-0943

前記決済サーバが、前記ネットワークを介して前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行することと、
前記決済サーバが、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信することと、
前記通信装置が、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信することと、
を含む決済処理方法。
【請求項１６】
決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理方法であって、
前記通信装置が、前記決済端末において前記決済金額情報を暗号化して生成された第１決済データを、近距離通信により前記決済端末から受信することと、
前記通信装置が、前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信することと、
前記通信装置が、送信した前記第２決済データを前記決済サーバが復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記決済サーバから受信することと、
前記通信装置が、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信することと、
を含む決済処理方法。

Petitioner Exhibit 1002-0944

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/053827

A. CLASSIFICATION OF SUBJECT MATTER
G06Q20/40(2012.01)i, *G06Q20/00*(2012.01)i, *G07G1/12*(2006.01)i, *G07G1/14*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q20/40, G06Q20/00, G07G1/12, G07G1/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2013
Kokai Jitsuyo Shinan Koho	1971-2013	Toroku Jitsuyo Shinan Koho	1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2007-241448 A (Panasonic Corp.), 20 September 2007 (20.09.2007), 0015, 0034 to 0048, 0066 to 0067, 0070 to 0072 (Family: none)	1-16
Y	JP 2004-185253 A (Mitsubishi Electric Corp.), 02 July 2004 (02.07.2004), 0016 to 0024 (Family: none)	1-16
Y	JP 2011-118789 A (Hitachi, Ltd.), 16 June 2011 (16.06.2011), 0008, 0048 to 0053, 0056 to 0059, 0070 to 0077 (Family: none)	1-16

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 March, 2013 (06.03.13)	19 March, 2013 (19.03.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

Petitioner Exhibit 1002-0945

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/053827

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2007-281948 A (NTT Docomo Inc.), 25 October 2007 (25.10.2007), 0062 to 0063 & US 2009/0287760 A1 & EP 2006768 A2 & WO 2007/116993 A1 & KR 10-2008-0098551 A & CN 101416159 A & KR 10-0971896 B1	3
A	JP 2003-051780 A (Toshiba Tec Corp.), 21 February 2003 (21.02.2003), 0016 to 0026; fig. 3 (Family: none)	1-16

Form PCT/ISA/210 (continuation of second sheet) (July 2009)

Petitioner Exhibit 1002-0946

国際調査報告

国際出願番号 PCT/JP2013/053827

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06Q20/40(2012.01)i, G06Q20/00(2012.01)i, G07G1/12(2006.01)i, G07G1/14(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06Q20/40, G06Q20/00, G07G1/12, G07G1/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2013年
日本国実用新案登録公報	1996－2013年
日本国登録実用新案公報	1994－2013年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2007-241448 A（パナソニック株式会社）2007.09.20, 0015、0034－0048、0066－0067、0070－0072（ファミリーなし）	1－16
Y	JP 2004-185253 A（三菱電機株式会社）2004.07.02, 0016－0024（ファミリーなし）	1－16
Y	JP 2011-118789 A（株式会社日立製作所）2011.06.16, 0008、0048－0053、0056－0059、0070－0077（ファミリーなし）	1－16

☑ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 06. 03. 2013	国際調査報告の発送日 19. 03. 2013
国際調査機関の名称及びあて先 日本国特許庁（ISA/JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 塩田 勝彦 SL 4533 電話番号 03－3581－1101 内線 3562

様式PCT/ISA/210（第2ページ）（2009年7月）

Petitioner Exhibit 1002-0947

国際調査報告 国際出願番号 PCT/JP2013/053827

C（続き）. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2007-281948 A (株式会社エヌ・ティ・ティ・ドコモ) 2007.10.25, ００６２－００６３ & US 2009/0287760 A1 & EP 2006768 A2 & WO 2007/116993 A1 & KR 10-2008-0098551 A & CN 101416159 A & KR 10-0971896 B1	3
A	JP 2003-051780 A (東芝テック株式会社) 2003.02.21, ００１６－００２６、第３図 (ファミリーなし)	１－１６

様式PCT/ISA/210（第2ページの続き）（２００９年７月）

Petitioner Exhibit 1002-0948

フロントページの続き

(51)Int.Cl.	F I		テーマコード（参考）
	G07F 7/08	L	

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC

（特許庁注：以下のものは登録商標）
1．ＦＡＣＥＢＯＯＫ
2．ＢＬＵＥＴＯＯＴＨ

Ｆターム(参考) 3E044 AA20 BA10 CA10 CB02 DC06 DE01
3E142 EA04 FA09 FA10 FA25 GA16 HA01 HA03 JA03 JA04
5L055 AA53 AA75

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。

Petitioner Exhibit 1002-0949

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2013 (28.11.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/177416 A2

(51) International Patent Classification:
G06Q 20/32 (2012.01)

(21) International Application Number:
PCT/US2013/042455

(22) International Filing Date:
23 May 2013 (23.05.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/651,276	24 May 2012 (24.05.2012)	US
61/772,260	4 March 2013 (04.03.2013)	US
61/794,545	15 March 2013 (15.03.2013)	US

(71) Applicant: **JVL VENTURES, LLC** [US/US]; 230 Park Avenue, Suite 2829, New York, NY 10169-0005 (US).

(72) Inventors: **BUSH, Larry, L.**; 13637 N. 12th Way, Phoenix, AZ 85022 (US). **TOMCZAK, Christopher, J.**; 1319 Lochness Drive, Allen, TX 75013 (US).

(74) Agents: **BERSCHADSKY, Jonathan** et al.; Fitzpatrick, Cella, Harper & Scinto, 1290 Avenue Of The Americas, New York, NY 10104-3800 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

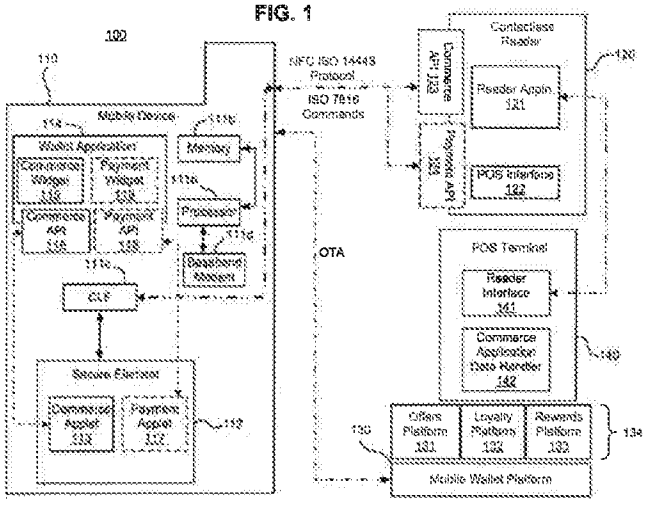
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING A CONTACTLESS PROTOCOL

FIG. 1



(57) Abstract: Systems, methods and computer program products are provided for managing contactless transactions. A first tap is performed when a system is placed within a predetermined proximity to a payment terminal. A first select command including an AID corresponding to a first application is received from the payment terminal. A first response based on the first select command is transmitted to the payment terminal. A data request including information indicating [illegible] is received from the payment terminal. A second response based on the data request and including transaction data is transmitted to the payment terminal.

Petitioner Exhibit 1002-0950

WO 2013/177416 A2

SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING A CONTACTLESS PROTOCOL

BACKGROUND

Field

[0001] Example aspects described herein relate generally to contactless protocols and more particularly to systems, methods, and computer program products for providing a contactless protocol allowing interoperation between mobile devices, near field communication (NFC) readers, and point of sale (POS) systems.

Related Art

[0002] NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are positioned within a certain proximity, generally less than ten centimeters apart. One use of such NFC technology is for making contactless transactions, including those for payment,

Petitioner Exhibit 1002-0951

access and ticketing. For example, an NFC-enabled mobile device can be provisioned with a payment application and payment account information (*i.e.*, credentials associated with a financial instrument such as credit or debit card) issued by a consumer's financial institution. Each payment application can store and manage multiple sets of commerce data associated with multiple merchants, manufacturers or brands on a secure element. The application and payment account information are typically encrypted and stored in a secure area in the mobile device. The mobile device can, in turn, use the NFC technology to communicate with NFC-enabled point of sale (POS) systems at attended locations such as stores and unattended locations such as vending machines. To pay, the consumer simply brings the mobile device to within approximately ten centimeters of a contactless payment-capable POS system and the transaction occurs. The process is typically the same as that used by the contactless credit and debit cards.

[0003] Placing the mobile device or contactless credit or debit card near an NFC-enabled reader so that they can be communicatively coupled is sometimes referred to as a "wave" or "tap". An application for a mobile device that allows consumers to "tap to pay" at a NFC-enabled POS systems is generally referred to as a "wallet application" or "mobile wallet client application." An application related to payments is generally referred to as a "payment" application. Common contactless payment applications are facilitated using any of the following technologies: American Express® "ExpressPay," Discover® "ZIP," Mastercard® "PayPass" or Visa® "PayWave".

[0004] NFC can also be used to read information about products or receive special offers, loyalty or rewards information from, for example, NFC tags, smart posters or smart billboards. An application related to offers, loyalty and rewards is generally referred to herein as a "commerce" application.

[0005] One technical challenge associated with utilizing payment and commerce technologies cooperatively involves the ability to allow the same tap event that sends payment information to include additional information associated with merchant loyalty cards, offers, rewards, and the like. To this end, messaging technologies in existing NFC readers or NFC-enabled payment POS terminals

Petitioner Exhibit 1002-0952

stand to be upgraded to effectively support a messaging technology that retrieves and/or receives both payment credentials (using the aforementioned payment protocols) and additional commerce data (loyalty, offers, rewards, etc.) from mobile devices used to perform the transactions. Yet another technical challenge involves publishing commerce elements (*e.g.*, offers, loyalty card credentials, rewards, and the like) into a mobile device such that those commerce elements may, in turn, be presented as part of a typical POS transaction (*e.g.*, a purchase).

BRIEF DESCRIPTION

[0006] The example embodiments presented herein meet the above-identified needs by providing systems, methods and computer program products for providing a contactless protocol.

[0007] In one embodiment, a system for managing contactless transactions includes at least one memory operable to store commerce data and financial instrument data, and at least one processor coupled to the at least one memory. A first tap is performed, the first tap occurring when the system is placed within a predetermined proximity to a payment terminal. A first select command including an AID corresponding to a first application is received from the payment terminal. A first response based on the first select command is transmitted to the payment terminal. A data request including information indicating supported data types is received from the payment terminal. A second response based on the data request and including transaction data is transmitted to the payment terminal. The transaction data includes at least a portion of the commerce data stored in the at least one memory.

[0008] In another embodiment, a method for managing contactless transactions includes: performing a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal; receiving from the payment terminal a first select command including an AID corresponding to a first application; transmitting to the payment terminal a first response based on the first select command; receiving from the payment terminal a data request including information indicating supported data types; and transmitting to the payment terminal a second response based on the data request, the second

Petitioner Exhibit 1002-0953

response including transaction data. The transaction data includes at least a portion of commerce data stored in at least one memory.

[0009] In another embodiment, a non-transitory computer-readable medium has sequences of instructions stored thereon for causing one or more processors to: perform a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal; receive from the payment terminal a first select command including an AID corresponding to a first application; transmit to the payment terminal a first response based on the first select command; receive from the payment terminal a data request including information indicating supported data types; and transmit to the payment terminal a second response based on the data request, the second response including transaction data. The transaction data includes at least a portion of commerce data stored in at least one memory.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The features and advantages of the example embodiments of the invention presented herein will become more apparent from the detailed description set forth below when taken in conjunction with the following drawings.

[0011] FIG. 1 is a graphical representation of a platform architecture in accordance with an exemplary embodiment.

[0012] FIG. 2 illustrates a single tap timing diagram according to an exemplary embodiment.

[0013] FIG. 3 shows a timing diagram illustrating a commerce process flow including a double tap and post transaction data transmission according to an exemplary embodiment.

[0014] FIG. 4 shows a timing diagram illustrating a commerce process flow including a double tap, and post transaction data and payment transmissions according to an exemplary embodiment.

[0015] FIG. 5 illustrates an exemplary multi-block data flow according to an example embodiment.

[0016] FIG. 6 illustrates windows or screen shots generated by the graphical user interface for a wallet application in accordance with an example embodiment of the present invention.

[0017] FIG. 7 illustrates a flow diagram illustrating an exemplary instant offer implementation according to an embodiment of the present invention.

[0018] FIG. 8 is a collaboration diagram of functional modules deployed on a computer system in accordance with an example embodiment of the present invention.

DETAILED DESCRIPTION

[0019] The example embodiments presented herein are directed to systems, methods and computer program products for providing a contactless protocol, which are now described herein in terms of an example merchant transaction. This description is not intended to limit the application of the example embodiments presented herein. In fact, after reading the following description, it will be apparent to one skilled in the relevant art(s) how to implement the following example embodiments in alternative embodiments (*e.g.*, involving mass transit transactions requiring a wireless communications connection between a mass transit terminal and a mobile device).

[0020] The terms "application," "applet," "widget," and/or the plural form of these terms are used interchangeably herein to refer to an application (functioning independently or in conjunction with other applications) or set or subset of instructions or code, which when executed by one or more processors (*e.g.*, in a mobile device, card reader, terminal, point of sale (POS) system, or server) causes the processor(s) to perform specific tasks. For example, a wallet application can be used to conduct transaction- or interface-related functions such as storing, processing, accessing or transmitting financial, loyalty, offer, membership, or account data. A wallet application may also incorporate or interact with one or more payment applications, such as ExpressPay from American Express®, Discover® Network Zip^{SM}, MasterCard® PayPass™ and Visa payWave™ payment applets.

Petitioner Exhibit 1002-0955

[0021] Generally, commerce-related services are made available through a suite of applications available on several different platforms. The first application (or suite of applications) exists onboard a server within a mobile commerce (MoCom) platform. The MoCom platform is responsible for the management of consumer data, including loyalty accounts and offers. In addition, the MoCom platform serves as a campaign manager for offers, providing a remote data store for offers made available to the consumer via the available merchant portals within a wallet application.

[0022] A second application exist onboard a mobile device in the form of a wallet application. The wallet application provides the consumer's primary user interface (UI) and additional commerce application services through which the wallet application may access additional resources onboard a secure element (SE) of a mobile device.

[0023] A third application exists onboard a secure element of a mobile device in the form of JavaCard applet. This applet stores commerce-related data such as loyalty and offer data and provides an interface through which the data may be managed. The applet is accessible through the use of Application Protocol Data Unit (APDU) commands as defined in International Standards Organization (ISO) 7816-4.

[0024] The fourth application exists onboard an NFC-enabled reader (referred to herein simply as a "reader"). The reader can be either a stand-alone device or attached to (and managed by) a point of sale (POS) terminal. This application facilitates or provides access to the interface with a secure element on a mobile device, performing specific tasks that optimize the APDU command/data exchange tasks. For example, it includes the reading of loyalty or offer information following the placement of a mobile device in proximity of a reader (*i.e.*, a "tap").

[0025] A fifth application (or suite of applications) exists onboard a merchant POS system, including a POS terminal and any additional merchant-specific hardware/software. These applications manage the data related to payment/loyalty/offers/rewards received from a secure element on a mobile

device via a reader. In most cases, this data will then be forwarded to a corresponding MoCom or merchant specific platform(s).

[0026] FIG. 1 is a graphical representation of a platform architecture in accordance with an exemplary embodiment. As shown in FIG. 1, system 100 includes a mobile device 110 communicatively coupled to a contactless (*e.g.*, proximity or NFC) reader 120 and a mobile wallet platform 130. Reader 120 also is communicatively coupled to a POS terminal 140. POS terminal 140 may be within the same housing as reader 120. Alternatively, POS terminal 140 and reader 120 are communicatively coupled with each other but each of these components is housed separately.

[0027] Mobile device 110 may be, for example, a cellular phone or the like, and includes a processor 111a, memory 111b, a contactless frontend (CLF) 111c, a baseband modem 111d, and a user interface such as a display (not shown). Baseband modem 111d is a digital modem that is used for mobile network communications. CLF 111c is circuitry which handles the analog aspect of contactless or NFC communications and the communication protocol layers of a contactless transmission link. CLF 111c also is used to exchange data between reader 120 and a secure element (or SE) 112 contained in mobile device 110, for example, to execute contactless transactions.

[0028] Secure element 112 may be implemented as a Universal Integrated Circuit Card (UICC), embedded SE card, secure micro secure digital (microSD) card, and the like. Secure element 112 is generally considered secure because it is a self-contained system, including dedicated memory, and is protected by hardware and software hardening techniques that are verified by independent testing.

[0029] Secure element 112 includes (*e.g.*, stored thereon) one or more commerce applets 113. Each commerce applet 113 is associated with a commerce service and an account issued by a commerce service provider (SP). A service provider is a company, organization, entity, or the like, that provides services to customers or consumers. Examples of service providers include account-issuing entities such as banks, merchants, card associations, marketing companies, and transit authorities. A service may be an activity, capability, functionality, work, or use

Petitioner Exhibit 1002-0957

that is permitted or provided by a service provider, such as a payment service, credit, debit, checking, gift, offer or loyalty service, transit pass service, and the like.

[0030] A commerce service provider can provision (or have provisioned) onto secure element 112 one or more separate commerce applets 113. In addition, other independent service providers can provision (or have provisioned) onto secure element 112 their own commerce applet(s) 113. Generally, a commerce applet 113 stores both loyalty and offers related data, providing an APDU interface through which this data can be managed. Commerce applet 113 operates as a generic storage container, allowing multiple loyalty/offers services to share mechanisms (*e.g.*, secure element, mobile device) for loyalty/offer data management. If memory restrictions and performance requirements limit the amount of loyalty/offers data that can be stored on secure element 112, additional data can be stored in mobile device memory 111b and managed by the consumer via commerce widget 115. For example, any graphic images related to an offer can be stored in memory 111b in order to optimize secure element memory allocation. Loyalty/offers data management can be handled by the corresponding offer platform 131, loyalty platform 132, or rewards platform 133.

[0031] Commerce applet 113 includes a cached merchant data table enabling the storage/management of all data related to a given merchant. This allows the commerce data for a given merchant to be pre-loaded in secure element 112 or mobile device 110 by a wallet application. Exemplary commerce elements (and their corresponding tag values used during Tag Length Value (TLV) encoding) that are included in the cached merchant data table are defined below. This data is stored in a record oriented data buffer. In an exemplary embodiment, a merchant identifier (Merchant Identifier) is used as the key field for search/retrieval tasks. Optionally, an index (or hash table) may be created to improve performance.

[0032] One or more commerce applets 113 can be loaded onto the secure element 112, for example, during manufacture and/or configuration of the secure element 112 and may be personalized to enable its use to conduct commerce transactions. A commerce applet 113 interfaces with reader 120 via a commerce

Petitioner Exhibit 1002-0958

application programming interface (API) 123. In an exemplary embodiment, a commerce applet 113 is in the form of a JavaCard applet and is accessible through the use of APDU commands as defined in ISO 7816-4. Particularly, commerce applet 113 communicates commerce elements to reader 120 via secure element 112 using ISO 7816 commands over the NFC ISO 14443 protocol.

[0033] Secure element 112 can also include one or more payment applets 117 where each payment applet 117 is associated with a payment service and an account issued by a payment service provider. One or more payment applets 117 also can be loaded onto the secure element 112, for example, during manufacture and/or configuration of the secure element 112 and may be personalized to enable its use to conduct payment transactions. A payment applet 117 interfaces with reader 120 via API 124. In an exemplary embodiment, payment applet 117 is in the form of a JavaCard applet and is accessible through the use of APDU commands as defined in ISO 7816-4. Payment applet 113 also communicates payment elements to reader 120 via secure element 112 using ISO 7816 commands over the NFC ISO 14443 protocol.

[0034] It should be understood that other communications between the aforementioned devices may include communications with or through other intervening systems, hardware, and/or software, and such communications may include receiving, transferring, and/or managing data.

[0035] A wallet application 114 stored on mobile device 110 includes instructions which, when executed by the processor of the mobile device 110, cause the mobile device 110 to act as an instrument, for example, for processing transactions such as contactless commerce and/or payment transactions. Wallet application 114 communicates, through the use of APDU commands as defined in ISO 7816-4, with the commerce applet 113 via commerce API 116 and to payment applet 117 via payment API 118.

[0036] Commerce widget 115 is a component of the wallet application 114 that provides an interface for consumers to manage commerce elements (*e.g.*, loyalty card credentials, offers and rewards), for example, through interactions with the display or user interface of a mobile device. Commerce widget 115 maintains, for example, a master list of commerce elements present on the handset in a

Petitioner Exhibit 1002-0959

memory of the mobile device (*e.g.*, 111b). A subset of offers that have been identified as ready to be used are, in turn, moved to secure element 112 to be communicated to contactless reader 120 and POS terminal 140. Sensitive information, such as loyalty account identifiers can be stored on secure element 112.

[0037] Payment widget 119 is a component of the wallet application 114 that provides an interface for consumers to manage payment elements (*e.g.*, credit or debit card credentials), for example, through interactions with the display or user interface of a mobile device.

[0038] Reader 120 includes a reader commerce application 121 (referred to herein simply as a "reader application") and a POS interface 122. Reader 120 manages two interfaces: one interface is with the secure element 112 in the mobile device 110 and the other interface is with POS terminal 140 which includes a reader interface 141 and a commerce application data handler 142. The functionality of reader 120 is the same whether reader 120 is standalone and connected to a payments terminal or merchant POS, or is integrated therein. Contactless payment functionality is also contained in reader 120 but is not shown.

[0039] Mobile device 110 is further communicatively coupled to a mobile wallet platform 130, which in turn is communicatively coupled to offers platform 131, loyalty platform 132 and rewards platform 133. Collectively, offers platform 131, loyalty platform 132 and rewards platform 133 can be referred to as a mobile commerce (MoCom) platform 134 and are implemented on one or more servers, referred to herein individually and collectively as a MoCom server (now shown).

[0040] In one embodiment, a customer may use mobile device 110 to conduct a contactless transaction at a POS equipped with reader 120. The customer places the mobile device 110 within a predetermined required proximity of the contactless reader 120 (*i.e.*, taps) causing CLF 111c of the mobile device 110 to communicate with reader 120 using, for example, NFC ISO 14443 protocols. Reader 120 also communicates with wallet application 114, commerce applet

113, and/or payment applications on the mobile device 110 to execute contactless transactions.

[0041] A secure element employs a Proximity Payment System Environment (PPSE) that serves as a directory of available credentials currently stored in secure element 112. Each credential is assigned a corresponding application identifier (AID) associated with a payment application and stored in the PPSE. When an NFC enabled-mobile device containing secure element 112 is placed in the vicinity of an NFC-enabled contactless reader, the contactless reader reads the credential and completes the transaction. Before doing so, however, the reader is initialized.

[0042] On mobile device 110, PPSE is an application used to maintain a list of payment applications stored on secure element 112, and provides accessibility to each payment application stored on the mobile device 112 by making them visible or not visible (*i.e.*, accessible) to systems or devices.

Reader Initialization

[0043] Initialization of the reader 120 will now be described in more detail. In one embodiment, reader 120 implements a function referred to as an Entry Point Manager (EPM) to control which application in a mobile device is selected. In this embodiment, EPM controls whether reader 120 sends a command to mobile device 110 to select an application that performs a commerce transaction or a command that performs a payment transaction. A command to select a commerce application is referred to herein as "Select Commerce." A command to select a payment application is referred to herein as "PPSE Select."

[0044] EPM also controls the start mode for the reader 120 and subsequent application switching during a checkout process. EPM thus facilitates switching (at reader 120) between the Select Commerce command for a commerce transaction and the PPSE Select command for payment transactions.

Commencing a Commerce Transaction on a Reader

[0045] A reader can be configured to initiate a commerce transaction on a reader according to several modes, which are described below in further detail. In one mode, referred to as "auto start", reader application 121 is the default application

Petitioner Exhibit 1002-0961

on the reader 120. Being the default application allows reader application 121 to be available to the consumer as a first tap option (*i.e.*, upon an initial coupling communication between the mobile device 110 and contactless reader 120).

[0046] Another mode, referred to as "manual start," allows manual intervention to be used to initiate reader commerce application 121. Manual intervention can be in the form of a command from POS terminal 130 (*e.g.*, initiated by using a POS terminal interface) or from a consumer selecting a commerce application on a mobile device by using commerce widget 115.

[0047] Another mode, referred to as "payment with post transaction data," involves controlling how payments are handled in an activity stream. If a merchant supports the provisioning of post transaction data, for example, then payment and receipt of merchant data can be accomplished by the same tap event, such as after the final total for a transaction has been calculated.

[0048] Another mode is referred to as "payment first," The payment first option works in conjunction with the auto start mode and/or the manual start mode to initiate a PPSE Select command for payment and then a Select Commerce command to obtain commerce data (*e.g.*, loyalty data, offer data, reward data, and the like). Commerce data is interchangeably referred to herein as "commerce elements."

Auto Start Mode

[0049] Referring to FIG. 1, auto start mode provides commerce functionality on reader 120 at the beginning of a POS checkout process. When mobile device 110 taps reader 120, reader application 121 causes reader 120 to send a "Select Commerce" message to mobile device 110 including the AID corresponding to the commerce application to be used to execute a contactless transaction. If the message is accepted by mobile device 110 it sends a positive response message in return. Next, reader 120 sends mobile device 110 a "Get Commerce Data" command. The Get Commerce Data command contains merchant specific data that secure element 112 uses to perform a commerce transaction. Also, control passes to the mobile device 110 upon successful completion of the Get Commerce Data transaction. If reader 120 receives a negative response to "Select Commerce" message it passes control back to the EPM.

Petitioner Exhibit 1002-0962

Manual Start Mode

[0050] Referring still to FIG. 1, in manual startup mode, reader 120 starts reader application 121 in response to a request from either the consumer or the POS terminal 140. In this manual start mode, at the beginning of a checkout process, reader 120 is in a PPSE select state. For a consumer initiated commerce transaction, the consumer selects the commerce application at the customer facing device (*e.g.*, commerce widget 115). The customer facing device then sends a command to reader 120 to start the reader application 121 via the EPM. For a POS terminal initiated commerce transaction, POS terminal 140 commands reader 120 to initialize the reader application 121. In one embodiment, this is initiated by a cashier via an interface on the POS terminal 140.

[0051] Once reader commerce application 121 has been started on reader 120, the commerce application will function as described in the auto start mode above.

Payment with Post Transaction Data

[0052] In payment with post transaction data mode, a payment transaction can be made such that post transaction data is communicated between POS terminal 140, reader 120, and secure element 112. This option allows the commerce protocol to start at the beginning of the consumer checkout, but payment is not requested by the reader 120 until the final transaction total has been calculated.

[0053] POS terminal 140 sends a "Post Transaction" command to reader 120 with, for example, a transaction identifier (ID) and redeemed coupon IDs. Reader 120 then transmits a request for a tap for payment. The tap allows reader 120 to first request payment credentials from secure element 112 and then cause the reader application 121 to send commerce data (*e.g.*, coupon data) to secure element 112. Both functions are performed in a single tap by the mobile device 110 at reader 120.

Payment First

[0054] In payment first mode, a payment can be made first, prior to a commerce transaction. This option accommodates a situation where the payment/PPSE process must precede any commerce processing. Payment first mode works in

Petitioner Exhibit 1002-0963

conjunction with both auto and the manual start modes discussed above. Payment and commerce processing is accomplished in a single tap.

EXEMPLARY COMMERCE PROCESS FLOWS

Normal Commerce Process Flow (Single Tap)

[0055] FIG. 2 illustrates a single tap timing diagram 200 according to an exemplary embodiment. The following process flow can commence as items being purchased are being scanned at a POS. For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 201. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable.

[0056] A merchant POS system 202 can be a merchant server operated by a merchant which controls the operation of payment terminal 201. In an exemplary embodiment, merchant POS system 202 commands payment terminal 201 to activate the reader ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user (or consumer) to place a mobile device 110 in proximity of reader 120, as shown in step 250 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 250), a consumer taps mobile device 110 onto reader 120, as shown in step 251.

[0057] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 260 and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 262. Steps 260 may be performed before steps 262, afterward, or substantially simultaneously.

[0058] Referring first to steps 262, after a mobile device has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (*e.g.*,

Petitioner Exhibit 1002-0964

commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command ("Get Commerce Data") to secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty, offer or reward schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120, and any merchant capability data.

[0059] Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty data, offer data, reward data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, commerce applet 113 builds a package containing the commerce data (*e.g.*, a buffer or set of buffers including loyalty data, offer data, or rewards data). In another embodiment, the buffer is pre-built using memory space in the secure element 112.

[0060] Referring to steps 260, in one embodiment, reader 120 begins payment processing by sending a PPSE request ("PPSE Select") to secure element 112.

[0061] If the Select Commerce AID and PPSE Select requests are successful, as shown in step 264 ("Read Success Indication"), payment terminal 201 forwards the commerce application data and payment credentials it has received to the merchant POS system 202 for processing ("Payment & Commerce Data"). Merchant POS system 202, in turn, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 266. This concludes the commerce application process and the payment processing proceeds.

[0062] Once scanning has completed and a transaction amount has been approved for payment, a payment authorization request to a payment platform 203 is made ("Payment Auth Request"). In turn, payment platform 203 returns an authorization result ("Authorization Result") indicating whether or not the payment has been authorized.

Petitioner Exhibit 1002-0965

[0063] Referring again to steps 260, in one embodiment, a PPSE Select request by reader 120 to secure element 112 causes secure element 112 to return a PPSE payment AID indicating which payment applet (and hence which corresponding payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID indicating that it supports the particular applet ("Select AID"). File control information (FCI) associated with the payment applet (*e.g.*, FIG 1, 117) is sent by secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").

[0064] FIG. 3 shows a timing diagram 300 illustrating a commerce process flow including a double tap and post transaction data transmission according to an exemplary embodiment. This embodiment can be used when a merchant has data to communicate back to a mobile device. For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 301. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable. Generally, POS terminal 140 (FIG. 1) initiates a request for a second tap by sending a command, "Post Transaction Command", to reader 120. Reader 120, in turn requests a second tap from the consumer.

[0065] A merchant POS system 302 can be a merchant server operated by a merchant which controls the operation of payment terminal 301. In an exemplary embodiment, merchant POS system 302 commands payment terminal 301 to activate reader 120 ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user to place a mobile device 110 in proximity of reader 120, as shown in step 350 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 350), a consumer taps mobile device 110 onto reader 120, as shown in step 351.

[0066] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between

Petitioner Exhibit 1002-0966

secure element 112 and reader 120 include steps 360 and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 362. Steps 360 may be performed before steps 362, afterward, or substantially simultaneously.

[0067] Referring first to steps 362, after mobile device 110 has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (*e.g.*, commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command to the secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty and offer schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120 and any merchant capability data ("Get Commerce Data"). Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty and offers data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, this is accomplished by commerce applet 113, which builds a package of data (essentially a buffer or set of buffers including offers and loyalty data). In another embodiment, the buffer can be pre-built using memory space in the secure element 112.

[0068] Referring next to steps 360, in one embodiment, a PPSE Select request by reader 120 to secure element 112 causes secure element 112 to return a PPSE payment AID indicating which payment applet (and hence payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID indicating that it supports the particular applet ("Select AID"). FCI associated with the payment applet (*e.g.*, 117) is sent by secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").If the Select Commerce AID and PPSE Select requests are successful, as

Petitioner Exhibit 1002-0967

shown in step 364, payment terminal 301 forwards the commerce application data and payment credentials it has received to the merchant POS system 302 for processing ("Payment & Commerce Data"). Merchant POS system 302, in turn, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 366.

[0069] Once scanning has completed and a transaction amount has been approved for payment, a payment authorization request to a payment platform 303 is made ("Payment Auth Request"). In turn, payment platform 303 returns an authorization result ("Authorization Result") indicating whether or not the payment has been made.

[0070]

[0071] If there is data to send back to payment terminal 301, merchant POS system creates a command, "Post Transaction Data", with correctly formatted TLVs and forwards the data to reader 120. Upon receipt of a Post Transaction command payment terminal 301 will request a second tap from the consumer, as shown in step 368 ("Request 2nd 'tap'").

[0072] Referring to step 369 and steps 370, when the mobile device 110 is placed within proximity of reader 120 for the second time as shown in step 369, reader 120 sends a secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (*e.g.*, commerce applet 113).

[0073] If a negative response is received reader 120 terminates the reader commerce application 121. If a positive response is received, then reader 120 forwards to secure element 112 the data received in the Post Transaction Data command from the POS terminal 140 ("Post Transaction Data"). This concludes commerce processing for this transaction.

[0074] FIG. 4 shows a timing diagram 400 illustrating a commerce process flow including a double tap, and post transaction data and payment transmissions according to an exemplary embodiment. In this scenario the payment and post transaction data are processed after a basket has been totaled and all discounts

Petitioner Exhibit 1002-0968

have been applied. Usage of this flow is controlled by a reader start mode data element with a particular bit (*e.g.*, "Payment with Post Transaction") set on.

[0075] For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 401. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable. Generally, merchant POS system 402 initiates a request for a second tap by sending a post transaction data command to reader 120. Reader 120, in turn requests a second tap from the consumer.

[0076] A merchant POS system 402 can be a merchant server operated by a merchant which controls the operation of payment terminal 401. In an exemplary embodiment, merchant POS system 402 commands payment terminal 401 to activate the reader ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user to place a mobile device 110 in proximity of reader 120, as shown in step 450 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 450), a consumer taps mobile device 110 onto reader 120, as shown in step 451.

[0077] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated. The command exchanges are performed for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 472, and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 462 and 474.

[0078] Referring first to steps 462, after a mobile device has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 to cooperate with (*e.g.*, commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command

Petitioner Exhibit 1002-0969

to the secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty and offer schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120 and any merchant capability data ("Get Commerce Data"). Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty and offers data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, this is accomplished by commerce applet 113, which builds a package of data (*e.g.*, a buffer or set of buffers including offers and loyalty data). In another embodiment, the buffer can be pre-built using memory space in the secure element 112.

[0079] At step 464, reader 120 indicates to the consumer that the transaction is complete and that the handset can be removed from payment terminal 401, which causes reader 120 to forward the commerce application data to the POS terminal 140 and, in turn, merchant POS system for processing ("Loyalty & Offers Data"). A clerk may continue to process the shopping basket.

[0080] Merchant POS system 402, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 466. After the basket total has been calculated, merchant POS system 402 sends a request for payment to payment terminal 401 and sends post transaction data to payment terminal 401 (if data is available to send) ("Send Post Transaction Data and Payment Req").

[0081] At step 468, payment terminal 140 requests a tap for payment. Reader 120, in turn, activates the reader field. When mobile device 110 is detected in the field of reader 120, payment processing is performed as shown in steps 472. Particularly, a PPSE Select request is made by reader 120 to secure element 112 to cause secure element 112 to return a PPSE payment AID indicating which payment applet (and hence payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID command indicating that it supports the particular applet ("Select AID"). FCI associated with the payment applet (*e.g.*, FIG. 1, 117) is sent by

Petitioner Exhibit 1002-0970

secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").

[0082] Referring to steps 474, if payment terminal 401 has received post transaction data from merchant POS system 402, reader 120 starts the commerce application 121 (FIG. 1) and sends secure element 112 the Select Commerce command along with a particular commerce AID ("Select Commerce AID") after a mobile device has tapped reader 120 a second time. The Select Commerce AID identifies which commerce applet within secure element 112 should be used to cooperate with reader 120. In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends post transaction data to the secure element 112 ("Post Transaction Data"), with correctly formatted TLVs. This concludes commerce processing for this transaction.

[0083] If the Select Commerce AID and PPSE Select requests are successful, payment terminal 401 forwards the payment application data and payment credentials it has received to the merchant POS system 402 for processing ("Payment/Card Data"). In turn, merchant POS system sends a payment authorization request to a payment platform 403 ("Payment Auth Request"). In turn, payment platform 403 returns an authorization result (Authorization Result) indicating whether or not the payment has been authorized.

[0084] If the commerce and payment credentials and information have been successfully read, reader 120 can provide a notification either through an interface on payment terminal 140, commerce widget 115 (FIG. 1) or payment widget 119 (FIG. 1), as shown in step 478 ("Read Success Indication").

Commerce Message Specifications

Data Encoding

[0085] In one embodiment, all command/response data is encoded using BER-TLV (ISO 7816-4 Annex D) format. In some cases, the TLV (Tag, Length,Value) may be nested (embedded TLV). Due to the flexible nature of the

Petitioner Exhibit 1002-0971

TLV encoding format, the tagged data may be placed in any order. This is true when formatting the data for both incoming and outgoing payloads. In addition, this data is stored in record oriented tables. The order of the TLV encoded data elements stored therein is not critical; however, some data may be placed at the beginning of the record to enhance index/search performance. Thus, the record data tables provided in this document are supplied as samples for reference purposes.

[0086] A tag is encoded using a "private" tag class and a tag type representing a primitive data object encoded on one or more subsequent bytes. Therefore, the first byte (tag class) is set to 0xDF. In all cases, the data element tag is defined on a single byte. Therefore, the second tag byte has the most significant bit (b8) set to 0. This allows up to 128 valid tag values (0x00 – 0x7F).

[0087] Length encoding supports both the short or long forms. When the length is less that (<) 128 bytes, the most significant bit (b8) is set to 0 and the actual length is specified in the remaining bits (b7 – b1). When the length is greater than (>) 128 bytes, the most significant bit (b8) is set to 1 (length mask = 0x80) and the remaining bits (b7-b1) define the number of subsequent bytes in the length field. Those subsequent bytes encode an integer equal to the number of bytes in the value field.

BER-TLV Example

[0088] Assuming the incoming data uses a tag value of 0x21 (Consumer ID) with a length of 8 bytes and a value of (0x1122334455667788), the data is encoded as shown in Table 1:

TABLE 1

Tag	Length	Value
DF 21	08	11 22 33 44 55 66 77 88
DF 21	81 08	11 22 33 44 55 66 77 88
DF 21	82 00 08	11 22 33 44 55 66 77 88

[0089] TLV encoding allows for the length indicator to be expressed in multiple bytes. Preferably multi-byte length is supported. In short form, the length field consists of a single byte where bit 8 is set to 0 and bits 7 to 1 encode the number

Petitioner Exhibit 1002-0972

of bytes in the value field. One byte can thus encode any number from zero to 127. Any number from one to 127 is encoded in the same way in BER-TLV length field as in Lc and Le fields. The encoding differs for zero, 128 and more. See, for example, the coding of data objects in the Get Commerce Data command described below.

[0090] In long form, the length field consists of two or more bytes. Bit 8 of the first byte is set to 1 and bits 7 to 1 are not all equal, thus encoding the number of subsequent bytes in the length field. Those subsequent bytes encode the number of bytes in the value field. ISO/IEC 7816 does not use the "indefinite length" specified by the basic encoding rules of ASNI ISO/IEC 7816, which supports length fields of one, two, ... up to five bytes (Table 2). In ISO/IEC 7816, the values '80' and '85' to 'FF' are invalid for the first byte of length fields.

TABLE 2 – BER-TLV length fields in ISO/IEC 7816

	1st byte	2nd byte	3rd byte	4th byte	5th byte	N
1 byte	'00' to '7F'	-	-	-	-	0 to 127
2 bytes	'81'	'00' to 'FF'	-	-	-	0 to 255
3 bytes	'82'	'0000' to 'FFFF'		-	-	0 to 65 535
4 bytes	'83'	'000000' to 'FFFFFF'			-	0 to 16 777 216
5 bytes	'84'	'00000000' to 'FFFFFFFF'				0 to 4 294 967 296

Select Commerce Applet

[0091] In one embodiment, the processing starts when reader 120 detects a mobile device 110 in the field of reader 120 and NFC communications have commenced. At that time, reader 120 sends a command to secure element 112 to select a commerce applet, particularly a "Select Commerce" command. The Select Commerce command (also referred to as a "Select Commerce Applet" command) is standardized as defined in the ISO 78016-3 specification. An example Select Commerce command structure is shown in Table 3:

TABLE 3 – Select Commerce Applet

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	00	09	A00000048510010101	00

[0092] Secure element 112 in mobile device 110 validates the "Select Commerce" command and sends back an appropriate response. Example responses (also referred to as "Status Codes") are shown in Table 4:

TABLE 4 – Status Codes

SW1	SW2	Description
90	00	Successful execution of command
67	00	Wrong data length
69	01	Application ID not supported
69	99	Application not available
6A	82	Application not installed

[0093] All responses other than '90 00' ("Successful execution of command") cause commerce application 121 (FIG. 1) to terminate in reader 120 and pass control to the EPM.

Get Commerce Data

[0094] Upon commencement of the reader application 121 and communications between reader 120 and secure element 112 initiating, reader 120 sends a command to mobile device 110 to obtain commerce data, "Get Commerce Data." An exemplary Get Commerce Data command is defined below in Tables 5 and 6. In this example, specific loyalty and offers data is being requested. The "Merchant Capability" field is utilized by reader 120 to determine which fields need to be present in the request and response data.

[0095] Date and time stamp information are optional. In one embodiment, the date time is in synchronization with the POS. In the event that this information is not available from the POS, the date/time from the POS terminal 140 can be used. If date and time is not available, reader 120 will not send the date time stamp data element.

[0096] In an exemplary embodiment, the data elements contained in the Get Commerce Data request are preconfigured in the reader 120 or POS terminal 140 at setup time. The data may be modified after the reader 120 has been installed and configured.

Petitioner Exhibit 1002-0974

TABLE 5 – Get Commerce Data

CLA	INS	P1	P2	Lc	Data	Le
90	50	00	00	xx	Merchant ID/ Store ID [+ Loyalty IDs +Coupon Types + Date/Time-Stamp +Application Version + Merchant Capability]	00

TABLE 6 – Command Data

Data Element	Byte Size	Value	Req
Merchant Identifier Tag	2	0xDF 31	Y
Identifier Length	1	xx	
Merchant Identifier	xx	[MerchantID]	
MerchantStore_ID Tag	2	0xDF 32	Y
Merchant_Store_ID Length	1	xx	
Merchant_Store_ID	xx	(StoreID/Location)	
Loyalty_ID Tag #1 For Secondary loyalty	2	0xDF 41	Opt
Identifier Length #1	1	xx	
LoyaltyID_#1	xx	[Loyalty ID] (Hex)	
.....			
Loyalty_IDr Tag #X For Secondary loyalty	2	0xDF 41	Opt
Loyalty Identifier Length #X	1	xx	
LoyaltyID_#X	xx	Loyalty ID (Hex)	
Date_Time_Stamp Tag	2	0xDF 11	Opt
Date_Time_Stamp Length	1	0x07	
Date_Time_Stamp	7	BCD (yyyymmddhhmmss)	
Commerce_App_Version Tag	2	0xDF 12	Y
Commerce_App_Version Length	1	0x02	
Commerce_App_Version Data	2	[Major + Minor] Hex	
Merchant_Capability Tag	2	0xDF 33	Y
Merchant_Capability Length	1	0x02	
Merchant_Capability Data	2	2 Bytes Hex	
Terminal_Startup_Mode_Tag	2	0xDF 34	Opt
Terminal_Startup_Mode_Length	1	0x02	
Terminal_Startup_Mode_Data	1	1 Bytes Hex	
Total:	<var>		

[0097] Table 7 defines the possible Status Word values that may be returned by the Get Commerce Data command.

Petitioner Exhibit 1002-0975

TABLE 7 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
61	xx	More data to follow
67	00	Wrong Data Length
69	09	Internal Error

[0098] Any response other than'61 xx' or '90 00' will result in reader 120 terminating commerce application 121 and passing control to the EPM, after recording the error and storing the data for forwarding to commerce widget 115.

[0100] If the Get Commerce Data request is correctly formatted, commerce applet 113 on secure element 112 filters the data based on the merchant identifier ("Merchant_ID"), loyalty identifier ("Loyalty_ID") and offer type code ("Offer_Type_Code") to format a response data for reader 120 based on the version number in the request. Commerce applet 113 may return more than one Loyalty ID and multiple Offers messages based on the configuration in the wallet. Table 8 lists exemplary response data:

TABLE 8 – Example Response Data

Data Element	Byte Size	Value
Consumer_ID Tag	2	0XDF21
Consumer_ID Length	1	0x10
Consumer_ID Data	16	[Consumer ID]
Loyalty_ID Tag #1	2	0xDF41
Loyalty_ID Length #1	1	xx
Loyalty Identifier #1	xx	[Loyalty ID]
Loyalty_Account_Code Tag #1	2	0xDF43
Loyalty_Account_Code Length #1	1	xx
Loyalty_Account_Code #1	xx	[Acct Code]
Loyalty_ID Tag #2	2	0xDF 41
Loyalty_ID Length #2	1	xx
Loyalty_ID Data #2	xx	[Loyalty ID]
Loyalty_Account_Code Tag #2	2	0xDF43
Loyalty_Account_Code Length #2	1	xx
Loyalty_Account_Code Code #2	xx	[Acct Code]
.....		
Offer_ID Tag #1	2	0xDF51
Offer_ID #1 ID Length	2	X'81 xx'

Petitioner Exhibit 1002-0976

Data Element	Byte Size	Value
Offer_ID #1 ID Value	xx	[Coupon ID]
Offer_Code #1 Code Tag	2	0xDF53
Offer_Code #1 Code Length	2	0x'81xx'
Offer_Code #1 Code Value	xx	[Coupon Code]
Offer_ID Tag #2	2	0xDF51
Offer_ID #2 ID Length	2	0x'81xx'
Offer_ID #2 ID Value	xx	[Coupon ID]
Offer_Code #2 Code Tag	2	0xDF53
Offer_Code #2 Code Length	2	0x'81xx'
Offer_Code #2 Code Value	xx	[Coupon Code]
.....		
Total:	<var>	

[0101] The following is an exemplary response data parsing sample. The NFC reader (or POS terminal) delivers this commerce data to a POS system in a string of data that may contain consumer, loyalty and/or offer data. The merchant POS system can then parse the data to obtain the loyalty and offer data, and process the data per the merchant's specifications.

```
DF 21 10 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF DF 41 06
18 DB 6E 23 F4 0B DF 43 0D 02 31 38 44 42 36 45 32 33 46 34 30 42
DF 51 08 88 77 66 55 44 33 22 05 DF 53 09 02 42 41 31 38 37 36 35
34 DF 51 08 88 77 66 55 44 33 22 06 DF 53 0C 02 41 39 39 39 39 31
33 33 35 37 38 DF 51 08 88 77 66 55 44 33 22 07 DF 53 10 02 5A 58
31 37 39 35 36 37 35 34 38 33 31 43 46 DF 51 08 88 77 66 55 44 33
22 08 DF 53 0C 02 31 38 30 30 38 37 32 30 30 30 31 DF 51 08 88 77
66 55 44 33 22 09 DF 53 33 02 57 4B 52 50 31 32 33 34 35 36 37 38
39 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 50 57 50 57 50
57 50 57 50 57 50 57 50 57 50 57 50 57 50 40 A1

Data parsing example

DF 21 10 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
(Consumer ID)

DF 41 06 18 DB 6E 23 F4 0B            (MoCom Loyalty ID)

DF 43 0D 02 31 38 44 42 36 45 32 33 46 34 30 42
(Consumer Loyalty Code)

DF 51 08 88 77 66 55 44 33 22 05      (MoCom Offer ID)  #1

DF 53 09 02 42 41 31 38 37 36 35 34   (Merchant Offer Code)  #1

DF 51 08 88 77 66 55 44 33 22
```

Post Transaction Data

[0102] As explained above, a Post Transaction Data command provides a mechanism to receive data back from a merchant POS system (MPOS). This command is initiated by the merchant POS terminal 140 and preferably is supported in the merchant capability field. In an exemplary embodiment, this command consists of a single frame of data with a maximum data size of 255 bytes. The contents of the data use standard TLV formatting but may also be variable. This command enables dynamic reconciliation or post transaction data consolidation. Additional data tags may be defined for the transmission of additional data from the POS terminal/MPOS to the secure element 112 in mobile device 110. An exemplary post transaction data command ("Post Transaction Data") is illustrated in tables 9 and 10:

TABLE 9 – Post Transaction Data Command

CLA	INS	P1	P2	Lc	Data	Le
90	52	00	00	xx	<TLV Encoded Post Transaction Data>	00

TABLE 10 – Command Data

Data Element	Byte Size	Value	Req
Transaction ID	2	0x DF 61	Opt
Transaction ID Length	1	xx	
Transaction ID Data	xx	Merchant generated Transaction ID	
Offer_ID Code #1	2	0XDF 51	Opt
Offer_ID Length #1	1	xx	
Offer_ID Data #1	xx	Coupon ID	
.....			
Offer_ID Code #X	2	0xDF 51	Opt
Offer_ID Length #X	1	xx	
Offer_ID Data #X	xx	Coupon ID	
Total:	<var>		

Multi-block data handling

[0103] FIG. 5 illustrates an exemplary multi-block data flow according to an example embodiment. When secure element 112 has more than 255 bytes of data to send, a Get Response command (C0) is used to retrieve the remaining response

Petitioner Exhibit 1002-0978

data. Particularly, this command is used to obtain the remaining data when the commerce applet 113 must send more than, for example, 255 bytes of response data.

[0104] Referring to FIG. 5, after a user taps a commerce-enabled mobile device 110 to reader 120, reader 120 sends a Select Commerce command to the secure element 112 of the mobile device 110. A positive response ('90 00') causes reader 120 to send a Get Commerce Data command. In response, secure element 112 returns loyalty and offers data. As shown in FIG. 5, the Get Commerce Data response status SW1 flag is set to '61' and the SW2 flag is set to '00'.

[0105] A Get Response command is triggered when the SW1 flag in the Get Commerce Data response is set to '61'. In this example, the SW2 flag is set to '00' because commerce applet 113 on mobile device 110 may not know how much data is left to send. The subsequent response to the Get Response command also contains an SW1 flag set to '61', causing a second Get Response command to be sent by reader 120 to mobile device 110.

[0106] This sequence will terminate when the SW1 flag of the Get Commerce Data response is set to any value other than '61'. For example, an SW1 value of '90' in response to a Get Response command as shown in FIG. 5 will indicate normal completion. Any other SW1 value can be logged as an error.

[0107] Table 11 defines exemplary settings for the Get Response Data APDU command:

TABLE 11 – Get Response Data

CLA	INS	P1	P2	Lc	Data	Le
90	C0	00	00	00	<none>	00

[0108] The actual length of the remaining data is variable. Therefore, the Le data length can be 0x00; allowing the commerce applet 113 to manage a variable length response.

[0109] Table 12 defines possible status word values ("Status Codes") that may be returned by the Get Response Data APDU command.

TABLE 12 – Status Codes

SW1	SW2	Description
90	00	Successful execution of command
61	xx	More data to follow
67	00	Wrong data length
69	09	Internal error

Reader Configuration Data

[0110] In one embodiment, during the installation and configuration of reader 120 certain merchant and commerce specific data are loaded and saved in reader 120. This data is used by reader 120 to fill in the Get Commerce Data command from reader 120. These data elements can be updated as new features and functions become available.

Commerce AID

[0111] As explained above, a commerce AID is sent in the Select Commerce command. If the command is accepted by mobile device 110, commerce applet 113 is started and APDU command / response flows will start between reader 120 and secure element 112. In an exemplary embodiment, the commerce AID value is A00000048510010101. This value can be hardcoded on reader 120. In one embodiment, reader 120 is not required to support partial selection.

Merchant_ID

[0112] A merchant identifier (Merchant_ID (DF31)) can be loaded onto reader 120. Merchant ID is a value assigned by a service provider. In one embodiment, this value is assigned by the MoCom platform operator. This is required to allow commerce applet 113 to filter the loyalty and coupon data, and send the appropriate items to the reader 120.

Merchant_Store_ID

[0113] A merchant store identifier value (Merchant_store_ID (DF32)) is loaded to the reader 120 and is a value assigned by a service provider. This value can be used, for example, for reporting purposes.

Petitioner Exhibit 1002-0980

Loyalty_ID

[0114] A loyalty identifier value (Loyalty_ID (DF41)) is used when multiple Loyalty IDs are being requested during a tap. This is accomplished by setting the Secondary Loyalty in Merchant Capabilities (DF33). This allows commerce applet 113 to return additional loyalty numbers in the response to a Get Commerce Data command. Multiple (*e.g.*, 5) additional Loyalty_IDs may be coded in the Get Commerce Data request.

Offer_Type_Codes

[0115] Offer type codes (Offer Type Codes (DF54)) are loaded onto reader 120. Values assigned to Offer Type Codes are assigned by a service provider. This value is used by the commerce applet 113 to filter offers and send only the appropriate items to reader 120. Multiple Offer_Type_Codes can be defined and sent to the secure element 112 in the Get Commerce Data command.

Commerce_Application_Version

[0116] A commerce application version number (Commerce_Application_Version) can be loaded onto reader 120 to represent the version of the commerce reader specification that the application on reader 120 is coded to and certified for.

Merchant_Capabilities

[0117] The Merchant Capabilities value represents the Commerce features supported by a particular merchant. This data element can also be used by reader 120 to format the Get Commerce Data command.

Terminal_Startup_Mode

[0118] A terminal start mode command (Terminal Start Mode (DF34)) commands reader 120 to provide the mechanism used to start commerce application 121. This data element is not sent to the secure element 112. This data element will also be used to define processing flows between reader 120 and secure element 112 on the handset.

Petitioner Exhibit 1002-0981

Get Commerce Data Fields

[0119] Table 13 provides an exemplary definition of data required by reader 120 to format the Select Commerce and Get Commerce Services commands:

TABLE 13

Data Element	Tag	Max Size Bytes	Data Format
Commerce AID		09	Hex
Merchant ID	DF 31	8	Hex
Merchant Store ID	DF 32	32	ASCCI
Loyalty Identifier #1 thru X	DF 41	8	BCD
Date and Time Stamp	DF 11	7	BCD
Specification Version (Major/Minor)	DF 12	2	Hex
Merchant Capabilities	DF 33	2	Binary
Commerce Start Mode	DF 34	2	Binary

Commerce Applet Version Format

[0120] A Commerce Applet Version value is a two-byte hex field the first byte containing the major version (xx) and the second byte contains the minor version (xx). These fields are updated in accordance to the specific version of the reader commerce technical specification that is implemented on reader 120. In an exemplary embodiment, the first official release of the commerce application 121 is 0x0100.

Merchant Capabilities

[0121] A merchant capabilities field (Merchant Capabilities Field (DF 33)) determines which commerce functions are being implemented by the merchant. Reader 120 can pass this field to mobile device 110, and mobile device 110 uses the information to build a response frame, referred to as Commerce Data Response frame. Table 14 illustrates exemplary merchant capabilities:

TABLE 14 – Merchant Capability Data

Commerce Start Mode Format

Byte	Bit	Value	NFC reader function
1	8 MSB	1=Merchant Loyalty Support	If Bit 8 is on the reader will send the required Merchant ID and optionally a

Petitioner Exhibit 1002-0982

		0=No	Loyalty ID for the merchant
1	7	1=Secondary Loyalty 0=No	Bit 8 must be on. Additional Loyalty ID's is included in the Get Commerce Data request
1	6	1=Offers Support 0=No	Offer Type fields is included in Get Commerce Data request
1	5	1=Additional Offer support 0=No	The merchant can request additional offers in the Get Commerce request
1	4	1=Contactless Payment support 0=No	Some merchants may choose to only accept Commerce but not contactless payments. This bit setting is information only. It will not stop the PPSE process from happening.
1	3	1=Enterprise Merch ID 0=No	
1	2	1=Cloud Based Offer 0=No	Indicates that the merchant can support cloud based offers (Future)
1	2	0	Reserved for Future Use
1	1	1=Post Transaction Data support 0=No	The reader will receive redemption data from the POS and forward it to the handset
2	8-1	0	Reserved for Future Use

Commerce Start Mode Format

[0122] A commerce start mode format value (Commerce Start Mode (DF34)) indicates to reader 120 what mechanism is to be used to start commerce application 121 on reader 120. In one embodiment, this data element is not sent to the mobile device 110 in the Get Commerce Data command. In another embodiment, this data element is optional. Table 15 illustrates exemplary start modes can be used to commence commerce application 121. In an exemplary embodiment, bits 7 and 8 are exclusive and only one bit is turned on at a time:

TABLE 15 – Commerce Start Mode

Byte	Bit	Value	Reader function
1	8 MSB	1=Auto Start 0=No	At the start of the check the reader will quest Commerce AID at the first TAP
1	7	1=Manual Start 0=No	The reader will only select Commerce AID after some user intervention.
1	6	1=Payment with	Payment and Post Transaction Data will

Petitioner Exhibit 1002-0983

		Post Transaction Data 0=No	occur on TAP 2
1	5	Payment First	Payment PPSE will precede in Auto or Manual start modes
1	4-1	0	Reserved for Future Use
2	8-1	0	Reserved for Future Use

Reader Message Forwarding

[0123] While reading commerce application data from the mobile device 110, reader 120 forwards the data to a merchant POS system or POS application resident on a POS terminal 140. Reader 120 strips off the APDU headers and un-blocks the data from the mobile device 110. The Tagged TLV frames are then wrapped in the appropriate protocol and forwarded to the merchant POS system or POS application running on the POS terminal for processing.

Commerce Response Data Description

[0124] During a successful interaction with a reader 120, data will be returned to the POS merchant system (or POS terminal). This information will typically be composed of a consumer loyalty number and/or some number of offers that the merchant defined and loaded to the consumer's wallet.

Consumer ID

[0125] A consumer identifier (Consumer ID) is a unique identifier that is assigned to a consumer during the wallet activation process. Typically, Consumer ID will stay with a consumer even if the consumer moves her wallet to a new mobile device or different mobile network. In a preferred embodiment, Consumer ID is sent from the mobile device to the reader on every commerce-related interaction, even if the handset has no loyalty or offers data to send. The presentation of Consumer ID can be used by the merchant POS system to trigger specific actions related to a payment-only tap.

Loyalty ID

[0126] A loyalty identifier (Loyalty ID) is sent along with each consumer loyalty number requested during a tap event. Loyalty ID is a unique value assigned to

Petitioner Exhibit 1002-0984

each merchant loyalty program assigned by the MoCom platform. In most cases the Loyalty ID received by the reader will match the Merchant ID that was configured by the Get Commerce data command. Use of this information by a merchant system is optional.

Consumer Loyalty Code

[0127] A consumer loyalty code (Consumer Loyalty Code) matches the loyalty number assigned to the consumer for a specific merchant loyalty program. Wallet application 114 allows for multiple loyalty numbers to be presented at the tap. If the system is set up for multiple consumer loyalty codes, each consumer loyalty code will be preceded by its unique loyalty ID.

Offer ID

[0128] A mobile commerce offer identifier (Offer ID) is sent along with each consumer offer number sent during a commerce-related session. The Offer ID is a unique value assigned to each offer delivered to a consumer wallet. In one embodiment, no two Offer IDs generated by the MoCom platform will have the same value.

Merchant Offer Code

[0129] A merchant offer code ("Merchant Offer Code" or "Offer Number") is generated by the merchant and loaded to the consumer's wallet application through various means. This number matches the same offer that is defined on the merchant POS system for processing. There can be multiple merchant offers (*e.g.*, 10) presented during a single commerce transaction. The merchant system parses the incoming data to extract the individual merchant offers.

Commerce Response Data Fields

[0130] Table 16 defines exemplary data elements that may be returned to the merchant POS system after a successful commerce transaction:

TABLE 16

Data Element	Tag	Max Size Bytes	Data Format
Consumer ID	DF 21	16	BCD
Loyalty ID	DF 41	8	Hex
Consumer Loyalty Code	DF 43	32	ASCII, Hex, BCD
Offer ID	DF 51	8	BCD
Merchant Offer Code	DF 53	48	ASCII, Hex, BCD

[0131] In one embodiment, a data element "Terminal Start Mode" is passed to reader 120 but will not be passed to the secure element 112. Reader 120 uses this information to control when Select Commerce and Select PPSE commands are sent to the secure element 112.

Reader Commerce Application Functionality

[0132] The following section provides a list of functions that the Commerce application within reader 120 performs. Some of these functions are automated, while others are triggered via an API call from the POS terminal or merchant POS.

Select Commerce AID Command

[0133] After the Commerce application is started on reader 120 and a device is detected in the field of reader 120, the first command sent is Select Commerce AID. The command will contain the RID value assigned by ISO and a PIX value generated by a commerce service provider. The Commerce AID value is A00000048510010101. This value should be hard coded on reader 120.

Get Commerce Data Command

[0134] The Get Commerce Services Data command is a general data request to the secure element 112. The Get Commerce Data has a number of required and optional fields that communicate information to commerce applet 113. Commerce applet 113 uses this information to build the data elements that need to be sent to reader 120. Reader 120 uses the fields in the Merchant Capability records to determine which optional fields need to be included in the request to the handset.

Post Transaction Data

[0135] The Post Transaction Data command was created to provide a mechanism to receive data back from the MPOS. This command consists of a single frame of data with a maximum data size of 255 bytes. The contents of the data use standard TLV formatting, but the contents may be variable. Additional data tags may be defined for the transmission of additional data from the POS Terminal/MPOS to secure element 112 in mobile device 110.

NFC Error recovery

[0136] In a preferred embodiment, reader 120 is able to recover from a reader error generated when the handset is prematurely removed from the NFC field. Reader 120 signals the read error to the consumer via a failure interface such as a speaker that outputs a "beep" or display that provides an optical indication such as via lights. The consumer is asked to tap again and the transaction that was in progress during the error is restarted. In the case where multiple transactions are being processed, such as a commerce transaction and a PPSE transaction, reader 120 will try to recover the last process being executed.

Large Data block support

[0137] In an exemplary embodiment, reader 120 reads and writes multiple 255-byte blocks of data to and from mobile device 112 in a single tap process.

Date and time stamp support

[0138] When reader 120 has connectivity to the merchant POS system, the date and time can be retrieved from the POS terminal at the start of the transaction.

TLV Master Tag List

[0139] Table 17 defines the data elements and corresponding tag values and target/max byte sizes used by commerce based applications. Additional values have been provided for those elements with a limited/fixed value range.

TABLE 17 – APDU Commands

Commerce Services			
Shared Data Elements			
Data Element	Tag	Max	Description

Petitioner Exhibit 1002-0987

		Size	
DATE_TIME_STAMP	0xDF11	7	Date/Time stamp (yyyymmddhhmmss)
COMMERCE_APP_VERSION	0xDF12	2	Supported Commerce application Version Number
Consumer Data Elements			
Data Element	Tag	Max Size	Description
CONSUMER_ID	0XDF21	16	MoCom Platform specific consumer identifier
CONSUMER_KEY	0xDF22	16	MoCom Platform generated consumer specific 3DES key
CONSUMER_CERT	0xDF23	8	MoCom Platform generated consumer signature/ certificate
Merchant Data Elements			
Data Element	Tag	Max Size	Description
MERCHANT_ID	0xDF31	8	MoCom Platform specific merchant identifier
MERCHANT_STORE_ID	0xDF32	32	MoCom Platform specific merchant store identifier ASCII character data
MERCHANT_CAPABILITY	0xDF33	2	Supported Commerce application Services
NFC READER_START_MODE	0xDF34	2	NFC enabled payment terminal startup mode (provided by Merchant POS System during initialization)
Merchant Capabilities			
Data Element	Value	Max Size	Description
MERCAP_MERCHANT_ LOYALTY	0x80	1	The Get Commerce Data request includes a valid merchant identifier used to determine the Loyalty data received by the applet.
MERCAP_ADDITIONAL_ LOYALTY	0x40	1	The Get Commerce Data request includes additional Loyalty Identifiers. Additional Loyalty data is determined by the specified Loyalty ID(s).
MERCAP_MERCHANT_ OFFERS	0x20	1	Offer type fields are included in Get Commerce Data request

Petitioner Exhibit 1002-0988

MERCAP_ADDITIONAL_ OFFERS	0x10	1	The Get Commerce Data request includes a valid merchant identifier used to determine the offers data received by the applet.
MERCAP_PAYMENT	0x08	1	Indicates merchant supports contactless payment.
MERCAP_ENTERPRISE	0x04	1	Indicates support for Enterprise Merchant ID
MERCAP_CLOUD	0x02	1	Indicates support for cloud based offers and Loyalty
MERCAP_REDEMPTION	0x01	1	The NFC reader supports the transmission of offer redemption data (from the POS) to the applet via the Redeem Offer command.
Service Provider Platform Data Elements			
PLATFORM_SIGNATURE	0x71	8	MoCom Platform generated MAC/Signature appended to command/data originating from the platform for remote verification purposes (data integrity/ authenticity).
PLATFORM_KEY	0x72	16	MoCom Platform Key
PLATFORM_CERT	0x73	8	MoCom Platform Certificate

Loyalty			
Loyalty Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ LOYALTY_DATA	0xDF40	xx	Embedded TLV loyalty data tag
LOYALTY_ID	0xDF41	8	MoCom Platform specific loyalty identifier
LOYALTY_STATUS	0xDF42	1	Loyalty card/account status (see below)
LOYALTY_ACCOUNT_ CODE	0xDF43	32	Loyalty account (barcode data)
LOYALTY_MAC_ SIGNATURE	0xDF44	8	MoCom Platform specific MAC/Signature for integrity/ authenticity verification

Transaction Log			
Transaction Data Elements			
Data Element	Tag	Max	Description

Petitioner Exhibit 1002-0989

		Size	
EMBEDDED_TLV_ TRANSACTION_LOG	0xDF60	xx	Transaction log record data tag
TRANSACTION_ID	0xDF61	16	Transaction ID (assigned by POS)
TRANSACTION_STATUS	0xDF62	3	Transaction log record data tag

Offers			
Offer Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ OFFER_DATA	0xDF50	xx	Embedded TLV offer data tag
OFFER_ID	0xDF51	8	MoCom Platform specific offer identifier
OFFER_STATUS	0xDF52	1	Offer status (see below)
OFFER_CODE	0xDF53	130	Offer (UPC/EPC/GS1 Databar) barcode data
OFFER_TYPE_CODE	0xDF54	9	Offer Type (see below)
OFFER_MAC_ SIGNATURE	0xDF55	8	MoCom Platform specific data security signature
OFFER_UPDATE_FLAG	0xDF56	1	Update flag (synchronization status)

[0140] Table 18 provides a master list of exemplary APDU commands supported by the Commerce Applet 113.

TABLE 18

Command	CLA	INS	P1	P2	Lc	Data	Le
Get Commerce Data	90	50	00	00	xx	Date/Time Stamp + Merchant ID + Store ID [+ Commerce application Version + Merchant Capabilities + Transaction ID + Loyalty IDs + Offer Codes]	00
Post Transaction Data	90	52	00	00	xx	<TLV-Encoded Transaction Data>	00
Get Remaining Data	90	C0	00	00	xx	None	

Specially Formatted Data Elements

[0141] Data elements included in the commerce data payload may include a format byte that identifies the data encoding used for that element. The data encoding is specified by the merchant to ensure compatibility at the point of sale. The formatted data value is supplied by the commerce platform to the wallet application 114. Thus, no additional interpreting/formatting is necessary between the platform 130, wallet 114, secure element 112, and reader 120/POS terminal 140 (collectively referred to as "payment terminal"). It is the role of the payment terminal (or merchant POS system) to properly interpret the data and supply it to the merchant system for processing.

[0142] In an exemplary embodiment, the following data elements include the following format value:

- Loyalty Account Code (DF 43)
- Offer Code (DF 53)

[0143] Table 19 defines possible format byte values and their corresponding encoding rule:

TABLE 19

Format Byte	Encoding Rule	Description
0x00	Hexadecimal	Each byte of data is encoded in (raw) hexadecimal format.
0x01	Binary Coded Decimal (BCD)	Each nibble represents a single digit. Thus, only decimal values are specified. A data stream containing an odd number (length) of digits includes the hex value 'F' in the first nibble of the data stream.
0x02	ASCII	Each byte represents an ACII value that is interpreted as such and handled as its corresponding CHAR value. In most cases, these data streams are converted into a String before being passed to the merchant POS system for processing.

[0144] A BCD encoded data value that includes the hexadecimal value 'F' in the first nibble shall identify a data stream containing an odd number of digits. Thus, the BCD data stream *12345* is encoded in 3 byte buffer as follows: *0xF12345*.

Petitioner Exhibit 1002-0991

Exemplary Implementations

[0145] FIG. 6 illustrates windows or screen shots generated by the graphical user interface for a wallet application in accordance with an example embodiment of the present invention. For purposes of this exemplary implementation, the mobile device 110 has some redeemable offers and loyalty cards stored in memory 111b.

[0146] The wallet home screen 601 features a strip of merchant tiles 604. A tile is present for every merchant that has a redeemable object (*e.g.*, a redeemable offer or loyalty card) present in the mobile wallet. The user may, for example, swipe through the tiles, left and right, to find a particular merchant. Once the particular merchant is found, the tile is selected to open a merchant offer view 602. This can be done prior to making a transaction or immediately prior to making the transaction, such as while waiting in line, or earlier (*e.g.*, while browsing through a store.).

[0147] The merchant offer view 602 presents a list of redeemable offers 603 available in the wallet. Non-redeemable promotions may be presented as well. If present, a loyalty card 605 is also presented and made accessible from the merchant offer view 602.

[0148] If the selected merchant is not a commerce-enabled merchant, there is no option presented to load offers for a commerce transaction. If the merchant is a commerce-enabled merchant, however, one or more buttons or icons 606a, 606b are presented allowing offers to be loaded for a commerce transaction.

[0149] The user may select an offer (*e.g.*, 606a), and then select the "Done" bar at the bottom of the screen.

[0150] In an exemplary embodiment, a limit as to the number of offers can be enforced by secure element 112 (*e.g.*, 10 offers), and the user interface of commerce widget 115 enforces this limit while the user is activating offers. The "Done" bar is the trigger to load the selected offers into secure element 112. If there are offers from another merchant in the secure element 112, they can be removed at the same time as the new offers are loaded – this ensures that there are only offers from one merchant present in the 112 at any given time.

[0151] When the secure element load is complete, the user taps the mobile device 110 to reader 120. What happens next depends on a few factors. If the reader that is tapped is not capable of processing commerce elements, the selected payment card is sent, but no commerce elements (*e.g.*, offers or loyalty credentials) are sent. A post-tap message is presented through the reader interface indicating that payment credentials were sent, with no other information.

[0152] If the reader that is tapped is capable of processing commerce elements, but the merchant-ID does not match the selected merchant, offers will not be sent. Commerce applet 113 in secure element 112 can search for a loyalty card for this merchant-ID and transmit loyalty credentials, if present. A post-tap message is presented through an interface indicating that an event took place, identifying the merchant and reporting that loyalty credentials were sent (if they were available) as well as the payment credentials.

[0153] If the reader that is tapped is a commerce-enabled reader and the merchant-ID matches the selected merchant, selected offers and (if present) the loyalty card credentials for the merchant are sent. Mobile device 110 can present a post-tap message through the commerce widget 115 user interface confirming that offers and loyalty (if present) were sent, along with payments.

[0154] Following the tap, offers that were loaded into the secure element 112 are left in secure element 112 until the user removes them or selects offers from another merchant. Alternatively, if the offers expire, it is removed from the secure element 112 when wallet maintenance is performed. In an exemplary embodiment, the selected merchant will remain the "active" merchant on the wallet home page until the user selects a different merchant.

Instant Offer Implementation

[0155] FIG. 7 illustrates a flow diagram illustrating an exemplary instant offer implementation according to an embodiment of the present invention. In this embodiment, a mobile commerce (MoCom) platform can be integrated with merchant POS system to implement a mechanism for users to select offers by using a wallet application and/or instant offers merchants make available to consumers.

Petitioner Exhibit 1002-0993

[0156] A wallet application running on a mobile device can be used to allow consumers to pay for purchases and present loyalty and offers via a payment terminal. One way a consumer can redeem an offer is by selecting the offer via the wallet application to be presented at checkout.

[0157] Consumers can also be provided with offers that can be instantly redeemed through the wallet application. Such offers are referred to herein as "instant offers". This feature allows merchants to reward consumers who use a mobile device running the wallet application to make purchases. Consumers benefit from the instant offer because, among other reasons, they do not need to specifically select an offer via the wallet application. Depending on the implementation, an instant offer can be used along with an offer explicitly selected by the consumer from the wallet application. Whether an offer is selected by the consumer or provided "instantly," a consumer identifier ("Consumer ID") value retrieved from the mobile device (*e.g.*, from secure element 112) is used as the key for retrieving and redeeming an instant offer.

[0158] Referring to FIG. 7, in one embodiment, a consumer selects offers from the wallet application to be presented at the checkout. At block 702, a payment is requested at a POS. If at block 704, it is determined that the payment is not a contactless payment, then at block 706 the payment process is completed via alternative means (*e.g.*, by using cash) and the checkout process is completed. If it is determined at block 704 that the payment will be a contactless payment, then the mobile device user is asked to tap his or her mobile device to the reader (*e.g.*, reader 120 described above).

[0159] In response, the mobile device is tapped to the reader. During the tap event, a number of data elements can be passed between the reader and a secure element on the mobile device as described above. In one embodiment, the payment card data, Consumer ID, loyalty number, and offer codes are passed to the reader during the tap of the reader. In this embodiment, Consumer ID is sent to the reader even if the tap is for a payment only transaction with no offers selected.

[0160] If at block 708 it is determined that a MoCom Consumer ID is not present, then at block 706 the payment process is completed and the checkout process is completed by processing the payment.

[0161] If it is determined at block 708 that a MoCom Consumer ID is present, then at block 710 a determination is made as to whether a MoCom offer is present (*e.g.*, an offer selected by the user via a wallet application). If at block 710 a determination is made that a MoCom offer is present, then a determination is made at block 712 as to whether a MoCom instant offer has been defined as well. If at block 712 it is determined that a MoCom instant offer has been defined, both the MoCom offer (*i.e.*, an offer selected by a user via a wallet application interface) and MoCom instant offer are processed, as shown in block 714. Once the MoCom offer and/or MoCom instant offer are processed, the payment associated with those offers is processed as shown at step 706.

[0162] If at block 710 a determination is made that a MoCom Offer is not present, then at block 716 a determination is made as to whether a MoCom instant offer has been defined. If not, the payment is completed as shown at step 706. If a determination is made at block 716 that the MoCom instant offer is present, the MoCom instant offer is processed as shown at block 718 and the payment associated with the MoCom instant offer processed as shown at block 706.

[0163] If a determination is made at block 712 that a MoCom instant offer has not been defined, then a standard MoCom offer is processed, as shown at block 720 and at block 706 the payment processed is completed.

[0164] The merchant POS system can use the presence of the ConsumerID to trigger the use of an instant offer. The offer could be, for example, a cents off or percentage off type offer that a merchant using the MoCom system defines. This can be, for example, applied for the purchase of a specific item. In an exemplary implementation, the merchant is provided an option of turning instant offer functionality off or on when a wallet offer is presented during the tap.

[0165] The instant offer can be defined by a merchant and then distributed to its retail locations. The offer can also have an associated specific start and end date.

The ability to distribute instant offers to different geographical areas can be taken into account as well.

Commerce Applet Package/Applet/Instance Management

[0166] The following section defines the AID values and application specific parameters used during download/installation of commerce applet 113 (FIG. 1). Table 20 defines AIDs.

TABLE 20 – AIDs

Description	AID
Package AID	A0 00 00 04 85 10 01 01
Applet AID	A0 00 00 04 85 10 01 01 00
Instance AID	A0 00 00 04 85 10 01 01 01

Applet-Specific Installation Parameters

[0167] The commerce applet's initial commerce services data characteristics may be provisioned via applet-specific installation parameters. This data follows the standard JavaCard AID and installation parameters.

These parameters must be coded as shown in Table 21:

TABLE 21 – Applet Installation Parameters

Provisioning Data	Byte Size	Default Value
Maximum Number of Loyalty Records	2	20
Maximum Number of Pre-Load Merchant Records	2	1
Maximum Number of Transaction Records	2	3
Total:	6	

Memory Requirements

[0168] Exemplary memory specifications are listed in Table 22 below. The first memory specification, "Package Download," indicates the approximate amount of non-volatile (EEPROM) memory space required to download the commerce applet package. The second memory specification, "Instantiation," indicates the amount of memory required to instantiate a new instance of the commerce applet.

Petitioner Exhibit 1002-0996

The final memory requirement, "Transient Data Space," indicates the amount of volatile (RAM) memory that is used by each instance of the commerce applet.

TABLE 22 – Applet Memory Requirements

Memory	Byte Size
Package Download	9396
Instantiation	6260
Transient Data Space	518

Data Management

[0169] The available commerce (*e.g.*, loyalty, offers, rewards, etc.) data is stored within the commerce applet 113 onboard the secure element 112. All of the relevant commerce data is stored in three separate data tables. These data tables are managed by the commerce applet 113. Additional commerce data may be stored/managed within a corresponding commerce widget 115 onboard the handset.

[0170] In one embodiment, the data elements defined herein have a variable length. Therefore, all elements (included those with a fixed length) will be assigned a maximum length. As a result, all lengths and byte size references should be interpreted as maximum values.

Commerce Data

[0171] Commerce applet 113 manages a few data fields that are shared by all commerce service applications. These data fields are stored in persistent data variables. An exemplary data element, Consumer ID, is defined in Table 23. Additional elements may be stored as well, such as consumer/platform keys and certificates.

TABLE 23

Variable	Type	Description
ConsumerID	byte[]	Unique consumer ID assigned to a specific MoCom consumer/user.

Loyalty Data Table

[0172] Commerce applet 113 also includes loyalty data tables enabling the storage/management of all consumer loyalty data.

[0173] Table 24 defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the loyalty data table.

TABLE 24 – Loyalty Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead
LOYALTY_PROGRAM_ID	0xDF41	8	3
LOYALTY_ACCOUNT_CODE	0xDF43	32	3
Total:		40	6
Minimum TLV Encoded Record Size:		46	

[0174] The data is stored in a record oriented data buffer, where the loyalty identifier ("Loyalty ID") is utilized as the key field for search/retrieval tasks.

[0175] In an exemplary embodiment, TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

[0176] In an alternative embodiment, an index (or hash table) may be created internally to speed up the Loyalty ID search task.

Cached Merchant Data Table

[0177] Commerce applet 113 also includes a merchant cached data table enabling the storage/management of all data related to a given merchant. This feature allows the commerce data for a given merchant to be pre-loaded by the wallet application 114 in order to improve performance.

[0178] Table 25 defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the cached merchant data table.

TABLE 25 – Cached Merchant Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead
MERCHANT_ID	0xDF31	8	3
LOYALTY_PROGRAM_ID	0xDF41	8	3
LOYALTY_ACCOUNT_CODE	0xDF43	32	3

Petitioner Exhibit 1002-0998

OFFER_ID	0xDF51	8	3
OFFER_CODE	0xDF53	130	3
.....			
Maximum		104	6
Minimum TLV Encoded Record Size:		110	

[0179] The data is stored in a record oriented data buffer, where the merchant identifier ("Merchant ID") is utilized as the key field for search/retrieval tasks. An index (or hash table) may be created internally to speed up the Merchant ID search task.

[0180] In an exemplary embodiment, TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

Transaction Log

[0181] Commerce applet 113 includes a transaction log that is used to track usage within the MoCom platform at the merchant point-of-sale. During commerce widget 115 and secure element 112 synchronization tasks, this transaction log is transmitted up to the commerce widget 115 for later over-the-air ("OTA") synchronization with the MoCom platform.

[0182] The actual content of the transaction log depends upon the Get Commerce Data command data/parameters provided by reader 120 during the transaction process at the merchant point-of-sale. An exact copy of the data payload sent to the commerce applet 113 by reader 120 via the Get Commerce Data APDU command is stored within that commerce transaction's record.

[0183] The transaction status is determined based on the logical result of the commerce data processing. If a data/processing error is detected within the commerce applet 113, the corresponding internal error code can be appended to the transaction log.

[0184] The following table defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the transaction log.

TABLE 26 – Transaction Log Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead

Petitioner Exhibit 1002-0999

Get Commerce Data command parameter(s)/data	xx	255	4
TRANSACTION_STATUS	0xDF62	3	3
Total:		266	7
Maximum TLV Encoded Record Size:		273	

[0185] The data is stored in a record oriented data buffer. A variable Get Commerce Data command data size is supported.

[0186] TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

Error Management

[0187] In an exemplary embodiment, error detection and management is handled at two levels. First, the response of the APDU command includes a two-byte Status Word result value. These responses are standardized and dictated by ISO 7816-4. However, a second level of error handling is managed internally by the Commerce Services applet. The second level of management includes the issuance of a standard 0x6909 status word in the response to the APDU command. Following this response, the client may issue a second command ("Get Internal Error Code") to obtain a two-byte internal error code. This code may be cross-referenced to Table 27. Table 27 provides details on where and why the error occurred within the applet.

[0188] Particularly, Table 27 provides a master list of all possible internal error codes returned by the Get Internal Error Code APDU command supported by the commerce applet.

TABLE 27 – Internal Error Codes

Error Code	Error Description
0x0101	SSE_INTERNAL_ERROR_APPLET_NOT_PROVISION
0x0102	SSE_INTERNAL_ERROR_COMMAND_NOT_ALLOWED_VIA_CONTACTLESS_INTERFACE
0x0103	SSE_INTERNAL_ERROR_COMMAND_NOT_ALLOWED_INVALID_CONTEXT
0x0201	SSE_INSTALL_INVALID_INSTALLATION_PARAMETER_LENGTH
0x0301	SSE_PARSE_COMMAND_DATA_INVALID_COMMERCE_TAG
0x0302	SSE_PARSE_COMMAND_DATA_INVALID_CONSUMER_ID_LENGTH

Petitioner Exhibit 1002-1000

0x0302	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_ID_LENGTH
0x0302	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_LOCATION_LENGTH
0x0303	SSE_PARSE_COMMAND_DATA_INVALID_DATE_TIME_STAMP_LENGTH
0x0304	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_COMMERCE_APP_VERSION_LENGTH
0x0305	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_CAPABILITIES_LENGTH
0x0306	SSE_PARSE_COMMAND_DATA_INVALID_LOYALTY_ID_LENGTH
0x0307	SSE_PARSE_COMMAND_DATA_INVALID_LOYALTY_ACCOUNT_CODE_LENGTH
0x0308	SSE_PARSE_COMMAND_DATA_INVALID_OFFER_ID_LENGTH
0x0309	SSE_PARSE_COMMAND_DATA_INVALID_OFFER_TYPE_CODE_LENGTH
0x030A	SSE_PARSE_COMMAND_DATA_INVALID_TRANSACTION_ID_LENGTH
0x030B	SSE_PARSE_COMMAND_DATA_INVALID_CACHED_MERCHANT_DATA_OFFER_COUNT_LENGTH
0x030C	SSE_PARSE_COMMAND_DATA_INVALID_CACHED_MERCHANT_DATA_LENGTH
0x030D	SSE_PARSE_COMMAND_DATA_INVALID_COMMERCE_TAG
0x0A01	SSE_GET_RESPONSE_REMAINING_DATA_INVALID_RESUME_STATE
0x0B01	SSE_VERIFY_REQUIRED_PARAMETERS_INVALID_PARAMETER_TAG
0x0B02	SSE_VERIFY_REQUIRED_PARAMETERS_DATE_TIME_STAMP_NOT_PRESENT
0x0B03	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_ID_NOT_PRESENT
0x0B04	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_STORE_ID_NOT_PRESENT
0x0B05	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_COMMERCE_APP_VERSION_NOT_PRESENT
0x0B06	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_CAPABILITIES_NOT_PRESENT
0x0B07	SSE_VERIFY_REQUIRED_PARAMETERS_LOYALTY_ID_NOT_PRESENT
0x0B08	SSE_VERIFY_REQUIRED_PARAMETERS_LOYALTY_ACCOUNT_CODE_NOT_PRESENT
0x0B0A	SSE_VERIFY_REQUIRED_PARAMETERS_CONSUMER_ID_NOT_PRESENT
0x0B0B	SSE_VERIFY_REQUIRED_PARAMETERS_CACHED_MERCHANT_DATA_OFFER_COUNT_NOT_PRESENT
0x0B0C	SSE_VERIFY_REQUIRED_PARAMETERS_EMBEDDED_TLV_CACHED_MERCHANT_DATA_NOT_PRESENT
0x0C01	SSE_GET_COMMERCE_DATA_INVALID_WALLET_STATE
0x0E01	SSE_UPDATE_CACHED_MERCHANT_DATA_FAILED_CMD_BUFFER_LENGTH_EXCEEDED
0x1101	LME_INVALID_LOYALTY_TAG
0x1102	LME_INVALID_LOYALTY_ID_LENGTH
0x1103	LME_INVALID_LOYALTY_ACCOUNT_CODE_LENGTH
0x1201	LME_GET_LOYALTY_DATA_RECORD_NOT_FOUND
0x1202	LME_GET_LOYALTY_DATA_INSUFFICIENT_BUFFER_LENGTH
0x1301	LME_UPDATE_LOYALTY_ID_NOT_SPECIFIED
0x1401	LME_DELETE_LOYALTY_ID_NOT_SPECIFIED
0x1402	LME_DELETE_LOYALTY_DATA_RECORD_NOT_FOUND

0x1501	LME_GET_LOYALTY_RECORD_INSUFFICIENT_BUFFER_LENGTH
0x3101	TLVME_MAX_DATA_LENGTH_EXCEEDED
0x3201	TLVME_APPEND_FAILED_INVALID_LENGTH
0x3301	TLVME_GET_NEXT_TAG_FAILED_INVALID_CONTEXT_NO_CURRENT_TAG
0x3401	TLVME_GET_TLV_OBJECT_FAILED_INVALID_TAG_CLASS
0x3402	TLVME_GET_TLV_OBJECT_FAILED_INVALID_LENGTH
0x3403	TLVME_GET_TLV_OBJECT_FAILED_TLV_LENGTH_NOT_SUPPORTED
0x3501	TLVME_GET_NEXT_ELEMENT_FAILED_INVALID_TAG_CLASS
0x3502	TLVME_GET_NEXT_ELEMENT_FAILED_TLV_LENGTH_NOT_SUPPORTED
0x3503	TLVME_GET_NEXT_ELEMENT_FAILED_INVALID_LENGTH
0x3504	TLVME_GET_NEXT_ELEMENT_FAILED_BUFFER_LENGTH_EXCEEDED
0x4101	DME_DATAMANAGER_INVALID_RECORD_NUMBER
0x4102	DME_DATAMANAGER_INVALID_RECORD_LENGTH
0x4103	DME_DATAMANAGER_RECORD_NOT_INITIALIZED
0x4104	DME_DATAMANAGER_RECORD_STORE_FULL
0x4105	DME_DATAMANAGER_INVALID_DATA_LENGTH
0x4106	DME_DATAMANAGER_INSUFFICIENT_BUFFER_SIZE
0x4201	DME_DATAMANAGER_PRIMARY_INDEX_NOT_ACTIVE
0x4202	DME_DATAMANAGER_PRIMARY_INDEX_KEY_NOT_SPECIFIED
0x4203	DME_DATAMANAGER_INVALID_PRIMARY_INDEX_KEY_LENGTH
0xA201	SUE_NO_INSTALL_PARAMETERS_FOUND
0xA202	SUE_INSUFFICIENT_APPLICATION_PARAMETER_BUFFER_LENGTH
0xA203	SUE_NO_APPLICATION_SPECIFIC_INSTALL_PARAMETERS_FOUND
0xD101	SSE_SECURITY_AUTHENTICATION_FAILED
0xD102	SSE_SECURITY_INVALID_CIPHER_DATA_LENGTH
0xD103	SSE_SECURITY_INVALID_KEY_DATA_LENGTH
0xD104	SSE_SECURITY_INVALID_DIVERSIFICATION_DATA_LENGTH
0xDC00	SSE_SECURITY_CRYPTO_EXCEPTION_UNDEFINED_REASON
0xDC01	SSE_SECURITY_CRYPTO_EXCEPTION_ILLEGAL_VALUE
0xDC02	SSE_SECURITY_CRYPTO_EXCEPTION_UNINITIALIZED_KEY
0xDC03	SSE_SECURITY_CRYPTO_EXCEPTION_NO_SUCH_ALGORITHM
0xDC04	SSE_SECURITY_CRYPTO_EXCEPTION_INVALID_INIT
0xDC05	SSE_SECURITY_CRYPTO_EXCEPTION_ILLEGAL_USE

Commerce Services

[0189] The following section provides a detailed description of the APDU commands available via the commerce applet 113.

APDU Commands

[0190] All communications/data exchanges with the commerce applet 113 will be performed via APDU commands as defined in the ISO 7816 standards. Additional restrictions and data handling are described below.

Command Usage Restrictions

[0191] For security reasons, a subset of the available commerce service commands can be restricted to specific connection modes. In one embodiment, referred to as "contact (wallet) mode," all of the APDU commands defined in Table 18 above are available. However, in contactless mode, the following commands are allowed:

- Get Version
- Get Internal Error Code
- Get Response (Remaining Data)
- Get Commerce Data

[0192] If any other APDU command is sent in contactless mode, an exception is thrown and the Internal Error Code is set to the corresponding invalid command mode value (0x0102).

[0193] In one embodiment, the Get Commerce Data command may only be successfully executed when wallet application 114 is open. When the wallet application 114 is either started or terminated by the consumer, it is the responsibility of the wallet application 114 to notify a wallet companion applet (WCAp) so that it can perform monitoring, management and/or security functions. The WCAp applet, in turn, notifies the commerce applet of the wallet application state via a shared interface. WCAp applets are discussed in U.S. Pat. Appln. No. 13/857,400 entitled "Systems, Methods, and Computer Program Products For Securing And Managing Applications On Secure Elements," which is hereby incorporated by reference in its entirety.

Data Payload Management

[0194] Commerce applet 113 validates that all required parameters have been included in the data payload. However, in most cases all non-relevant data elements can be ignored and a command will still process normally. In one

Petitioner Exhibit 1002-1003

embodiment, the length expected (Le) value is not verified by the commerce applet 113. It can be assumed to be the value zero, allowing the commerce applet 113 to send all available data via the response.

Get Version

[0195] The Get Version command is used to obtain the version information of the currently loaded commerce applet 113. The version will be stored in three bytes (xx.yy.zz), where xx = release version, yy = major version (Wave) number, and zz = minor version number. This information is assigned by, for example, a MoCom platform system, specified during applet development or packaging, or stored as a static value within the code, and cannot be changed.

[0196] Table 28 defines the settings for the Get Version APDU command:

TABLE 28 – Internal Get Version

CLA	INS	P1	P2	Lc	Data	Le
90	10	00	00	00	*<none>*	3

[0197] In one embodiment, no data is sent to the commerce applet. The Lc data length is 0x00.

[0198] The version information is contained within a three-byte response. The Le data length is 0x03. A length of 0x00 is also allowed. Exemplary response data elements are defined in Table 29:

TABLE 29 – Response Data

Data Element	Byte Size	Value
Commerce Specification Version Tag	1	0xDF12
Commerce Specification Version Length	1	3
Commerce Specification Version Value	3	[Version (xx.yy.zz)]
Total:	5	

[0199] Table 30 defines the possible Status Word values that may be returned by this command.

TABLE 30 – Status Codes

SW1	SW2	Description

Petitioner Exhibit 1002-1004

90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Provision Applet

[0200] An applet provisional command, "Provision Applet," allows the provisioning (or update) of the consumer related data, including the consumer ID and optionally related security data (key value and certificates). The new/updated data values are specified via the command data. In an exemplary embodiment, the Provision Applet command may only be used to update the Consumer ID.

[0201] Tables 31 and 32 define the settings for the Provision Applet APDU command:

TABLE 31 – Provision Applet

CLA	INS	P1	P2	Lc	Data	Le
90	12	00	00	XX	TLV-Encoded Provisioning Data	00

[0202] The incoming data, illustrated in table 31, consists of the TLV encoded provisioning data. Therefore, the Lc data length is variable.

[0203] In one embodiment, no data is returned by the commerce applet 113. The Le data length is 0x00.

TABLE 32 – Command Data

Data Element	Byte Size	Value
Provisioning Data Element Tag	1	[Element Tag]
Element Data Length	1	xx
Element Data Value	xx	[Data]
.....		
Total:	<var>	

[0204] Table 33 defines the possible Status Word values that may be returned by Provision Applet command

TABLE 33 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length

Petitioner Exhibit 1002-1005

69	09	Internal Error

Get Consumer Info

[0205] The Get Consumer Info command is used to obtain a subset of static data related to the token owner (*i.e.*, consumer). This data includes the following:

Consumer Identifier

[0206] Table 34 defines the settings for the Get Consumer Info APDU command:

TABLE 34 – Get Consumer Info

CLA	INS	P1	P2	Lc	Data	Le
90	14	00	00	00	*<none>*	00

[0207] No data is sent to the commerce applet 113. The Lc data length is, for example, 0x00. The actual length of the requested consumer information returned by the applet is variable, specific to the available consumer data. Therefore, the Le data length is 0x00, allowing the applet to manage a variable length response.

[0208] The response data is returned as a TLV formatted data steam. The Consumer ID may also be returned.

TABLE 35 – Response Data

Data Element	Byte Size	Value
Consumer ID Tag	1	0XDF21
Consumer ID Length	1	16
Consumer ID	16	[Consumer ID]
Total:	<var>	

[0209] Table 36 defines the possible Status Word values that may be returned by this command.

TABLE 36 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Petitioner Exhibit 1002-1006

Get Commerce Data

[0210] The Get Commerce Data command provides commerce information (*e.g.*, loyalty, offers and rewards) for a specified merchant (or set of merchants), based on the specified merchant/loyalty identifiers and supported offer types. This command provides a single point of contact for reader 120 attached to the merchant POS system (*e.g.*, POS terminal).

[0211] A date/time stamp, merchant ID, store ID, commerce protocol version, and merchant capabilities byte can be sent as part of the incoming data. Additional loyalty identifiers may also be sent in order to specify (filter) the loyalty information requested. The applet shall search a loyalty data table (Table 5), for the specified merchant/loyalty program ID(s) and retrieve the corresponding loyalty data. Additional offer type codes may be also sent as part of the incoming data in order to specify the type of offer information requested. The commerce applet 113 searches the cached merchant data table (Table 25) for the specified merchant identifier/offer code(s) and retrieves the corresponding offer data.

Required Parameters include:

- Date/Time Stamp
- Merchant ID
- Store ID
- App Version

[0212] Once transmission has been successfully completed, the applet shall create an entry in its transaction log recording the commerce data request.

[0213] Tables 37 and 38 define the settings for the Get Commerce Data APDU command:

TABLE 37 – Get Commerce Data

CLA	INS	P1	P2	Lc	Data	Le
90	50	00	00	xx		00

Petitioner Exhibit 1002-1007

[0214] The incoming data consists of a date/time stamp (used for transaction logging), merchant identifier, store identifier, merchant capabilities byte, and an optional set of additional data elements, including one or more additional loyalty identifiers (indicating loyalty programs supported by the merchant location), and additional offer codes (indicating the type of offers supported by the merchant location). In one embodiment, if a merchant does not specify a Merchant Capability parameter, a default mode supporting only merchant based loyalty and offers is used.

[0215] The actual length of the requested commerce data returned by the applet is variable specific to the available loyalty/offers related data. Therefore, the Le data length is 0x00, allowing the applet to manage a variable length response.

TABLE 38 – Command Data

Data Element	Byte Size	Value
Date/Time Stamp Tag	1	0xDF11
Date/Time Stamp Length	1	7
Date/Time Stamp	7	[Date/Time Stamp]
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID	8	[Merchant ID]
Store ID Tag	1	0x32
Store ID Length	1	32
Store ID	32	[Store ID]
Commerce Version Tag	1	0xDF12
Commerce Version Length	1	3
Commerce Version Data	2	[Commerce App Version]
Merchant Capability Tag	1	0xDF33
Merchant Capability Length	1	2
Merchant Capability Data	1	[Merchant Capability Code]
Transaction ID Tag	1	0xDF61
Transaction ID Length	1	16
Transaction ID	16	[Transaction ID]
Additional Loyalty ID Tag	1	0xDF41
Additional Loyalty ID Length	1	8
Additional Loyalty ID	8	[Loyalty ID]
.....		
Additional Offer Type Tag	1	0xDF54
Additional Offer Type Length	1	9
Additional Offer Type Code	9	[Offer Type Code]

Petitioner Exhibit 1002-1008

.....		
Total:	<var>	

[0216] The response data is returned as a TLV formatted data steam. The MoCom platform-specific consumer identifier and all relevant loyalty/offers data are returned in a single data payload.

Consumer ID

[0217] The Consumer ID is sent in TLV format, where the data is sent using the tag CONSUMER_ID (0XDF21). In one embodiment, unless an error is detected, the consumer ID shall always be returned.

Loyalty

[0218] In one embodiment, each instance of loyalty data shall consist of the following TLV encoded data elements:

- Loyalty Identifier
- Loyalty Account Code

[0219] Within this data stream, the first tag shall contain the Loyalty Identifier tag (*T*) byte (0xDF41). The length (*L*) byte shall specify the length of the Loyalty Identifier. The value (*V*) shall contain the actual Loyalty Identifier of *L* length for the corresponding Loyalty Data that will immediately follow.

[0220] The second tag should contain the Loyalty Account Code tag (*T*) byte (0xDF43). The length (*L*) byte shall specify the total length of the account code data linked to the previous Loyalty Identifier. The value (*V*) shall contain the actual loyalty data of *L* length.

[0221] Any additional loyalty identifiers found within the loyalty data table are appended to the TLV encoded data payload using this same format.

Offers

[0222] Each instance of offer data shall consist of the following TLV encoded data elements:

- Offer ID
- Offer Code

[0223] Within this data stream, the first tag contains the Offer ID tag (*T*) byte (0xDF51). The length (*L*) byte specifies the length of the Offer ID. The value (*V*) contains the Offer ID for the corresponding offer data that will immediately follow.

[0224] The second tag preferably contains the Offer Code tag (*T*) byte value (0xDF53). The length (*L*) byte specifies the length of the Offer Type Code. The value (*V*) contains the Offer Code data for the corresponding Offer ID.

[0225] Any additional offer identifiers found within the offer data table are appended to the TLV encoded data payload using this same format. Exemplary response data is defined in Table 39.

TABLE 39 – Response Data

Data Element	Byte Size	Value
Consumer Identifier Tag	1	0XDF21
Consumer Identifier Length	1	16
Consumer Identifier	16	[Consumer ID]
Loyalty Identifier Tag	1	0xDF41
Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	32
Loyalty Account Code	32	[Acct Code]
.....		
Offer ID Tag	1	0xDF51
Offer ID Length	1	8
Offer ID Value	8	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	130
Offer Code Value	130	[Offer Code]
.....		
Total:	<var>	

[0226] Commerce applet 113 manages the transmission of multiple response packets (using the Get Response command) when the total data length exceeds 256 bytes. Table 40 defines the possible Status Word values that may be returned by the Get Response command.

TABLE 40 – Status Codes

SW1	SW2	Description

Petitioner Exhibit 1002-1010

90	00	Successful Execution of Command
61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
69	09	Internal Error

Post Transaction Data

[0227] The Post Transaction Data command provides a method through which the Merchant PoS system or payment terminal may return post-transaction data, including redeemed coupons, new offers, e-receipts, or other enhanced commerce data.

[0228] Tables 41 and 42 define the settings for the Post Transaction Data APDU command:

TABLE 41 – Post Transaction Data

CLA	INS	P1	P2	Lc	Data	Le
90	52	00	00	xx	<TLV-Encoded Transaction Data>	00

[0229] The incoming data consists of the TLV encoded provisioning data and a platform signature for authenticity purposes. Therefore, the Lc data length is variable.

[0230] Data need not be returned by commerce applet 113. The Le data length is 0x00.

TABLE 42 – Command Data

Data Element	Byte Size	Value
Post Transaction Data Element Tag	1	[Element Tag]
Element Data Length	1	xx
Element Data Value	xx	[Data]
.....		
Total:	<var>	

[0231] Table 43 defines the possible Status Word values that may be returned by the Post Transaction Data command.

TABLE 43 – Status Codes

SW1	SW2	Description

90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Get Transaction Log

[0232] The Get Transaction Log is used to obtain all data stored in the transaction log. This command is typically used by the commerce widget for the purpose of widget and secure element data synchronization tasks.

[0233] Table 44 defines the settings for the Get Transaction Log APDU command:

TABLE 44 – Get Transaction Log

CLA	INS	P1	P2	Lc	Data	Le
90	54	00	0x	00	*<none>*	

P2 Value	Applet Behavior
0x00	Normal processing.
0x01	Clear transaction log. No data transmitted.
0x02	Get Transaction Log Status

[0234] In one embodiment, no data is sent to the commerce applet. The Lc data length is 0x00. The actual length of the transaction data returned by the applet is variable, depending on the number of transaction records and the variable length of the corresponding transaction log data. Therefore, the Le data length can be 0x00, allowing commerce applet 113 to manage variable length response.

[0235] Preferably, response data is returned as a TLV formatted data steam.

Transaction Log Response Data

[0236] Each transaction log record shall consist of an Embedded-TLV Transaction Log tag followed by all related data elements. The data elements included in the transaction record are a mirror of those provided during the corresponding Get Commerce Data command requested by the Commerce-enabled payment terminal (NFC reader) at the merchant point-of-sale. Additional transaction log records are appended to the data using the same format. Table 45 illustrates exemplary response data.

Petitioner Exhibit 1002-1012

TABLE 45 – Response Data

Data Element	Byte Size	Value
Embedded TLV Transaction Record Tag	1	0xDF60
Embedded TLV Transaction Record Length	3	xx
TLV-encoded transaction data	xx	xx
.....		
Total:	<var>	

[0237] In one embodiment, commerce applet 113 manages the transmission of multiple response packets using the Get Response command when the total data length exceeds 256 bytes.

Transaction Log Status Response Data

[0238] When the transaction log status is requested, the commerce applet responds with status information within an embedded TLV data payload. This data includes the number of available transaction log records, loyalty and offer records sent during the last transaction. This is the same data payload provided to WCAp via the shared interface. Table 46 illustrates exemplary response data.

TABLE 46 – Response Data

Data Element	Byte Size	Value
Embedded TLV Transaction Status Tag	1	0xE4
Embedded TLV Transaction Record Length	1	0x0C
Transaction Record Count Tag	1	0xDB
Transaction Record Count Length	1	0x02
Transaction Record Count Value	2	xx
Last Transaction Loyalty Count Tag	1	0xDC
Last Transaction Loyalty Count Length	1	0x02
Last Transaction Loyalty Count Value	2	xx
Last Transaction Offer Count Tag	1	0xDD
Last Transaction Offer Count Length	1	0x02
Last Transaction Offer Count Value	2	xx
Total:	14	

[0239] Table 47 defines possible Status Word values that may be returned by the Get Transaction Log command.

TABLE 47 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command

Petitioner Exhibit 1002-1013

61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
6B	00	Wrong P1/P2 Parameter
69	09	Internal Error

Get Internal Error Code

[0240] The Get Internal Error Code command is used to retrieve the last internal error code generated by the Commerce Services applet. This code provides a value that can be cross-referenced with the Internal Error Codes table (Table 26), providing a more specific description of the error. This command is used for more detailed diagnostic and error resolution.

[0241] Table 48 defines the settings for the Get Internal Error Code APDU command:

TABLE 48 – Get Internal Error Code

CLA	INS	P1	P2	Lc	Data	Le
90	70	00	00	00	*<none>*	02

[0242] In one embodiment, no data is sent to the applet. The Lc data length is 0x00. The error code is contained within a two-byte response. Therefore, the Le data length is 0x02.

[0243] The following table defines the possible Status Word values that may be returned by this command.

TABLE 49 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Loyalty Services

Get Loyalty Data

[0244] The Get Loyalty Data command defined in Tables 50 and 51 is used to obtain the stored loyalty information based on a specified loyalty identifier. The

two-byte loyalty identifier may be sent as part of the incoming data in order to specify the loyalty information requested. Commerce applet 113 searches a table of loyalty data for the specified merchant/loyalty ID and retrieves all of the corresponding loyalty data.

TABLE 50 – Get Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	30	00	00	xx	[TLV-Encoded Loyalty ID]	00

[0245] The (optional) incoming data shall consist of a TLV encoded loyalty identifier indicating the loyalty information requested. If Lc is set to 0x00 (no data incoming data is specified), all available loyalty identifiers are returned.

[0246] The actual length of the requested loyalty data returned by the applet is variable specific to the requested/available loyalty data. Therefore, the Le data length is 0x00, allowing the applet to manage a variable length response.

TABLE 51 - Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Loyalty Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Total:	<var>	

[0247] The response data (Table 51) is returned as a TLV formatted data stream. All of the relevant loyalty data is returned in a single data payload.

[0248] In one embodiment, if a loyalty data dump is requested (Lc = 0x00), a list of all Loyalty Identifiers is returned in LV (no tag) format. Thus, only the Loyalty Identifier for each entry is included in the data payload.

[0249] Each instance of loyalty data includes the following data elements:

- Loyalty Identifier
- Loyalty Account Code

TABLE 52 – Response Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41

Petitioner Exhibit 1002-1015

Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	xx
Loyalty Account Code	xx	[Acct Code]
Total (Max):	<var>	

[0250] Table 53 defines the possible Status Word values that may be returned by this command.

TABLE 53 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
69	09	Internal Error

Update Loyalty Data

[0251] The Update Loyalty Data command is used to add or update the specified merchant loyalty data. The data is sent as TLV formatted data stream. If the specified loyalty identifier exists, the corresponding loyalty data elements are updated. If the loyalty identifier does not exist, a new data record is created in the loyalty data table. Tables 54 and 55 define the settings for the Update Loyalty Data APDU command:

TABLE 54 – Update Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	32	00	00	xx	TLV-Encoded Loyalty Data	00

[0252] The incoming data shall consist of TLV encoded loyalty data. Therefore, the Lc data length is variable. In one embodiment, no data is returned by the applet. The Le data length is be 0x00.

TABLE 55 – Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Identifier Length	1	8

Petitioner Exhibit 1002-1016

Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	xx
Loyalty Account Code	Xx	[Acct Code]
Total:	<var>	

[0253] Table 56 defines the possible Status Word values that may be returned by this command.

TABLE 56 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Delete Loyalty Data

[0254] The Delete Loyalty Data command is used to delete the specified merchant loyalty data. The one-byte merchant code is specified via the command data. Alternatively, the P2 byte may be used to purge all existing offers. If P2 is set to 0xFF, the entire offer data store is deleted.

[0255] Tables 57 and 58 define the settings for the Delete Loyalty Data APDU command:

TABLE 57 – Delete Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	34	00	xx	xx	TLV-Encoded Loyalty ID	00

[0256] The incoming data consists of a TLV-encoded loyalty identifier. Therefore, the Lc data length is variable.

[0257] In one embodiment, no data is returned by commerce applet 113. The Le data length is 0x00.

TABLE 58 – Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Loyalty Identifier Length	1	xx
Loyalty Identifier	Xx	[Loyalty ID]
Total:	<var>	

Petitioner Exhibit 1002-1017

P2 Value	Applet Behavior
0x00	Normal processing.
0xFF	Purge loyalty table (delete all records)

[0258] Table 59 defines the possible Status Word values that may be returned by the Delete Loyalty Data command.

TABLE 59 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Merchant Cached Data Services

Get Cached Merchant Data

[0259] The Get Cached Merchant Data command is used to obtain all previously loaded data pertaining to a specific merchant. The merchant identifier may be sent as part of the incoming data in order to specify the pre-loaded data requested. If provided, the commerce applet searches a table of cached merchant data for the specified merchant ID and retrieves all of the corresponding data. This command may also be used to obtain information on all cached merchants stored within the Commerce Services applet.

[0260] Table 60 defines the settings for the Get Cached Merchant Data APDU command:

TABLE 60 – Get Cached Merchant Data

CLA	INS	P1	P2	Lc	Data	Le
90	56	00	00	xx	<none>	00

[0261] In one embodiment, no data is sent to the applet. The Lc data length is 0x00. The actual length of the requested cached merchant data returned by the applet is variable, specific to the requested/available cached merchant data. Therefore, the Le data length is 0x00; allowing the applet to manage a variable length response.

[0262] The response data (Table 61) may be returned as a TLV formatted data stream. All of the cached data is returned in a single data payload. Each instance of cached merchant data includes the following corresponding cached merchant data elements (if available):

- Merchant Identifier
- Loyalty Identifier
- Loyalty Account Code
- Offer Identifier(s)
- Offer Code(s)

TABLE 61 – Response Data

Data Element	Byte Size	Value
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID	8	[Merchant ID]
Loyalty ID Tag	1	0xDF41
Loyalty ID Length	1	8
Loyalty ID Value	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Loyalty Account Code Length	1	32
Loyalty Account Code Value	32	[Loyalty Account Code]
.....		
Offer ID Tag	1	0xDF51
Offer ID Length	1	xx
Offer ID Value	Xx	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	xx
Offer Code Value	Xx	[Offer Code]
.....		
Total:	<var>	

[0263] In an exemplary embodiment, the cached merchant data will be loaded/managed by the wallet application and may include multiple offer IDs/codes pertaining to that specific merchant. However, the applet shall prefix the consumer identifier to the response data and append any additional loyalty/offer data requested by the Get Commerce Data command.

[0264] Table 62 defines the possible Status Word values that may be returned by this command.

Petitioner Exhibit 1002-1019

TABLE 62 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Update Cached Merchant Data

[0265] The Update Cached Merchant Data command is used to update the cached (quick-response) data for a specified merchant. The data is sent as TLV formatted data stream, similar to the response data returned by the Get Commerce Data command. This command is used to pre-load a given merchant's Get Commerce Data response.

[0266] Tables 63 and 64 define the settings for the Update Cached Merchant Data APDU command:

TABLE 63 – Update Cached Merchant Data

CLA	INS	P1	P2	Lc	Data	Le
90	58	00	0x	xx	TLV-Encoded Cached Merchant Data]	02

P2 Value	Applet Behavior
0x00	Normal processing.
0x01	APDU Chain (data will be appended to CMD buffer)
0Xff	Delete cached merchant data [Lc = 0]

[0267] The incoming data consists of embedded TLV encoded cached merchant data. Therefore, the Lc data length is variable.

[0268] Commerce applet returns a two byte response containing the number of available bytes remaining in the cached merchant data buffer. Therefore, the Le data length is 0x02 (or 0x00).

TABLE 64 – Command Data

Data Element	Byte Size	Value
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID Value	8	[Merchant ID]
Cached Merchant Data Offer Count Tag	1	0x57
Cached Merchant Data Offer Count Length	1	1
Cached Merchant Data Offer Count Value	1	[CMD Offer Count]
Embedded TLV Cached Merchant Data Tag	1	0x58
Embedded TLV Cached Merchant Data Length	Xx	xx
Offer ID Tag	1	0xDF51
Offer ID Length	1	xx
Offer ID Value	Xx	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	xx
Offer Code Value	Xx	[Offer Code]
.....		
Total:	<var>	

[0269] The response data (Table 65) returned by the command consists of a 2-byte (short) value representing the number of remaining bytes available in the cached merchant data buffer. This allows the wallet application 114 to manage how many cached offers can "fit" into the Commerce Services applet.

TABLE 65 – Response Data

Data Element	Byte Size	Value
Available Cached Merchant Data Buffer (bytes) Size	2	xx
Total:	2	

[0270] Table 66 defines the possible Status Word values that may be returned by this command.

TABLE 66 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

[0271] Table 67 defines the data elements and corresponding tag values and target/max byte sizes used by commerce based applications according to the example aspects described herein. Additional values have been provided for those elements with a limited/fixed value range.

TABLE 67

Commerce Services			
Shared Data Elements			
Data Element	Tag	Max Size	Description
DATE_TIME_STAMP	0x11	7	Date/Time stamp
COMMERCE_APP_VERSION	0x12	3	Supported Commerce App Version Number
Consumer Data Elements			
Data Element	Tag	Max Size	Description
CONSUMER_ID	0x21	16	MoCom Platform specific consumer identifier
CONSUMER_KEY	0x22	16	MoCom Platform generated consumer specific 3DES key
CONSUMER_CERT	0x23	8	MoCom Platform generated consumer signature/ certificate
Merchant Data Elements			
Data Element	Tag	Max Size	Description
MERCHANT_ID	0x31	8	MoCom Platform specific merchant identifier
MERCHANT_STORE_ID	0x32	32	MoCom Platform specific merchant store identifier
MERCHANT_CAPABILITY	0x33	2	Supported Commerce App Services
READER_START_MODE	0x34	2	NFC enabled payment terminal startup mode (provided by Merchant POS System during init)
Merchant Capabilities			
Data Element	Value	Max Size	Description
MERCAP_MERCHANT_LOYALTY	0x80	1	The Get Commerce Data includes a valid merchant identifier used to determine the Loyalty data received by the applet.
MERCAP_ADDITIONAL_	0x40	1	The Get Commerce Data request

Petitioner Exhibit 1002-1022

LOYALTY			includes additional Loyalty Identifiers. Additional Loyalty data is determined by the specified Loyalty ID(s).
MERCAP_MERCHANT_ OFFERS	0x20	1	Offer type fields aincluded in Get Commerce Data request
MERCAP_ADDITIONAL_ OFFERS	0x10	1	The Get Commerce Data includes a valid merchant identifier used to determine the offers data received by the applet.
MERCAP_PAYMENT	0x08	1	Merchant supports contactless payment.
MERCAP_CLOUD	0x02	1	The merchant supports cloud redemption. Only the Consumer ID will be returned by the applet for resolution in the cloud.
MERCAP_REDEMPTION	0x01	1	The Merchant & Payment Terminal support the transmission of offer redemption data (from the ECR) to the applet via the Post Transaction command.
MoCom Platform Data Elements			
PLATFORM_SIGNATURE	0x71	8	MoCom Platform generated MAC/Signature appended to command/data originating from the platform for remote verification purposes (data integrity/ authenticity).
PLATFORM_KEY	0x72	16	MoCom Platform Key
PLATFORM_CERT	0x73	8	MoCom Platform Certificate

Loyalty			
Loyalty Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ LOYALTY_DATA	0x40	xx	Embedded TLV loyalty data tag
LOYALTY_ID	0x41	8	MoCom Platform specific loyalty identifier
LOYALTY_STATUS	0x42	1	Loyalty card/account status (see below)
LOYALTY_ACCOUNT_ CODE	0x43	32	Loyalty account (barcode data)
LOYALTY_MAC_ SIGNATURE	0x44	8	MoCom Platform specific MAC/Signature for integrity/

Petitioner Exhibit 1002-1023

			authenticity verification
Loyalty Status			
Data Element	Value	Max Size	Description
LOYALTY_STATUS_ DEACTIVATED	0x00	1	Loyalty account inactive. Not available.
LOYALTY_STATUS_ ACTIVE	0x01	1	Loyalty account active. Available for use.

Transaction Log			
Transaction Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ TRANSACTION_LOG	0x60	xx	Transaction log record data tag
TRANSACTION_ID	0x61	16	Transaction ID (assigned by ECR)
TRANSACTION_STATUS	0x62	11	Transaction status; including status byte (see below), 2-byte status word, 2-byte internal error code, 2-byte number of available transaction records, 2-byte last transaction loyalty count, 2-byte last transaction offer count
Transaction Status			
Data Element	Value	Max Size	Description
TRANSACTION_STATUS_SU CCESSFUL	0x00	1	Commerce data received. Result pending.
TRANSACTION_STATUS_FA ILED	0x01	1	Error detected. Internal error code appended.

Offers			
Offer Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ OFFER_DATA	0x50	xx	Embedded TLV offer data tag
OFFER_ID	0x51	8	MoCom Platform specific offer identifier
OFFER_STATUS	0x52	1	Offer status (see below)
OFFER_CODE	0x53	48	Offer (UPC/EPC/GS1 Databar) barcode data
OFFER_TYPE_CODE	0x54	9	Offer Type (see below)
OFFER_MAC_ SIGNATURE	0x55	8	MoCom Platform specific data security signature

OFFER_UPDATE_FLAG	0x56	1	Update flag (synchronization status)
CACHED_MERCHANT_DATA_OFFER_COUNT	0x57	1	Offer Count within Cached Merchant Data
EMBEDDED_TLV_CACHED_MERCHANT_DATA	0x58	xx	Embedded TLV Cached Merchant (Offer) Data
Offer Status			
Data Element	Value	Max Size	Description
OFFER_STATUS_DEACTIVATED	0x00	1	Offer present in data store, but not available for redemption.
OFFER_STATUS_ACTIVE	0x01	1	Offer present in data store. Available for redemption.
OFFER_STATUS_EXPIRED	0x10	1	Expired Offer
OFFER_STATUS_SUBMITTED	0x20	1	Offer has been presented for redemption. Result pending.
OFFER_STATUS_REDEEMED	0x40	1	Offer has been redeemed.
Offer Type			
Data Element	Value	Max Size	Description
OFFER_TYPE_CLASS_01	0x01	1	Offer Class: Merchant Specific (merchant ID appended)
OFFER_TYPE_CLASS_02	0x02	1	Offer Class: CPG
OFFER_TYPE_CLASS_03	0x03	1	Offer Class: Misc

Specially Formatted Data Elements

[0272] A few of the data elements included in the commerce data payload include a format byte that identifies the data encoding used for that element. The data encoding is specified by the merchant to ensure compatibility at the point of sale. The formatted data value is supplied by the MoCom platform to the wallet application. Thus, no additional interpreting/formatting is necessary between the platform, wallet, secure element, and payment terminal. It is the role of the payment terminal (or merchant POS system) to properly interpret the data and supply it to the merchant system for processing.

[0273] The following data elements shall include the format byte:

- Loyalty Account Code
- Offer Code

[0274] Table 68 defines the possible format byte values and their corresponding encoding rule:

TABLE 68

Format Byte	Encoding Rule	Description
0x00	Hexadecimal	Each byte of data is encoded in (raw) hexadecimal format.
0x01	Binary Coded Decimal (BCD)	Each nibble represents a single digit. Thus, only decimal values are specified. A data stream containing an odd number (length) of digits includes the hex value 'F' in the first nibble of the data stream.
0x02	ASCII	Each byte represents an ACII value that is interpreted as such and handled as its corresponding CHAR value. In most cases, these data streams will be converted into a String before being passed to the merchant POS system for processing.

[0275] A BCD encoded data value that includes the hexadecimal value 'F' in the first nibble shall identify a data stream containing an odd number of digits. Thus, the BCD data stream *12345* is encoded in 3 byte buffer as follows: *0xF12345*.

Computer Readable Medium Implementation

[0276] The example embodiments described above such as, for example, the systems and procedures depicted in or discussed in connection with FIGs. 1- 7 or any part or function thereof, may be implemented by using hardware, software or a combination of the two. The implementation may be in one or more computers or other processing systems. While manipulations performed by these example embodiments may have been referred to in terms commonly associated with mental operations performed by a human operator, no human operator is needed to perform any of the operations described herein. In other words, the operations may be completely implemented with machine operations. Useful machines for performing the operation of the example embodiments presented herein include general purpose digital computers or similar devices.

[0277] FIG. 8 is a block diagram of a general and/or special purpose computer 800, in accordance with some of the example embodiments of the invention. The computer 800 may be, for example, a user device, a user computer, a client computer and/or a server computer, among other things.

[0278] The computer 800 may include without limitation a processor device 810, a main memory 825, and an interconnect bus 805. The processor device 810 may include without limitation a single microprocessor, or may include a plurality of microprocessors for configuring the computer 800 as a multi-processor system. The main memory 825 stores, among other things, instructions and/or data for execution by the processor device 810. The main memory 625 may include banks of dynamic random access memory (DRAM), as well as cache memory.

[0279] The computer 800 may further include a mass storage device 830, peripheral device(s) 840, portable storage medium device(s) 850, input control device(s) 880, a graphics subsystem 860, and/or an output display 870. For explanatory purposes, all components in the computer 800 are shown in FIG. 8 as being coupled via the bus 805. However, the computer 800 is not so limited. Devices of the computer 800 may be coupled via one or more data transport means. For example, the processor device 810 and/or the main memory 825 may be coupled via a local microprocessor bus. The mass storage device 830, peripheral device(s) 840, portable storage medium device(s) 850, and/or graphics subsystem 860 may be coupled via one or more input/output (I/O) buses. The mass storage device 830 may be a nonvolatile storage device for storing data and/or instructions for use by the processor device 810. The mass storage device 830 may be implemented, for example, with a magnetic disk drive or an optical disk drive. In a software embodiment, the mass storage device 830 is configured for loading contents of the mass storage device 830 into the main memory 825.

[0280] The portable storage medium device 850 operates in conjunction with a nonvolatile portable storage medium, such as, for example, a compact disc read only memory (CD-ROM), to input and output data and code to and from the computer 800. In some embodiments, the software for storing an internal identifier in metadata may be stored on a portable storage medium, and may be inputted into the computer 800 via the portable storage medium device 850. The

Petitioner Exhibit 1002-1027

peripheral device(s) 840 may include any type of computer support device, such as, for example, an input/output (I/O) interface configured to add additional functionality to the computer 800. For example, the peripheral device(s) 840 may include a network interface card for interfacing the computer 800 with a network 820.

[0281] The input control device(s) 880 provide a portion of the user interface for a user of the computer 800. The input control device(s) 880 may include a keypad and/or a cursor control device. The keypad may be configured for inputting alphanumeric characters and/or other key information. The cursor control device may include, for example, a mouse, a trackball, a stylus, and/or cursor direction keys. In order to display textual and graphical information, the computer 800 may include the graphics subsystem 860 and the output display 870. The output display 870 may include a cathode ray tube (CRT) display and/or a liquid crystal display (LCD). The graphics subsystem 860 receives textual and graphical information, and processes the information for output to the output display 870.

[0282] Each component of the computer 800 may represent a broad category of a computer component of a general and/or special purpose computer. Components of the computer 800 are not limited to the specific implementations provided here.

[0283] Portions of the example embodiments of the invention may be conveniently implemented by using a conventional general purpose computer, a specialized digital computer and/or a microprocessor programmed according to the teachings of the present disclosure, as is apparent to those skilled in the computer art. Appropriate software coding may readily be prepared by skilled programmers based on the teachings of the present disclosure.

[0284] Some embodiments may also be implemented by the preparation of application-specific integrated circuits, field programmable gate arrays, or by interconnecting an appropriate network of conventional component circuits.

[0285] Some embodiments include a computer program product. The computer program product may be a storage medium or media having instructions stored thereon or therein which can be used to control, or cause, a computer to perform

any of the procedures of the example embodiments of the invention. The storage medium may include without limitation a floppy disk, a mini disk, an optical disc, a Blu-Ray Disc, a DVD, a CD-ROM, a micro-drive, a magneto-optical disk, a ROM, a RAM, an EPROM, an EEPROM, a DRAM, a VRAM, a flash memory, a flash card, a magnetic card, an optical card, nanosystems, a molecular memory integrated circuit, a RAID, remote data storage/archive/warehousing, and/or any other type of device suitable for storing instructions and/or data.

[0286] Stored on any one of the computer readable medium or media, some implementations include software for controlling both the hardware of the general and/or special computer or microprocessor, and for enabling the computer or microprocessor to interact with a human user or other mechanism utilizing the results of the example embodiments of the invention. Such software may include without limitation device drivers, operating systems, and user applications. Ultimately, such computer readable media further includes software for performing example aspects of the invention, as described above.

[0287] Included in the programming and/or software of the general and/or special purpose computer or microprocessor are software modules for implementing the procedures described above.

[0288] While various example embodiments of the invention have been described above, it should be understood that they have been presented by way of example, and not limitation. It is apparent to persons skilled in the relevant art(s) that various changes in form and detail can be made therein. Thus, the invention should not be limited by any of the above described example embodiments, but should be defined only in accordance with the following claims and their equivalents.

[0289] In addition, it should be understood that the figures are presented for example purposes only. The architecture of the example embodiments presented herein is sufficiently flexible and configurable, such that it may be utilized and navigated in ways other than that shown in the accompanying figures.

[0290] Further, the purpose of the Abstract is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientists, engineers and practitioners in the art who are not familiar with patent or legal

terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The Abstract is not intended to be limiting as to the scope of the example embodiments presented herein in any way. It is also to be understood that the procedures recited in the claims need not be performed in the order presented.

Petitioner Exhibit 1002-1030

WHAT IS CLAIMED IS

1. A system for managing contactless transactions, comprising:

at least one memory operable to store commerce data and financial instrument data;

at least one processor coupled to the at least one memory, the one or more processors being operable to:

perform a first tap, the first tap occurring when the system is placed within a predetermined proximity to a payment terminal;

receive from the payment terminal a first select command including an application identifier (AID) corresponding to a first application;

transmit to the payment terminal a first response based on the first select command;

receive from the payment terminal a data request including information indicating supported data types; and

transmit to the payment terminal a second response based on the data request, the second response including transaction data;

wherein the transaction data includes at least a portion of the commerce data stored in the at least one memory.

2. The system of Claim 1, the at least one processor being further operable to:

receive from the payment terminal a payment AID request;

transmit to the payment terminal the AID corresponding to a second application;

receive from the payment terminal a second select command including the AID corresponding to the second application;

transmit to the payment terminal file control information (FCI) corresponding to the second application; and

transmit payment data to the payment terminal;

wherein the payment data includes at least a portion of the financial instrument data stored in the at least one memory.

3. The system of Claim 1 or Claim 2, the at least one processor being further operable to perform a second tap, the second tap occurring when the system is placed within a predetermined proximity to the payment terminal.

4. The system of Claim 1 or Claim 2, the at least one processor being further operable to perform a second tap, the second tap occurring when the system is placed within a predetermined proximity to the payment terminal,

wherein the first tap and the second tap occur in response to a first tap request and a second tap request, respectively, received from the payment terminal.

5. The system of Claim 1, the at least one processor being further operable to:

perform a second tap, the second tap occurring when the system is placed within a predetermined proximity to the payment terminal,

receive from the payment terminal a payment AID request;

transmit to the payment terminal the AID corresponding to a second application;

receive from the payment terminal a second select command including the AID corresponding to the second application;

transmit to the payment terminal file control information (FCI) corresponding to the second application;

transmit payment data to the payment terminal, the payment data including at least a portion of the financial instrument data stored in the at least one memory;

receive from the payment terminal a third select command including an AID corresponding to the first application;

transmit to the payment terminal a third response based on the third select command;

receive from the payment terminal post-transaction data; and

transmit to the payment terminal a fourth response based on the post-transaction data.

6. The system of Claim 1, wherein the payment terminal comprises a contactless reader and/or a point of sale terminal.

Petitioner Exhibit 1002-1032

7. A method for managing contactless transactions, the method comprising steps of:

performing a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal;

receiving from the payment terminal a first select command including an application identifier (AID) corresponding to a first application;

transmitting to the payment terminal a first response based on the first select command;

receiving from the payment terminal a data request including information indicating supported data types; and

transmitting to the payment terminal a second response based on the data request, the second response including transaction data;

wherein the transaction data includes at least a portion of commerce data stored in at least one memory.

8. The method of Claim 7, further comprising steps of:

receiving from the payment terminal a payment AID request;

transmitting to the payment terminal the AID corresponding to a second application;

receiving from the payment terminal a second select command including the AID corresponding to the second application;

transmitting to the payment terminal file control information (FCI) corresponding to the second application; and

transmitting payment data to the payment terminal;

wherein the payment data includes at least a portion of the financial instrument data stored in the at least one memory.

9. The method of Claim 7 or Claim 8, further comprising a step of performing a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal.

10. The method of Claim 7 or Claim 8, further comprising a step of performing a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal,

wherein the first tap and the second tap occur in response to a first tap request and a second tap request, respectively, received from the payment terminal.

11. The method of Claim 7, further comprising steps of:

performing a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal,

receiving from the payment terminal a payment AID request;

transmitting to the payment terminal the AID corresponding to a second application;

receiving from the payment terminal a second select command including the AID corresponding to the second application;

transmitting to the payment terminal file control information (FCI) corresponding to the second application;

transmitting payment data to the payment terminal, the payment data including at least a portion of the financial instrument data stored in the at least one memory;

receiving from the payment terminal a third select command including an AID corresponding to the first application;

transmitting to the payment terminal a third response based on the third select command;

receiving from the payment terminal post-transaction data; and

transmitting to the payment terminal a fourth response based on the post-transaction data.

12. The method of Claim 7, wherein the payment terminal comprises a contactless reader and/or a point of sale terminal.

13. A non-transitory computer-readable medium having stored thereon sequences of instructions for causing one or more processors to:

Petitioner Exhibit 1002-1034

perform a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal;

receive from the payment terminal a first select command including an application identifier (AID) corresponding to a first application;

transmit to the payment terminal a first response based on the first select command;

receive from the payment terminal a data request including information indicating supported data types; and

transmit to the payment terminal a second response based on the data request, the second response including transaction data;

wherein the transaction data includes at least a portion of commerce data stored in at least one memory.

14. The computer-readable medium of Claim 13, having stored thereon sequences of instructions for further causing the one or more processors to:

receive from the payment terminal a payment AID request;

transmit to the payment terminal the AID corresponding to a second application;

receive from the payment terminal a second select command including the AID corresponding to the second application;

transmit to the payment terminal file control information (FCI) corresponding to the second application; and

transmit payment data to the payment terminal;

wherein the payment data includes at least a portion of the financial instrument data stored in the at least one memory.

15. The computer-readable medium of Claim 13 or Claim 14, the one or more processors being further operable to perform a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal.

16. The computer-readable medium of Claim 13, the one or more processors being further operable to perform a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal,

wherein the first tap and the second tap occur in response to a first tap request and a second tap request, respectively, received from the payment terminal.

17. The computer-readable medium of Claim 13, having stored thereon sequences of instructions for further causing the one or more processors to:

perform a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal,

receive from the payment terminal a payment AID request;

transmit to the payment terminal the AID corresponding to a second application;

receive from the payment terminal a second select command including the AID corresponding to the second application;

transmit to the payment terminal file control information (FCI) corresponding to the second application;

transmit payment data to the payment terminal, the payment data including at least a portion of the financial instrument data stored in the at least one memory;

receive from the payment terminal a third select command including an AID corresponding to the first application;

transmit to the payment terminal a third response based on the third select command;

receive from the payment terminal post-transaction data; and

transmit to the payment terminal a fourth response based on the post-transaction data.

18. The computer-readable medium of Claim 13, wherein the payment terminal comprises a contactless reader and/or a point of sale terminal.

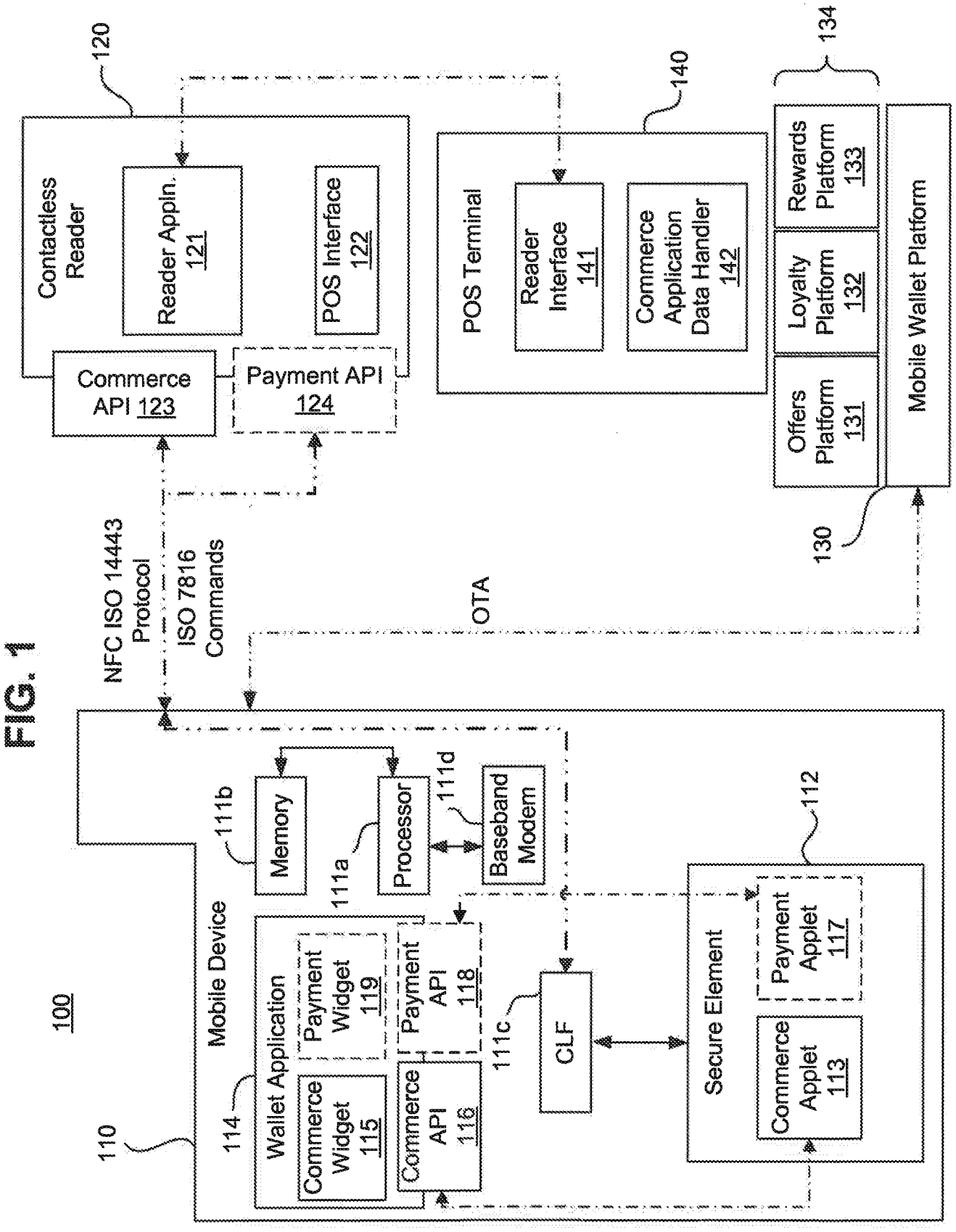

100
110
Mobile Device
Wallet Application
114
Commerce Widget 115
Payment Widget 119
Commerce API 116
Payment API 118
111a
Processor
111b
Memory
111c
CLF
111d
Baseband Modem
112
Secure Element
Commerce Applet 113
Payment Applet 117
NFC ISO 14443 Protocol
ISO 7816 Commands
OTA
120
Contactless Reader
Reader Appln. 121
POS Interface 122
Commerce API 123
Payment API 124
140
POS Terminal
Reader Interface 141
Commerce Application Data Handler 142
134
Rewards Platform 133
Loyalty Platform 132
Offers Platform 131
130
Mobile Wallet Platform

FIG. 1

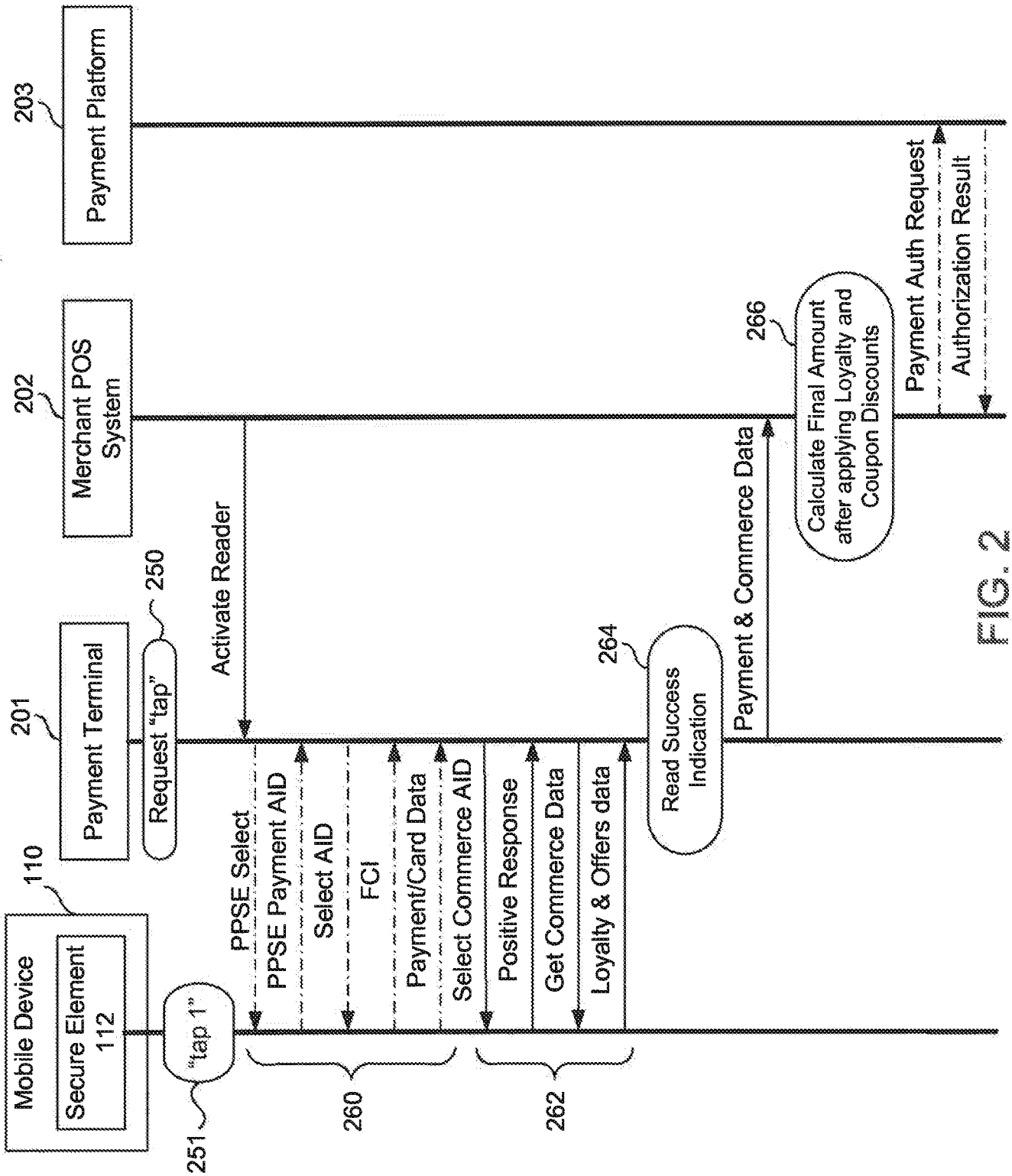

200
Mobile Device
110
Secure Element
112
Payment Terminal
201
Merchant POS System
202
Payment Platform
203
"tap 1"
251
Request "tap"
250
Activate Reader
PPSE Select
PPSE Payment AID
Select AID
FCI
Payment/Card Data
Select Commerce AID
Positive Response
Get Commerce Data
Loyalty & Offers data
260
262
Read Success Indication
264
Payment & Commerce Data
Calculate Final Amount after applying Loyalty and Coupon Discounts
266
Payment Auth Request
Authorization Result

FIG. 2

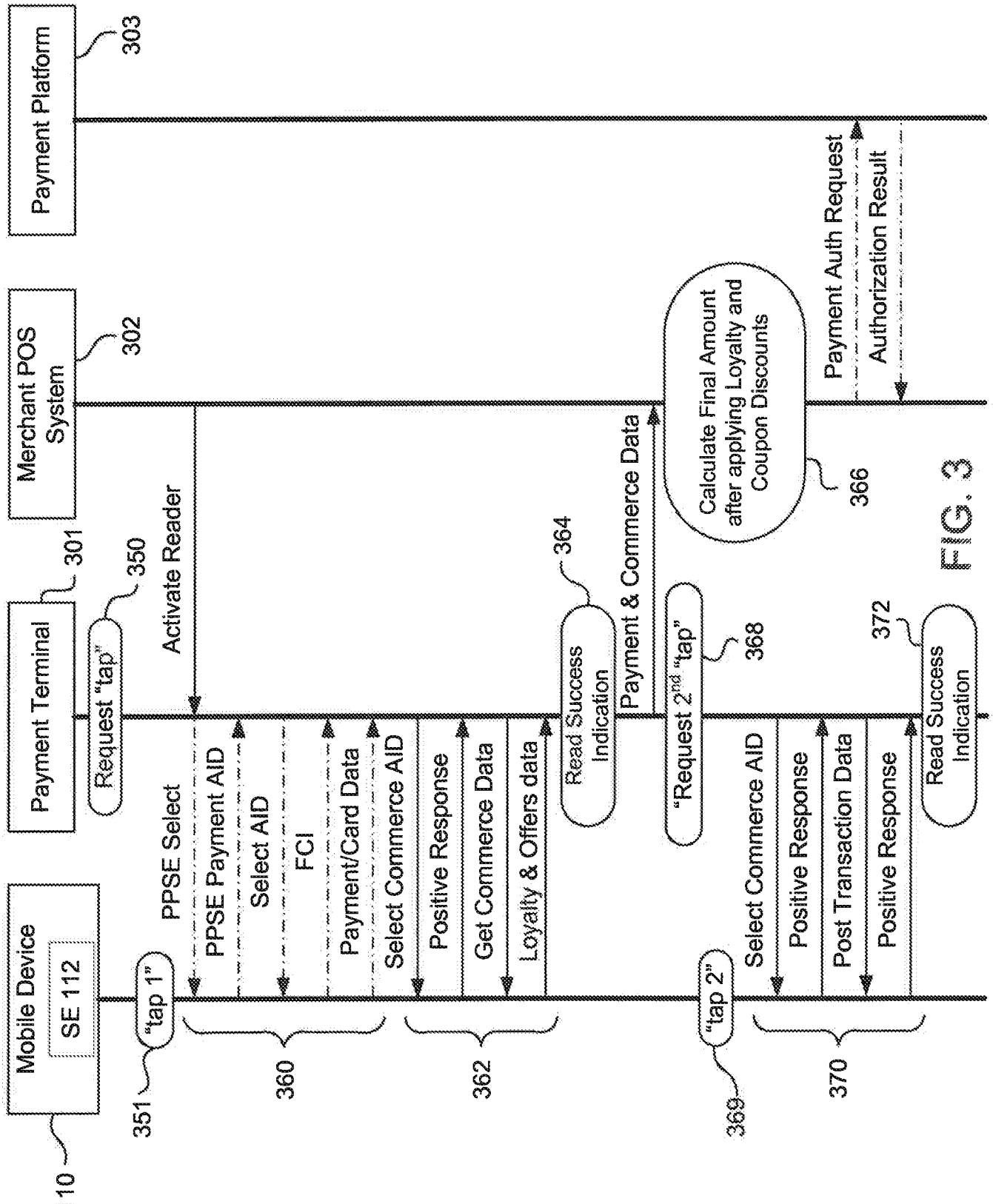

300
Mobile Device
SE 112
110
Payment Terminal
301
Merchant POS System
302
Payment Platform
303
"tap 1"
351
Request "tap"
350
Activate Reader
PPSE Select
PPSE Payment AID
Select AID
FCI
Payment/Card Data
360
Select Commerce AID
Positive Response
Get Commerce Data
Loyalty & Offers data
362
Read Success Indication
364
Payment & Commerce Data
Calculate Final Amount after applying Loyalty and Coupon Discounts
366
Payment Auth Request
Authorization Result
"Request 2nd "tap"
368
"tap 2"
369
Select Commerce AID
Positive Response
Post Transaction Data
Positive Response
370
Read Success Indication
372

FIG. 3

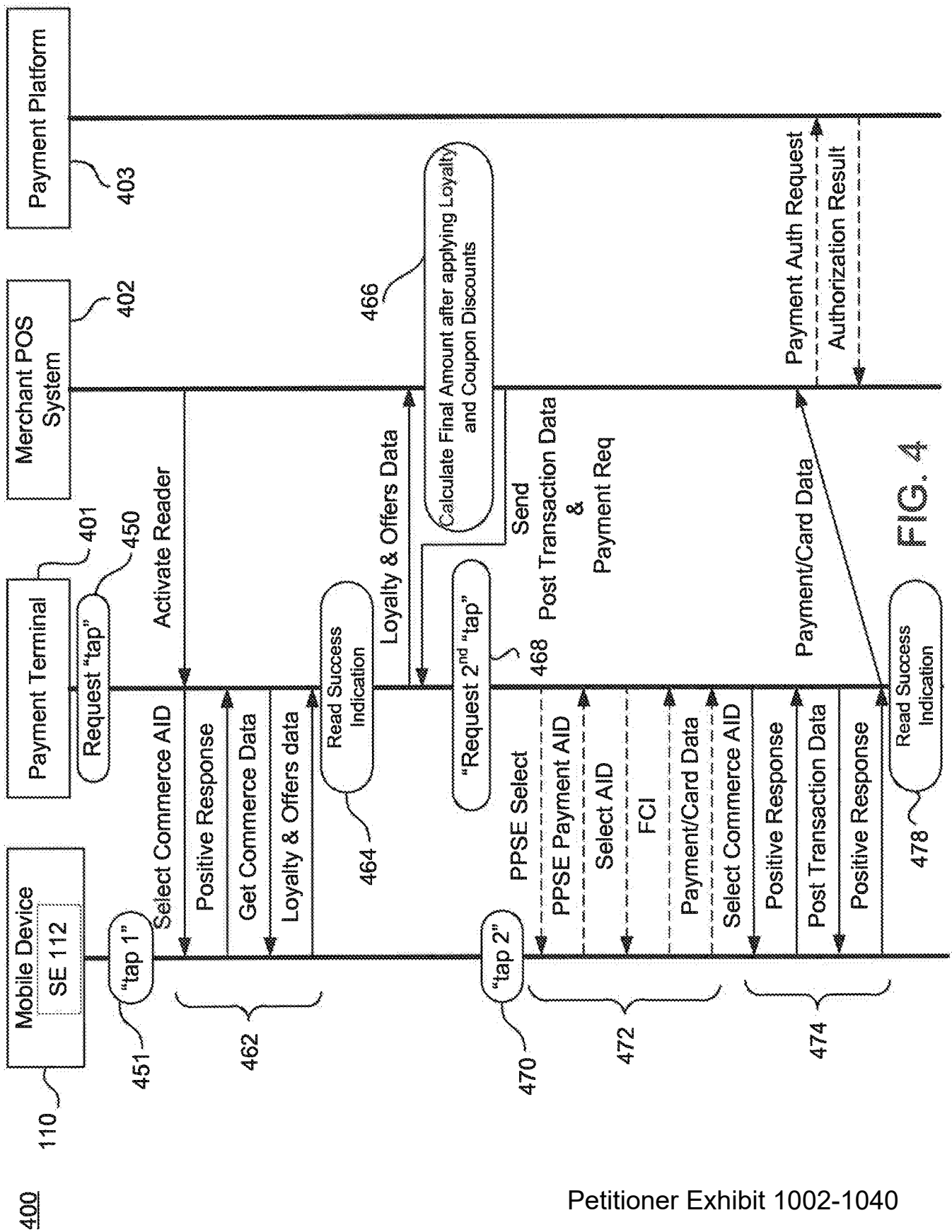

400
Mobile Device
SE 112
110
Payment Terminal
401
Merchant POS System
402
Payment Platform
403
"tap 1"
451
Request "tap"
450
Activate Reader
Select Commerce AID
Positive Response
Get Commerce Data
Loyalty & Offers data
462
Read Success Indication
464
Loyalty & Offers Data
Calculate Final Amount after applying Loyalty and Coupon Discounts
466
"Request 2nd "tap"
468
Send Post Transaction Data & Payment Req
"tap 2"
470
PPSE Select
PPSE Payment AID
Select AID
FCI
Payment/Card Data
472
Payment/Card Data
Payment Auth Request
Authorization Result
Select Commerce AID
Positive Response
Post Transaction Data
Positive Response
474
Read Success Indication
478

FIG. 4

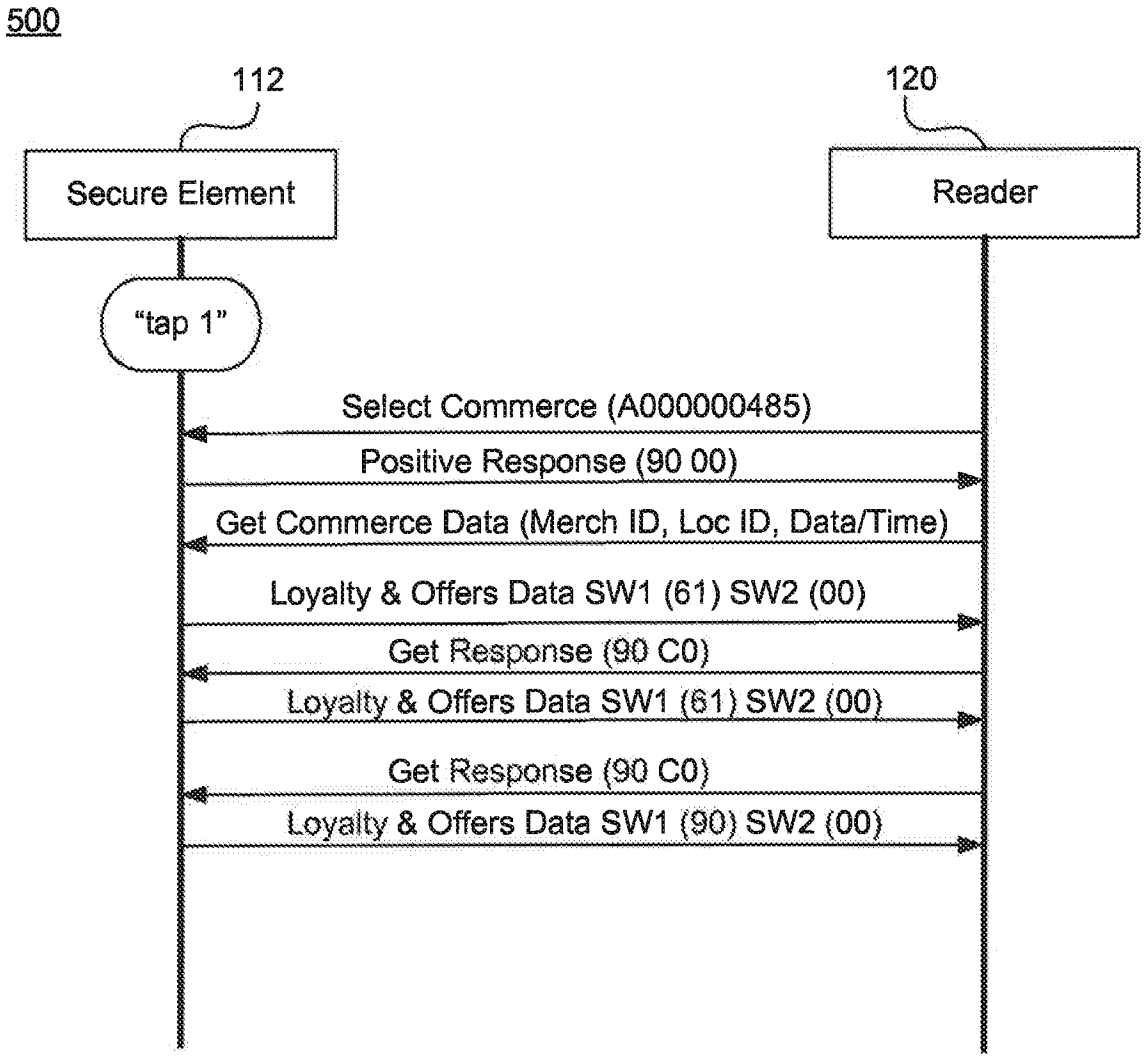

500
112
120
Secure Element
Reader
"tap 1"
Select Commerce (A000000485)
Positive Response (90 00)
Get Commerce Data (Merch ID, Loc ID, Data/Time)
Loyalty & Offers Data SW1 (61) SW2 (00)
Get Response (90 C0)
Loyalty & Offers Data SW1 (61) SW2 (00)
Get Response (90 C0)
Loyalty & Offers Data SW1 (90) SW2 (00)

FIG. 5

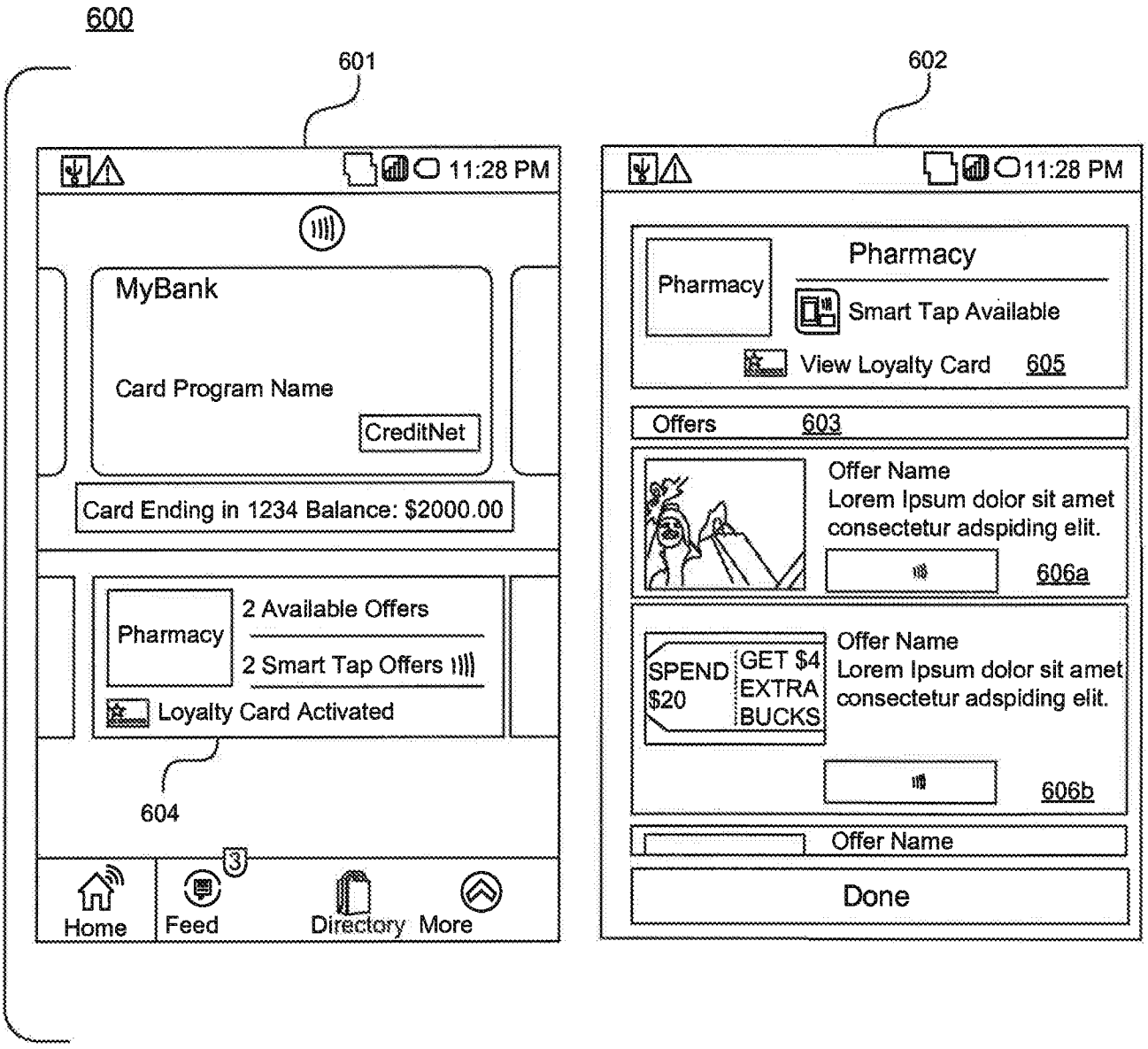

600
601
602
11:28 PM
MyBank
Card Program Name
CreditNet
Card Ending in 1234 Balance: $2000.00
Pharmacy
2 Available Offers
2 Smart Tap Offers
Loyalty Card Activated
604
Home
Feed
Directory
More
11:28 PM
Pharmacy
Pharmacy
Smart Tap Available
View Loyalty Card 605
Offers 603
Offer Name
Lorem Ipsum dolor sit amet consectetur adspiding elit.
606a
SPEND $20
GET $4 EXTRA BUCKS
Offer Name
Lorem Ipsum dolor sit amet consectetur adspiding elit.
606b
Offer Name
Done

FIG. 6

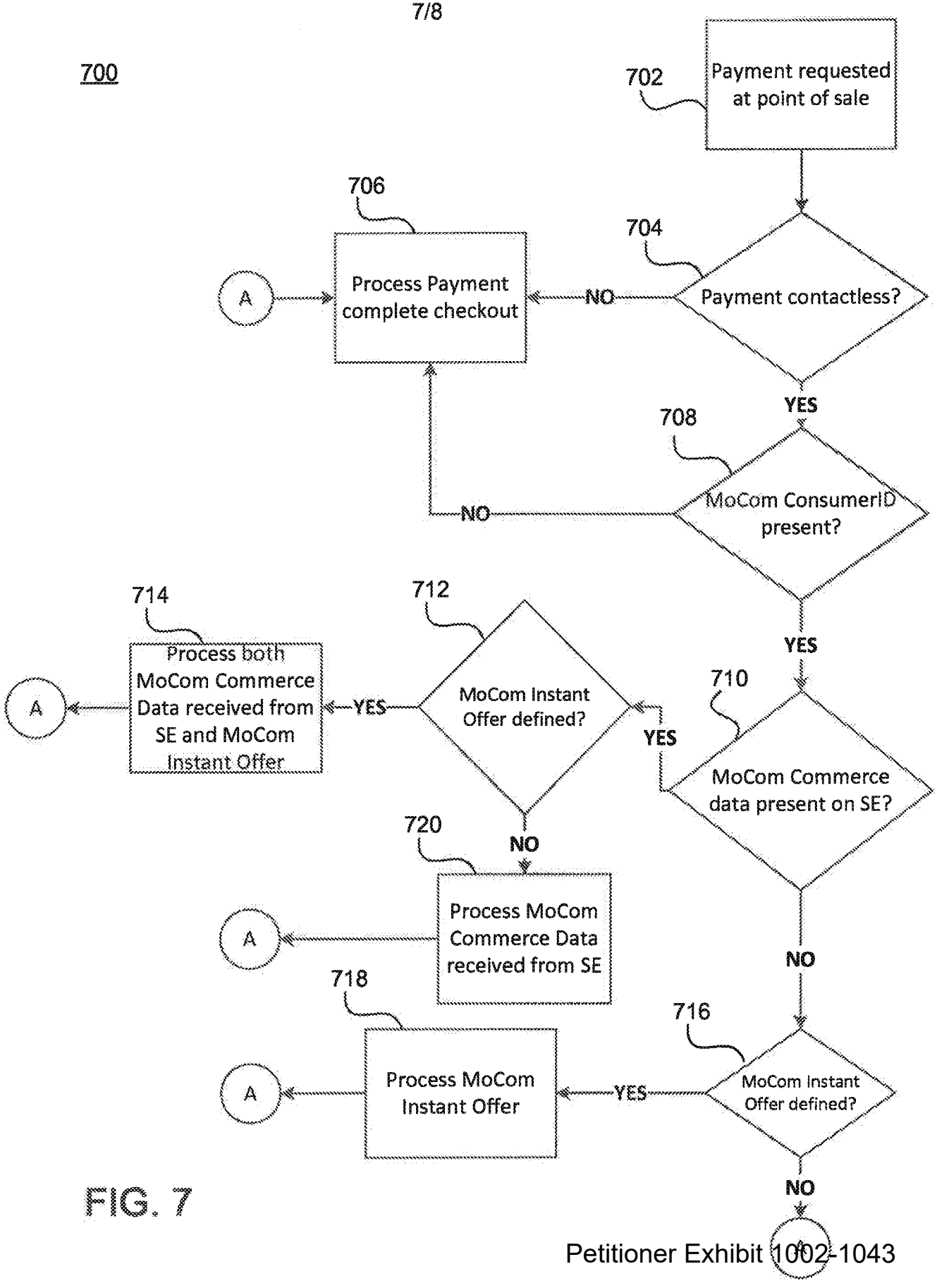

700
702
Payment requested at point of sale
704
Payment contactless?
NO
706
Process Payment complete checkout
A
YES
708
MoCom ConsumerID present?
NO
YES
710
MoCom Commerce data present on SE?
YES
712
MoCom Instant Offer defined?
YES
714
Process both MoCom Commerce Data received from SE and MoCom Instant Offer
A
NO
720
Process MoCom Commerce Data received from SE
A
NO
716
MoCom Instant Offer defined?
YES
718
Process MoCom Instant Offer
A
NO
A

FIG. 7

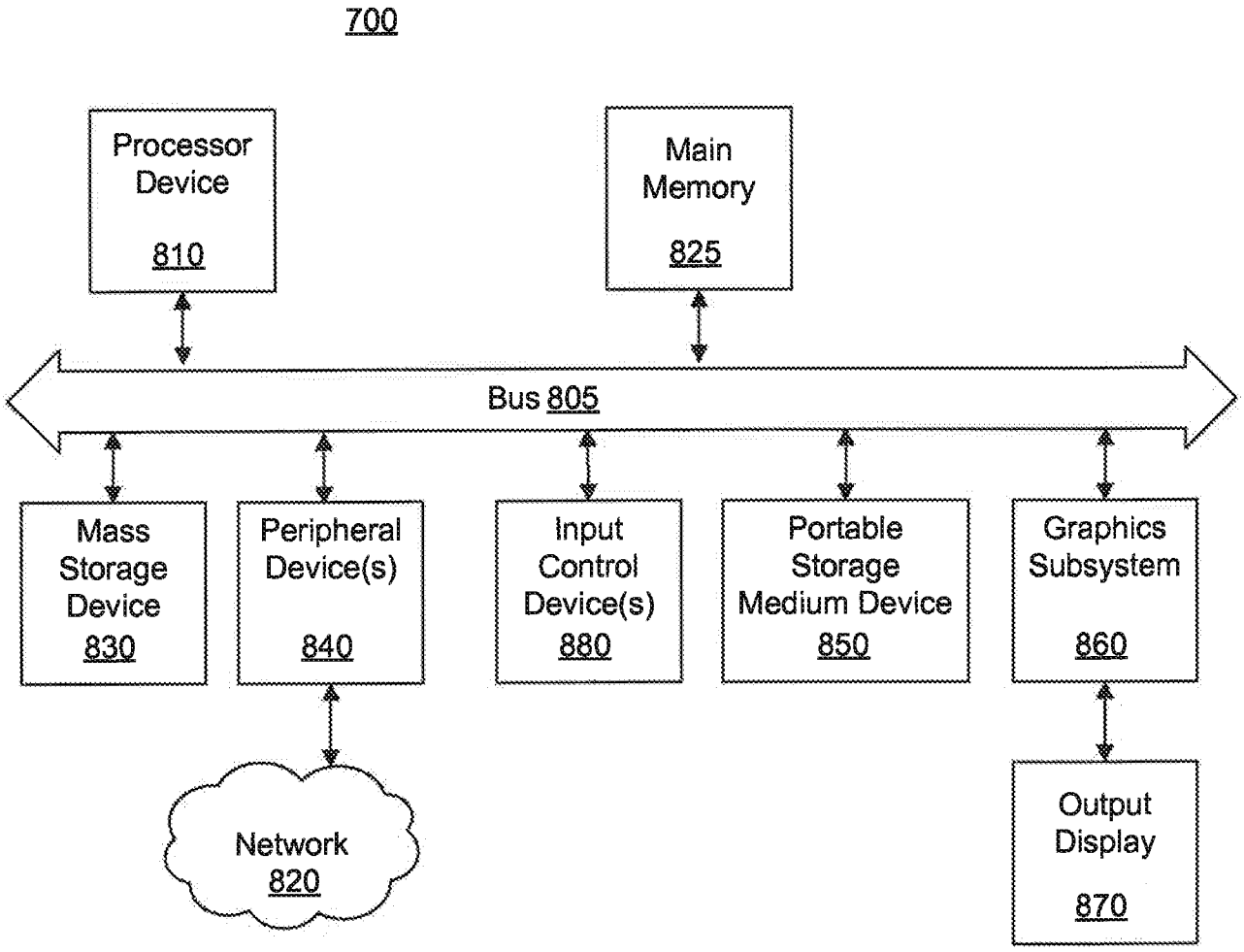

700
Processor Device 810
Main Memory 825
Bus 805
Mass Storage Device 830
Peripheral Device(s) 840
Input Control Device(s) 880
Portable Storage Medium Device 850
Graphics Subsystem 860
Network 820
Output Display 870

FIG. 8

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 June 2014 (19.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/093857 A1

(51) International Patent Classification:
G06Q 20/20 (2012.01)

(21) International Application Number:
PCT/US2013/075077

(22) International Filing Date:
13 December 2013 (13.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/737,409 14 December 2012 (14.12.2012) US

(71) Applicant: **MEI INC.** [US/US]; 3222 Phoenixville Pike, Suite 200, Malvern, PA 19355 (US).

(72) Inventors: **ANDERSON, Thomas**; 422 Brandham Way, Downingtown, PA 19335 (US). **TEDDER, Bradford, Reams**; 2528 Drew Valley Rd, Atlanta, GA 30319 (US). **HADDON, Douglas, Brian**; 3000 Georgetown Road, Cinnaminson, NJ 08077 (US).

(74) Agents: **MIRABITO, Jason, A.** et al.; Mintz Levin Cohn Ferris Glovsky And Popeo, PC., One Financial Center, Boston, MA 02111 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) Title: POINT OF SALE PLATFORM FOR CONSUMER MEDIA INTERACTION

(57) Abstract: A point of sale system includes a host, an intermediate controller, a user interface device, and one or more peripheral devices. The intermediate controller includes an operating environment and is in communication with the host. The user interface device is associated with and in communication with the intermediate controller. The user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more applications for interaction with a customer. The one or more peripheral devices are coupled to at least the intermediate controller via a bus. Related apparatus, systems, techniques, and articles are also described.

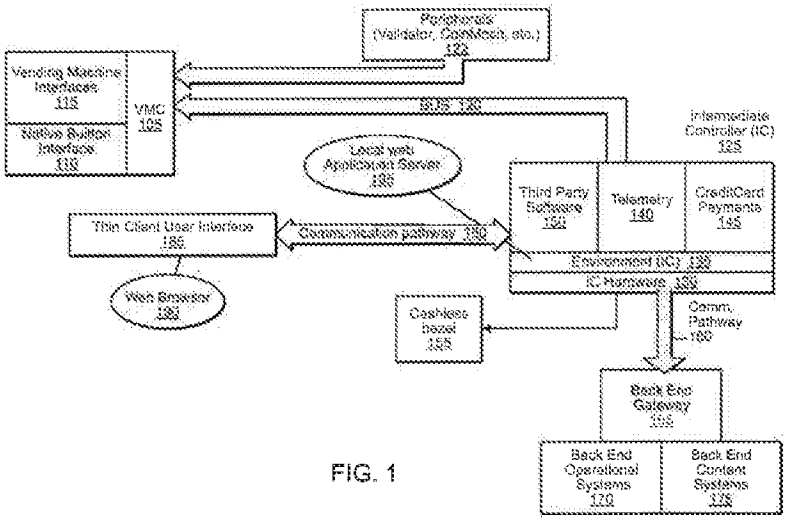


FIG. 1

WO 2014/093857 A1

Petitioner Exhibit 1002-1045

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

Petitioner Exhibit 1002-1046

Point of Sale Platform for Consumer Media Interaction

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 61/737409 filed December 14, 2012, the entire contents of which are hereby incorporated by reference herein.

TECHNICAL FIELD

[0002] The subject matter described herein relates, in general, to electronic transaction systems and, in particular, to a dynamic consumer-interactive vending platform.

BACKGROUND

[0003] Electronic transaction systems, such as vending machines, typically utilize Digital Exchange (DEX) and Multi-Drop Bus (MDB) protocols. A DEX file is an electronic audit file having information such as sales, cash in bill validators, pricing, etc. A vending machine controller (VMC) generally stores the information on a timely basis and transmits it in DEX format as a DEX file as and when requested. MDB can provide an interface between the vending machine and different peripheral devices, such as coin acceptors, bill acceptors, credit-card acceptors, etc. Additionally, the VMC can recognize and enable the peripheral devices for operation, after which the device and the VMC can communicate. The communication enables components of the system to work in concert to perform the functions of the vending machine, such as accepting payment, vending product, logging transactions, and transmitting transactional information to an external server.

[0004] However, conventional vending machines pre-configure to work with a specific set of peripheral devices and require replacement to support additional devices. Thus,

Petitioner Exhibit 1002-1047

the VMC is an integrated component that supports a specific set of functionalities and may require cost consuming replacements or extensions to offer additional functionalities. As an example, conventional VMC's only enable the following operations: receive a vending request; accept cash or credit to process the request; and process the vending request after receiving the intended amount. Furthermore, consumer interaction is limited to a static set of interface components, typically buttons. Prior attempts to expand vending machine functionality focuses on configuration changes with the VMC, thereby suggesting and requiring replacement of the VMC. However, replacing the VMC can be cost-prohibitive and undesirable.

SUMMARY

[0005] In one aspect, a point of sale system includes a host, an intermediate controller, a user interface device, and one or more peripheral devices. The intermediate controller includes an operating environment and is in communication with the host. The user interface device is associated with and in communication with the intermediate controller. The one or more peripheral devices are coupled to at least the intermediate controller via a bus.

[0006] The intermediate controller can be an embedded personal computer control board. The intermediate controller operating environment can include an operating system and file system. The intermediate controller can receive data from a remote server. The user interface device and intermediate controller can be coupled via an Ethernet communication connection.

[0007] The intermediate controller can further include a telemetry module to configure alarms and notifications for instances such as door open, jammed item, temperature control, etc. The intermediate controller can further include one or more application modules, for example third party software applications. Further, at least one application module can be

Petitioner Exhibit 1002-1048

accessed by the user interface device. The application modules can support additional and enhanced functionalities. For example, the intermediate controller can include an application module, e.g. a web server module, to run a web browser on the user interface device. The user interface device thus hosts one or more applications for interaction with a customer. Furthermore, in one implementation, the web server module can be associated with a remoter server via a network (not shown). In this configuration, the web server module requests information pertaining to the customer, such as customer profiles, loyalty information, rewards, coupons, discounts, etc., and displays the information on the user interface device. The user can make further selections on the user interface module through the web browser, thus allowing the user to dynamically interact with the point of sale system. The web server can be HTTP compliant and the web server can be an HTTP application server.

[0008] In another example, the application module can include a multiple vend selection module, which supports the selections and vending of multiple items in a single transaction. In yet another example, the application module is a monitoring module configured to monitor and record details of the point of sale systems that request a specific application module. The application modules can also be associated with license numbers making it easier to track the updates and installations.

[0009] In one implementation, the application module can be a diet information module configured to store nutritional information for each of the vend items. Additionally or optionally, the diet information module may have access to the inventory and specific information on items. Further, the diet information module stores the selections made by the customer in each transaction with the nutritional information. The diet information module can provide suggestions and recommendations based on the customer purchasing history.

[0010] The point of sale system can further include a cashless bezel coupled to the intermediate controller. The intermediate controller can further include a cashless module for

Petitioner Exhibit 1002-1049

enabling cashless transactions. The bus, communicatively coupled with the intermediate controller and the host, can be a multi-drop data bus (MDB). Additionally, the peripheral devices can be communicatively coupled, directly or indirectly, to the host and the intermediate controller via the bus. The host can be a vending machine controller (VMC). The VMC can include a vending machine interface and one or more native button interfaces. Conventionally, the VMC is designed to be the master controller that controls all the peripheral devices through the bus. However, in one embodiment, the intermediate controller is assigned the peer role by controlling the application modules and/or peripheral devices and translating instructions into a language understood by the VMC. In another embodiment, the intermediate controller controls one or more peripheral devices through the bus, except the peripheral devices that are hardwired to the VMC. In this manner, the "master" role switches between the intermediate controller and the VMC based on the functionality.

[0011] In another aspect, a point of sale system includes a host, an intermediate controller, a user interface and one or more peripheral devices. The intermediate controller is in communication with the host and includes one or more third party applications utilizing an application interface to control components of the point of sale system according to predefined functions. The user interface device is associated with and in communication with the intermediate controller. The one or more peripheral devices are coupled to at least the intermediate controller via a bus.

[0012] In another aspect, a point of sale system includes an intermediate controller including an operating environment, a user interface device and one or more peripheral devices coupled to at least the intermediate controller via a bus. The user interface is associated with and in communication with the intermediate controller. The user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more applications for interaction with a customer.

Petitioner Exhibit 1002-1050

[0013] One or more of the following features can be included. For example, the components of the point of sale system can include one or more of mechanical, electrical, or software components. The components of the point of sale system can include one or more of the peripheral devices coupled to the intermediate controller. The components of the point of sale system can include the host. The components of the point of sale system can include the user interface device. A telemetry unit can be included and can be in communication with a remote licensing server. The user interface can include a web browser and the intermediate controller can include a webserver, the webserver hosting one or more of the third party applications for interaction with a customer. The one or more third party applications can have been installed on the point of sale system using a remote back end server to select the one or more third party applications for installation. The point of sale system can be in communication with a host remote from the point of sale system.

[0014] Computer program products are also described that comprise non-transitory computer readable media storing instructions, which when executed by at least one data processors of one or more computing systems, causes at least one data processor to perform operations herein. Similarly, computer systems are also described that may include one or more data processors and a memory coupled to the one or more data processors. The memory may temporarily or permanently store instructions that cause at least one processor to perform one or more of the operations described herein. In addition, methods can be implemented by one or more data processors either within a single computing system or distributed among two or more computing systems.

[0015] The subject matter described herein provides many advantages. For example, a customer's purchasing history can be tracked and they can be rewarded according to pre-defined rules. Using the current subject matter, a customer can dynamically interact with the point of sale machine creating a unique and individualized consumer experience.

Petitioner Exhibit 1002-1051

The subject matter described herein can be implemented in existing point of sale machines in a cost-effective manner with minimal software and hardware modifications. In other words, the current subject matter enables an inexpensive retrofit of existing vending machines that does not require replacement of the VMC. Further, the current subject matter can integrate into existing machines and the capabilities are modular and can be expanded based upon need. This allows retrofit integration across many different and often disparate technologies, which many prior integrated solutions do not provide.

[0016] The current subject matter enables a point-of-sale machine to support advanced media functionality, for example social media interactivity, targeted advertisement, and personalized point-of-sale machine experience.

[0017] The details of one or more variations of the subject matter described herein are set forth in the accompanying drawings and the description below. Other features and advantages of the subject matter described herein will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

[0018] FIG. 1 is a system block diagram illustrating components of an example embodiment of a point of sale machine, including an intermediate controller;

[0019] FIG. 2 is a system block diagram illustrating components of another example embodiment of a point of sale machine, including intermediate controller;

[0020] FIG. 3 is a block diagram illustrating the layers of an example operating system in an exemplary intermediate controller environment;

[0021] FIG. 4 is a block diagram illustrating the application module controlling loyalty information of customers, according to an embodiment of the present subject matter; and

Petitioner Exhibit 1002-1052

[0022] FIG.5 is a block diagram illustrating the sharing of the bus between the intermediate controller and the VMC according to an embodiment of the present subject matter.

[0023] Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0024] The current subject matter described herein supports additional functionalities to a point of sale system. In one implementation, the additional functionalities can be provided as a retrofit solution with little or no hardware modifications. Examples of point of sale systems include, but are not limited to, a vending machine, gaming machines, automated teller machines, banking machines, kiosks, bill pay machines, or any other host machine configured to accept payment in exchange for products and/or services. Such systems can dynamically interact with a variety of peripheral devices and provide additional functionalities. Additional functionalities include providing advertising, loyalty rewards, discounts, coupons, multiple vend items, social media interaction, mobile device or mobile wallet interaction, etc. Further, the point of sale machine can support dynamic engagement through a user interface, for example a touch screen. Existing point of service machines can be retrofit with the current subject matter, which will reduce cost associated with replacing an entire system. In addition, the device is configured to dynamically track and control software licenses and updates by interacting with a back end server or remote server or enterprise controller.

[0025] FIG. 1 is a block diagram illustrating components of an example embodiment of a point of sale system 100. In this embodiment, a VMC 105 is coupled to native button user interfaces 110 and other vending machine interfaces 115. The VMC 105 can connect via a bus 120 to a number of optional peripherals 125. The bus 120 can include an MDB bus or other suitable communications pathway such as Executive, BDV,

Petitioner Exhibit 1002-1053

micromech, cctalk, and Electromechanical. The optional peripherals 125 are peripherals that enable vending machine functionality. For example, a bill validator and coin validator are optional peripherals 122. Example bill validators and coin validators can include those described in, e.g., U.S. Patent No. 6,390,269, the content of which is expressly incorporated by reference, in its entirety.

[0026] The VMC 105 also connects via bus 120 to an intermediate controller (IC) 125. The IC 125 is an embedded computing platform with unique hardware architecture and software framework that provides for flexible, expandable, and dynamic point of sale functionality. In one embodiment, the IC 125 is an embedded PC control board that provides multi-purpose hardware architecture, operating system, run time environments, with expandable hardware and software capability, and further includes industry standard interfaces. The IC 125 is connected via a communications pathway 180 to a thin client user interface 185. In one embodiment, the communications pathway 180 can be hardwired, such as an Ethernet, serial, USB, or similar connection. The thin client user interface 185 can be a standalone computing device that includes at least a graphical display that presents to a customer. The thin client interface 185 can include a display system that can function as a medium of consumer input (e.g., the display system can be an LCD touch screen). In general, the thin client user interface 185 provides access to applications running on the IC 125. In one embodiment, the thin client user interface 185 includes a web browser 190 that operates as a client in a client-server relationship with a web server 195 running on the IC environment 135 of the IC 125. Communication can occur between the thin client user interface 185 and the IC 125 through TCP/UDP protocol. In this embodiment, web server 195 is capable of serving graphics, media, video, audio and any other MIME type (i.e. standard content format under HTML standards) to the thin client user interface 185.

Petitioner Exhibit 1002-1054

[0027] The IC 125 includes IC hardware 130 (e.g., an embedded PC control board) supporting an IC environment 135 (e.g., an operating system, file system, runtime environments, and other associated software applications). Optionally, the IC 125 can be powered via the bus 120. The IC 125 can also include a telemetry 140 module, a credit card payment 145 module, and third party software 150. The telemetry 140 module allows the point of sale machine to communicate with a back end or remote server, such as gateway 165. The telemetry 140 module provides for exchange of transactional and/or operational information (e.g., logging/audit, inventory information, etc.) between the point of sale machine and any backend services as well as deployment of software upgrades and additions to the point of sale machine. The telemetry 140 module can include dedicated communications hardware and associated software (e.g., for cellular, WiMax, WAN, LAN, etc.).

[0028] The credit card payment 145 module provides support for and controls a cashless bezel 155. The cashless bezel 155 is linked to the IC 125 and accepts credit card information through, e.g., magnetic swipe, contactless, chip card, IC Card, smartcard, EMV, and RFID tag interfaces. From the perspective of the VMC 105, the cashless bezel 155 is a cascaded peripheral that is controlled by the IC 125, but ultimately transactions that include the cashless bezel 155 will result in the IC 125 sending a credit message to the VMC to enable the transaction. The cashless bezel 155 can include those described in, e.g., U.S. Patent No. 8,157,167, the contents of which is herein expressly incorporated by reference, in its entirety.

[0029] The IC 125 is connected via a communications pathway 160 (e.g., a wireless APN utilizing cellular technology or other suitable mode of communications) to a backend gateway 165. The backend gateway 165 includes backend operational systems 170 and backend content systems 175. In addition to supporting credit transaction, the back end

Petitioner Exhibit 1002-1055

gateway 165 can provide access for third parties to communicate with the point of sale machine (possibly to the third party software they have installed). In one example use, a customer can swipe a rewards or loyalty card and the IC 125 can communicate with a third party server to determine and/or receive information regarding the customer's loyalty account including any discounts, credits, or free purchases that the customer may be entitled to.

[0030] Additionally, the IC 125 may be allowed access to customer preferences and profiles stored on the third party server. The IC 125 then enables the thin client user interface 185 to support advanced media functionality, for example social media interactivity, targeted advertisement, personalization of a customer transaction experience, and e-commerce like customer experiences. In some embodiments, the thin client user interface 185 can be configured to display still images, stored video files, dynamic content and interactive content to a user. The current subject matter provides a rich consumer media and social networking experience. Further, the user may utilize multiple payment methods to make a purchase at the point of sale machine.

[0031] The IC 125, upon validating a coupon, rewards club benefit, or other discount, can send a message to the VMC 105 to add a credit for the benefit amount. Thus, from the VMC's 105 perspective, the IC 125 is another peripheral 122 such as a coin mechanism that is accepting payment from the customer and providing a credit notice to the VMC 105. Since the IC 125 can host third party software 150, the third party software 150 can instruct the IC 125 to send a credit message to the VMC 105 for a broad range of reasons, as desired by the third party software.

[0032] In one embodiment, the VMC 105 is designated as the master controller, which controls peripheral devices including optional peripherals 122 and IC 125 through the bus 120. However, in another embodiment as shown in FIG. 2, the optional peripherals 122 cascade from the IC 125. In this configuration, the IC 125 intercepts normal communication

Petitioner Exhibit 1002-1056

between the VMC 105 and optional peripherals 122 and acts as a master controller and instructs or tricks the VMC 105 with respect to newly defined functionalities; with the exception of vend requests. The IC 125 can "trick" the VMC into performing desired operations that the VMC is not designed to handle. For example, a customer could input a rewards club loyalty identification, coin, and bill value and the IC 125 could, in order to provide a discount, send the VMC 105 a message indicating a total credit input by the customer, even though the customer has not input sufficient funds (but in fact is receiving a discount). In this configuration, the VMC 105 continues to handle vend requests.

[0033] In another embodiment, with reference again to FIG. 1, the intermediate controller 125 acts as a peer to the VMC 105 rather than a master and peripheral configuration. In this embodiment, the IC 125 can query the VMC 105 and transmit a message that there is credit. In this case, the IC 125 translates the additional functionalities into vend requests, which can then be interpreted by the VMC 105 as legitimate requests with credit.

[0034] In another embodiment, the IC 125 and VMC 105 may work in a "shared environment," that is, sharing functionalities. The VMC 105 can be configured to support at least a portion of newly defined functionalities. Thus, the "master" role is dynamic and switches between IC 125 and the VMC 105 based on a given functionality.

[0035] Functionalities supported include, but are not limited to: Multi Vend Selection (e.g. selection of multiple products or services within a single transaction), Discounts, Coupons, Advertisements, Recommendations/Suggestions based on customer profiling, Tracking and controlling software updates/licenses, other customer engagement. Examples of vending protocols include: Executive, MDB, BDV, Electromechanical.

[0036] Additionally or optionally, the gateway 165 may be associated with a monitoring module (not shown) within the IC 125. The gateway 165 interacts with a

Petitioner Exhibit 1002-1057

monitoring server designed to control the licenses downloaded on the point of sale machines coupled to the gateway 165. Such information is passed onto the monitoring module via the gateway 165. Thus, the monitoring module tracks software updates on the point of sale machines. This, in turn, helps in better management and handling of application modules stored on the point of sale machines.

[0037] The IC 125 provides for flexible expansion. For example, in one embodiment, a basic embedded computing platform can expand by adding to or improving the computing device (e.g., memory, hard drive, CPU, connectors, power supply, other third party removable component), onboard machine interfaces (e.g., USB 2.0, USB 3.0, MDB, EXEC, VCCS, Serial), expansion card (e.g., WAN Modem, CDMA, Ethernet, Bluetooth, Wifi, Memory Card, SD Card, Graphics Card, Secure Storage Card, Audio Card), software infrastructure (e.g., advanced data collection, distributed computing interfaces, VDI or other Data Exchange, VPN, DNS Utilization, Web/Application Server, Python, etc.), and any software application (e.g. a third party application).

[0038] Application Programming Interfaces (API) remove the need for point-of-sale machine specific designs thereby supporting and promoting development and use of third party applications that improve or control point-of-sale machine functionality. A standard interface (to mechanical, electrical, or software components of the point-of-sale machine) allows a third party (as distinguished from the original equipment manufacturer (OEM)) to create a third party application to utilize the point-of-sale machine (and, e.g., components thereof, including the IC 125, host, thin client user interface 185, and peripherals 122) according to pre-defined functions. For example, a web service interface that implements a device to server VDI standard can allow a third party to leverage the web service in developing a third party application.

Petitioner Exhibit 1002-1058

[0039] For a given point-of-sale machine, a machine manager can access a defined set of available services and interfaces. This allows third party components (e.g., mechanical, electrical, and/or software) to operate within the boundaries of that point-of-sale machine. The effect is a flexible point-of-sale machine that a manager can tailor to a specific use (e.g., for selling a specific product, selling a product in a specific region or country, etc.). For example, a third party application can deploy on the IC 125 and operate alongside the telemetry 140 module to provide enhanced capabilities for tracking consumer purchasing behavior or enhanced advertisement capability.

[0040] Third party software distribution can be managed by a library of existing and available third party or OEM software components. A point-of-sale machine manager can view the application through, for example, a web application on the back end, and select the software that the manager would like installed on the point-of-sale machine. The point-of-sale machine can download an upgrade package from a backend server and install or update the software. Licensing and version control can be applied on a point-of-sale machine level, and point-of-sale managers are able to customize their machines.

[0041] Using the current subject matter, a customer can, for example, present a form of identification (e.g., credit card or loyalty club rewards card) to the point of sale machine. The point of sale machine can then remotely access a backend or remote server that includes information specific to that customer and download preferences, targeted advertisements, account information (e.g. point balances), and other individualized information and present the information to the customer via a display device. The information can be dynamic and does not need to be stored locally at the point of sale machine. The customer can interact with the dynamic information in order to complete a transaction. Such functionality of the point of service machine can be controlled, upgraded, changed, etc.

Petitioner Exhibit 1002-1059

through use of applications (third party or OEM). The functionality can be modified remotely, without having to install new hardware or have a technician service the machine.

[0042] FIG. 3 is a block diagram illustrating the layers of an example operating system in an IC environment 135.

[0043] A point of service machine that includes an intermediate device 125 and thin user client 185 can present advertisements or other media. For example, the machine can be in an idle state and display one set of advertisements (e.g., static images or video). When a customer initiates a transaction, the machine can accept or determine identification of the customer. The IC 125 can then download targeted advertisement or other information for display by the thin client user interface 185.

[0044] The current subject matter can enable a point of sale machine, more specifically, a vending machine, to perform multiple vend operations using a single payment through say the multi product vend module (not shown). As an example, a customer can swipe a credit card. The IC 125 can validate the credit card for a predetermined amount (e.g., enough for three vends of product). The IC 125 can send three separate credit messages to the VMC 105 to enable a multi-vend procedure. For example, a customer swipes a credit card, authorization is performed, the VMC 105 is informed by the IC 125 that credit sufficient for a single product vend has been input, the customer selects the product using the native button interface 110, the VMC is again informed by the IC 125 that credit sufficient for a single product vend has been input (without additional customer input), and the customer can select the desired product using the native button interface 110. This process can be repeated for any number of vends (i.e., a multi-vend). Further, the MDB driver, shown in IC 125, allows the application modules to interact with the bus 120. In essence, the MDB driver acts as a translator between the application modules and the bus 120, ensuring that the protocol is followed. The IC 125 may also include a modem (not shown) to display content on external

Petitioner Exhibit 1002-1060

devices such as cellular phones via cellular network or any other network know in the art. Thus, in one implementation, a user may receive nutritional information or balance information on his cell phone.

[0045] FIG. 4 is a block diagram illustrating the application module controlling loyalty information of customers, according to an embodiment of the present subject matter. Loyalty information can be stored on a loyalty system in the back-end system. A S1 Gateway can interface with the loyalty system and provide consumer loyalty information to the controller. The controller can act as a bridge between the Bezel and the Gateway and can control a transaction.

[0046] FIG.5 is a block diagram illustrating the sharing of the bus between the intermediate controller and the VMC according to an embodiment of the present subject matter. The intermediate controller (or A5K) can provide credit amount from cash and the credit available to the thin client interface. When a consumer is ready to check out, the intermediate controller can cause a vend to occur without having further consumer interaction.

[0047] Various implementations of the subject matter described herein may be realized in digital electronic circuitry, integrated circuitry, specially designed ASICs (application specific integrated circuits), computer hardware, firmware, software, and/or combinations thereof. These various implementations may include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

[0048] These computer programs (also known as programs, software, software applications or code) include machine instructions for a programmable processor, and may be

Petitioner Exhibit 1002-1061

implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the term "machine-readable medium" refers to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory, Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor, including a machine-readable medium that receives machine instructions as a machine-readable signal. The term "machine-readable signal" refers to any signal used to provide machine instructions and/or data to a programmable processor.

[0049] To provide for interaction with a user, the subject matter described herein may be implemented on a computer having a display device (e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor) for displaying information to the user and a keyboard and a pointing device (e.g., a mouse or a trackball) by which the user may provide input to the computer. Other kinds of devices may be used to provide for interaction with a user as well; for example, feedback provided to the user may be any form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback); and input from the user may be received in any form, including acoustic, speech, or tactile input.

[0050] Although a few variations have been described in detail above, other modifications are possible. For example, the logic flow depicted in the accompanying figures and described herein do not require the particular order shown, or sequential order, to achieve desirable results. Other embodiments may be within the scope of the following claims.

Petitioner Exhibit 1002-1062

WHAT IS CLAIMED IS:

1. A point of sale system comprising:

a host;

an intermediate controller including an operating environment and in communication with the host;

a user interface device associated with and in communication with the intermediate controller, wherein the user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more applications for interaction with a customer; and

one or more peripheral devices coupled to at least the intermediate controller via a bus.

2. The point of sale system of claim 1, wherein the web browser is HTTP and the webserver is an HTTP application server.

3. The point of sale system of claim 1, wherein the intermediate controller further includes a telemetry module.

4. The point of sale system of claim 1, wherein the intermediate controller further includes a cashless module.

5. The point of sale system of claim 1, wherein the intermediate controller further includes one or more third party software applications.

6. The point of sale system of claim 5, wherein the third party software applications are accessible by the user interface device.

7. The point of sale system of claim 1, wherein the bus is a multi-drop data bus (MDB).

8. The point of sale system of claim 1, wherein the host is a vending machine controller (VMC) or a PC control board.

Petitioner Exhibit 1002-1063

9. The point of sale system of claim 1, further comprising a cashless bezel coupled to the intermediate controller and wherein the intermediate controller further includes a cashless module for enabling cashless transactions.

10. The point of sale system of claim 1, wherein the intermediate controller is an embedded personal computer control board.

11. The point of sale system of claim 1, wherein the intermediate controller operating environment includes an operating system and file system.

12. The point of sale system of claim 1, wherein the user interface device and intermediate controller are coupled via an Ethernet communication connection.

13. A point of sale system comprising:

a host;

an intermediate controller in communication with the host and including one or more third party applications utilizing an application interface to control components of the point of sale system according to predefined functions;

a user interface device associated with and in communication with the intermediate controller; and

one or more peripheral devices coupled to at least the intermediate controller.

14. The system of claim 13, wherein the components of the point of sale system include one or more of mechanical, electrical, or software components.

15. The system of claim 13, wherein the components of the point of sale system includes one or more of the peripheral devices coupled to the intermediate controller via a bus.

16. The system of claim 13, wherein the components of the point of sale system includes the host.

Petitioner Exhibit 1002-1064

17. The system of claim 13, wherein the components of the point of sale system includes the user interface device.

18. The system of claim 13 further comprising a telemetry unit in communication with a remote licensing server.

19. The system of claim 13, wherein the user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more of the third party applications for interaction with a customer.

20. The system of claim 13, further comprising a telemetry unit and wherein the one or more third party applications have been installed on the point of sale system using a remote back end server to select the one or more third party applications for installation.

21. A point of sale system comprising:

an intermediate controller including an operating environment;

a user interface device associated with and in communication with the intermediate controller, wherein the user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more applications for interaction with a customer; and

one or more peripheral devices coupled to at least the intermediate controller via a bus.

22. The point of sale system of claim 21, wherein the point of sale system is in communication with a host remote from the point of sale system.

Petitioner Exhibit 1002-1065

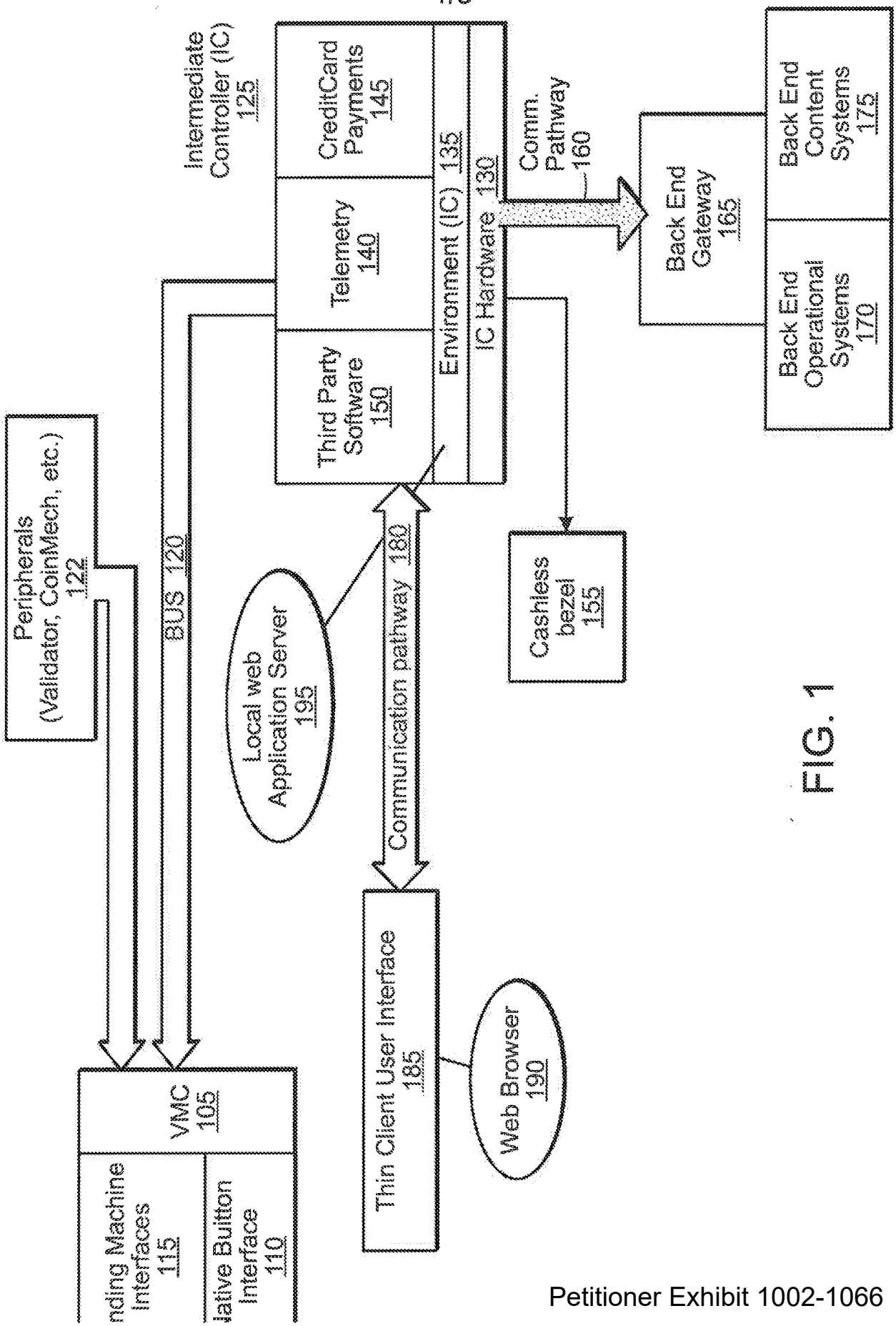

Intermediate Controller (IC) 125
CreditCard Payments 145
Telemetry 140
Third Party Software 150
Environment (IC) 135
IC Hardware 130
Comm. Pathway 160
Back End Gateway 165
Back End Content Systems 175
Back End Operational Systems 170
Peripherals (Validator, CoinMech, etc.) 122
BUS 120
Local web Application Server 195
Communication pathway 180
Cashless bezel 155
VMC 105
nding Machine Interfaces 115
lative Builtton Interface 110
Thin Client User Interface 185
Web Browser 190

FIG. 1

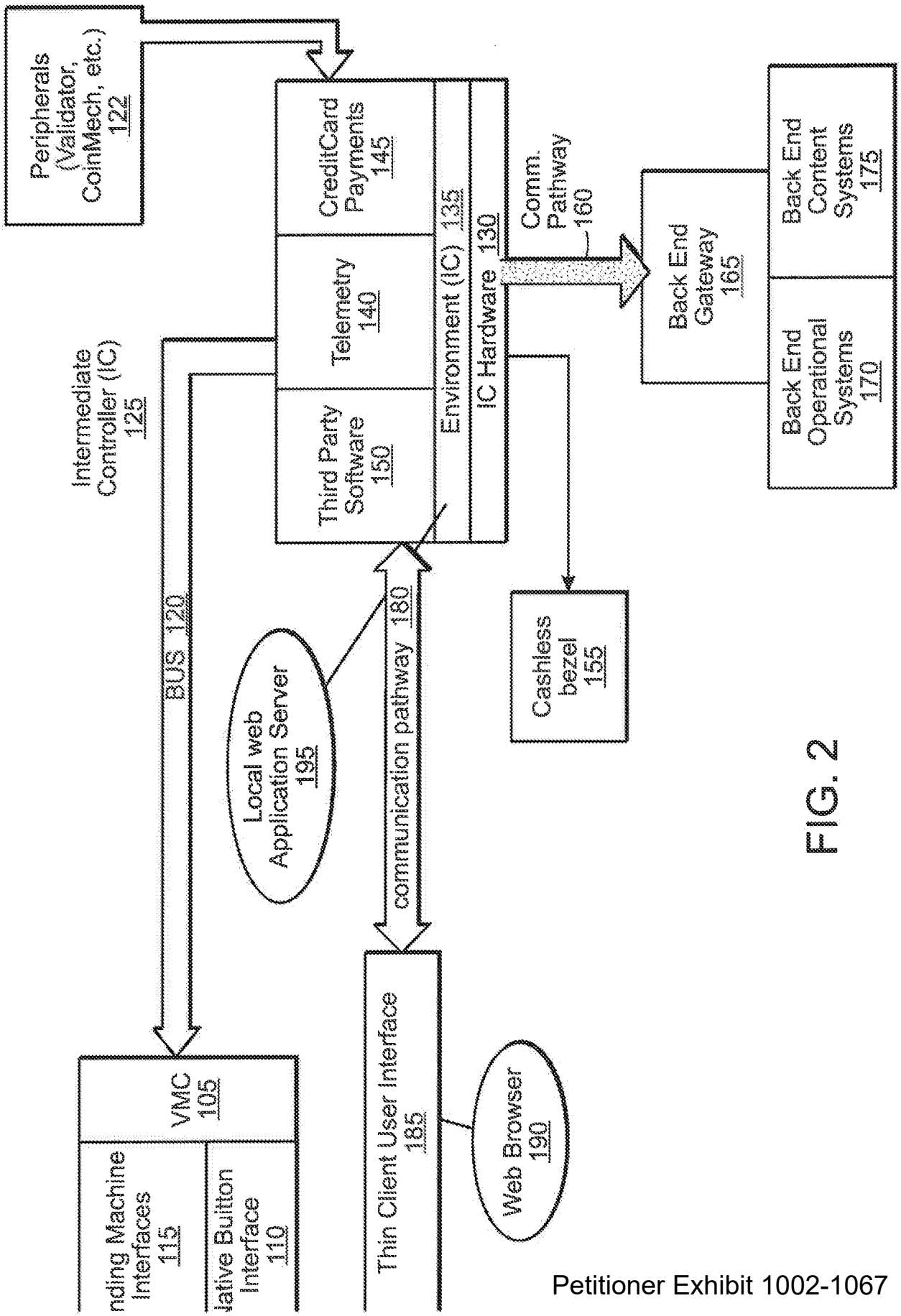

Peripherals (Validator, CoinMech, etc.) 122
CreditCard Payments 145
Telemetry 140
Third Party Software 150
Environment (IC) 135
IC Hardware 130
Comm. Pathway 160
Back End Gateway 165
Back End Content Systems 175
Back End Operational Systems 170
Intermediate Controller (IC) 125
BUS 120
Local web Application Server 195
communication pathway 180
Cashless bezel 155
VMC 105
nding Machine Interfaces 115
iative Buitton Interface 110
Thin Client User Interface 185
Web Browser 190

FIG. 2

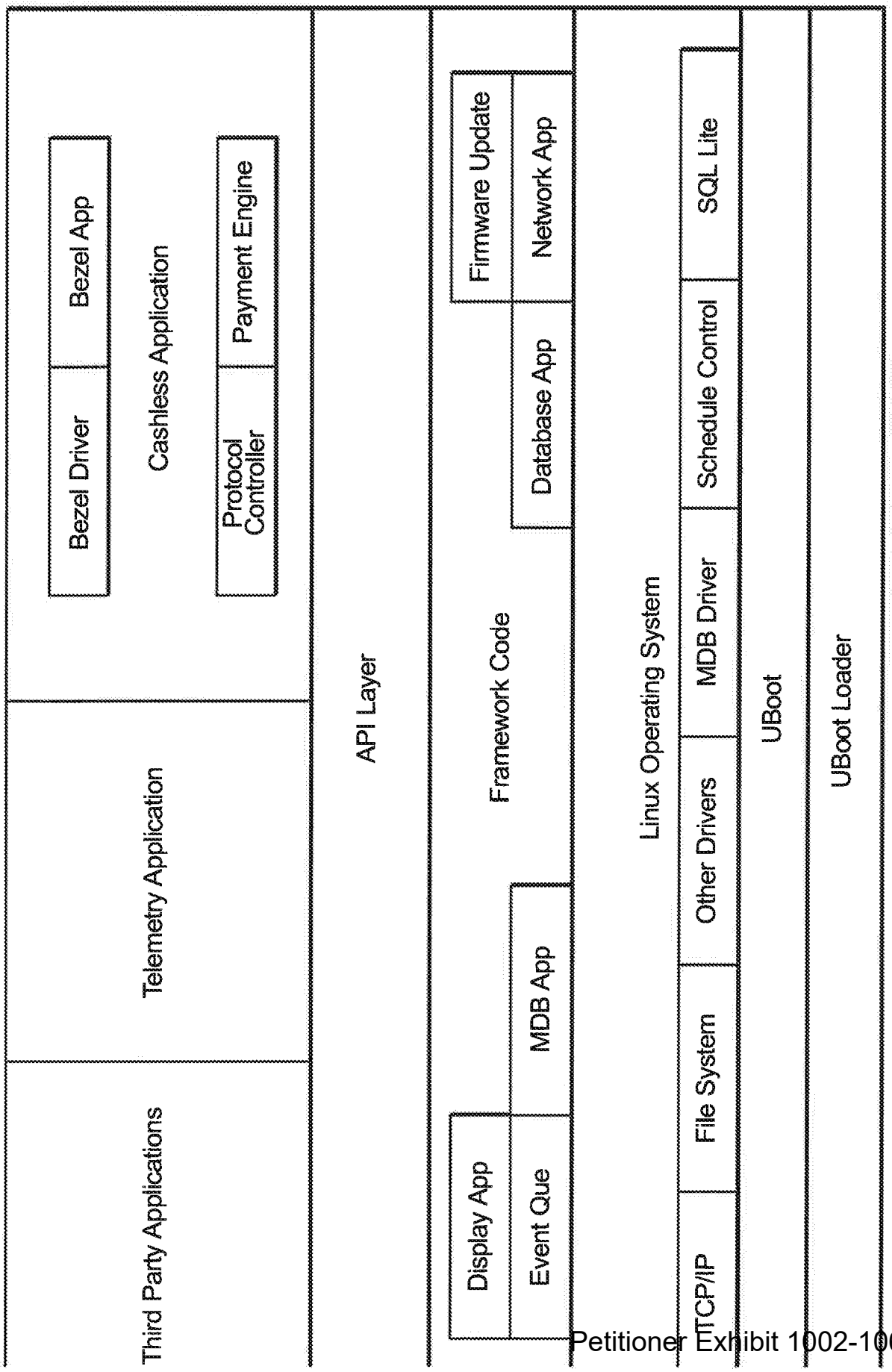


FIG. 3

Petitioner Exhibit 1002-1068

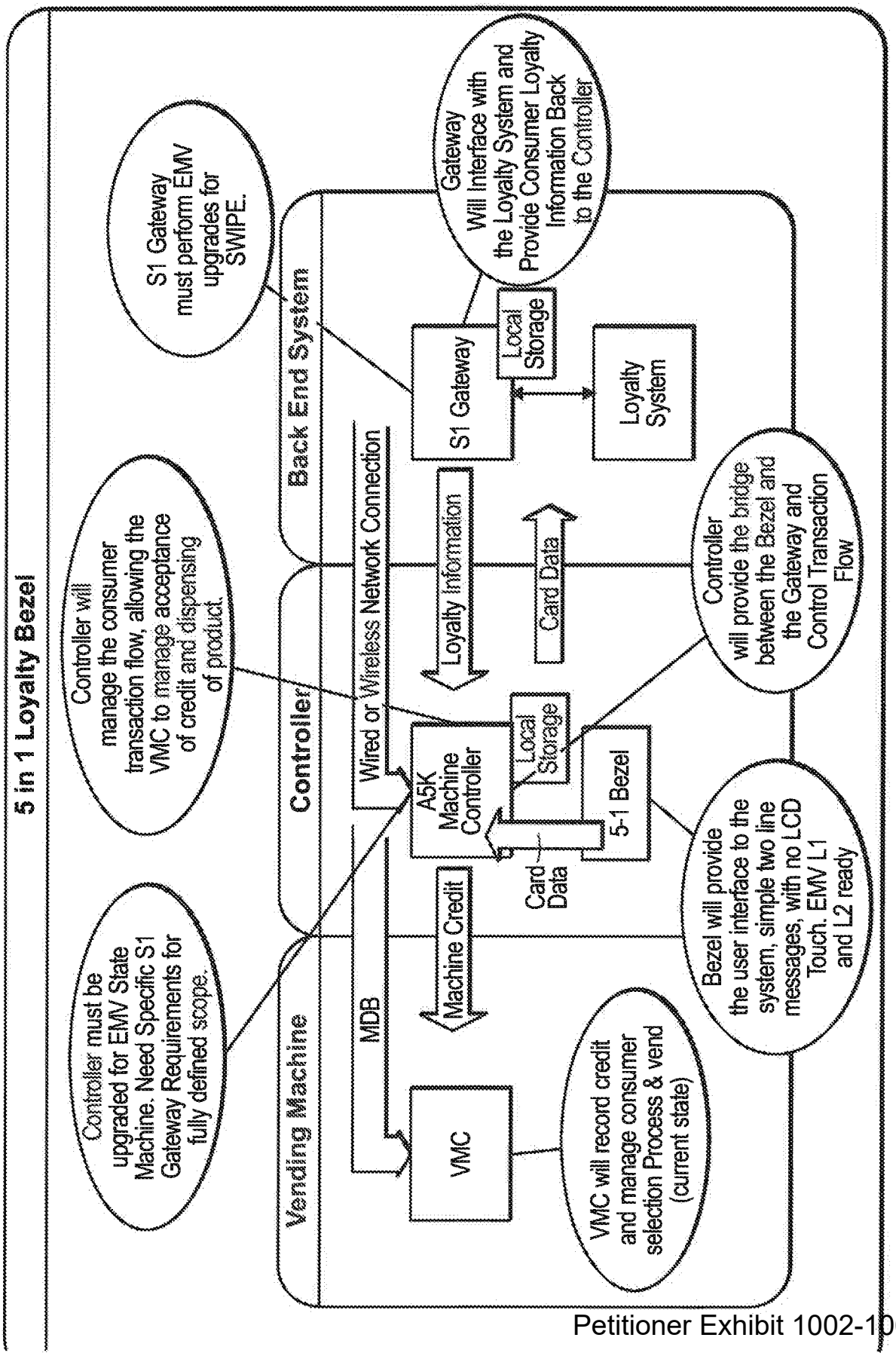

5 in 1 Loyalty Bezel
Vending Machine
Controller
Back End System
MDB
VMC
Machine Credit
Wired or Wireless Network Connection
A5K Machine Controller
Local Storage
Card Data
5-1 Bezel
Loyalty Information
Card Data
S1 Gateway
Local Storage
Loyalty System
Controller must be upgraded for EMV State Machine. Need Specific S1 Gateway Requirements for fully defined scope.
Controller will manage the consumer transaction flow, allowing the VMC to manage acceptance of credit and dispensing of product.
S1 Gateway must perform EMV upgrades for SWIPE.
Gateway Will Interface with the Loyalty System and Provide Consumer Loyalty Information Back to the Controller
Controller will provide the bridge between the Bezel and the Gateway and Control Transaction Flow
Bezel will provide the user interface to the system, simple two line messages, with no LCD Touch. EMV L1 and L2 ready
VMC will record credit and manage consumer selection Process & vend (current state)

FIG. 4

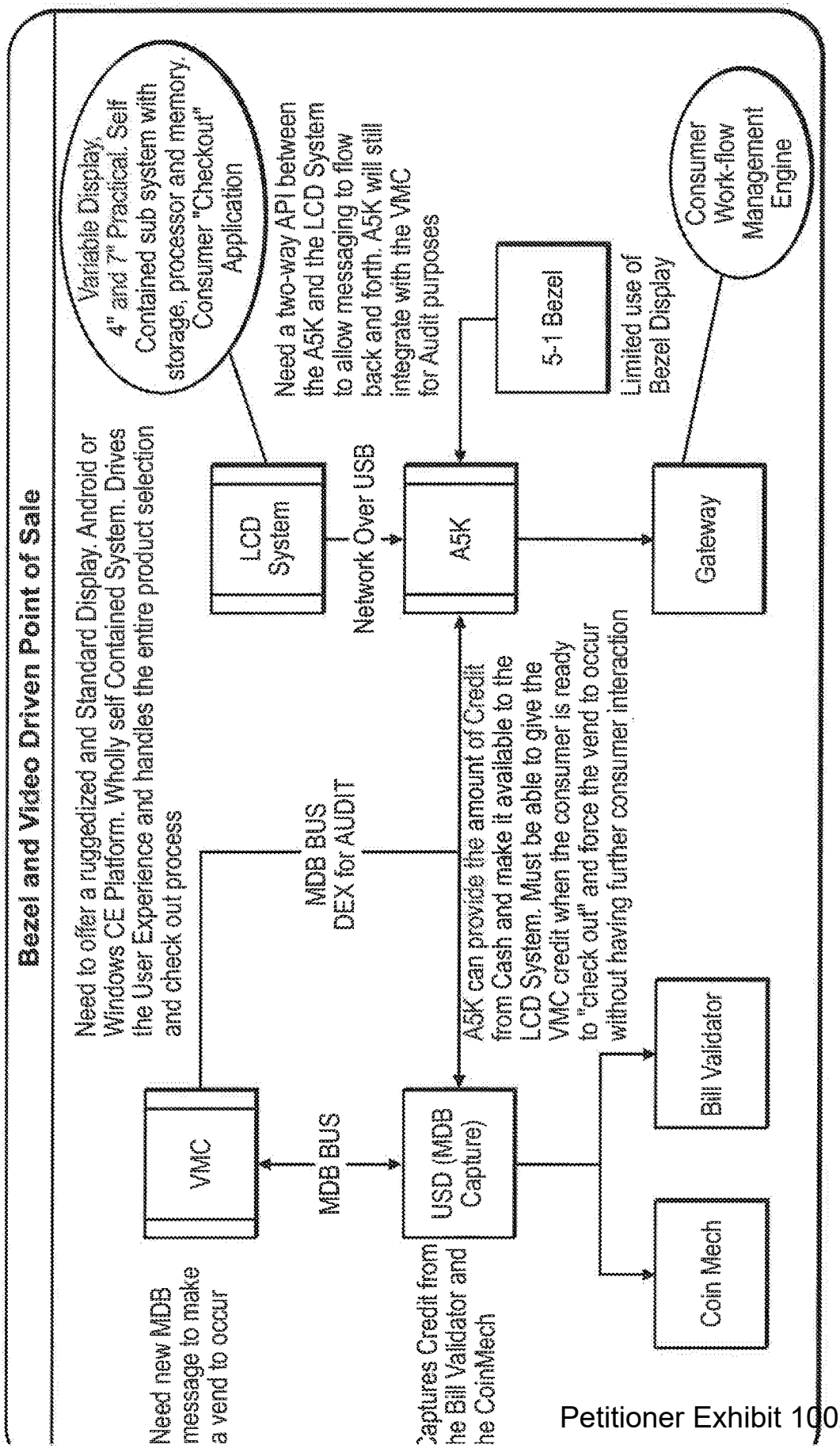


FIG. 5

Petitioner Exhibit 1002-1070

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/075077

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/20 (2014.01)
USPC - 705/16
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06Q 20/20, 30/06 (2014.01)
USPC - 700/214; 705/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G06Q 20/20, 30/0613, 30/0641 (2014.02)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents, Google

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009/0013028 A1 (CANTER et al) 08 January 2009 (08.01.2009) entire document	1-22
Y	US 2006/0252523 A1 (WALKER et al) 09 November 2006 (09.11.2006) entire document	1-22
A	WO 2011/120104 A1 (FELIQUE) 06 October 2011 (06.10.2011) entire document	1-22
A	US 2002/0194387 A1 (DEFOSSE) 19 December 2002 (19.12.2002) entire document	1-22
A	US 2009/0076650 A1 (FAES) 19 March 2009 (19.03.2009) entire document	1-22
A	US 2007/0170249 A1 (RADEMACHER) 26 July 2007 (26.07.2007) entire document	1-22

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 April 2014	16 APR 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

Petitioner Exhibit 1002-1071

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2016 (04.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/123545 A1

(51) International Patent Classification:
G06Q 30/02 (2012.01) *G06Q 30/06* (2012.01)
G06Q 20/18 (2012.01)

(21) International Application Number:
PCT/US2016/015763

(22) International Filing Date:
29 January 2016 (29.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/611,065 30 January 2015 (30.01.2015) US
14/614,336 4 February 2015 (04.02.2015) US

(71) Applicant: **PAYRANGE, INC.** [US/US]; 700 NE Multomah Street, Suite 1400, Portland, OR 97232 (US).

(72) Inventor: **PATEL, Paresh, K.**; 700 NE Multomah Street, Suite 1400, Portland, OR 97232 (US).

(74) Agents: **CRISMAN, Douglas J.** et al.; Morgan Lewis & Bockius LLP, 2 Palo Alto Square, 3000 El Camino Real, Suite 700, Palo Alto, CA 94306 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD AND SYSTEM FOR PROVIDING OFFERS FOR AUTOMATED RETAIL MACHINES VIA MOBILE DEVICES

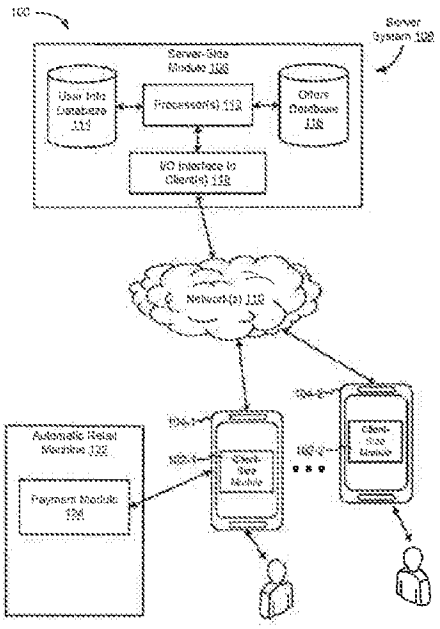


Figure 1

(57) Abstract: A mobile device with a display, processor(s), and memory: displays promotional offers; detects a user input selecting one of the promotional offers; and initiates performance of a transaction with an automatic retail machine to purchase a product stocked by the automatic retail machine. The mobile device also: receives a transaction completion notification from the payment module indicating that the product corresponding to the selected promotional offer was vended by the automatic retail machine; and, in response to receiving the transaction completion notification, provides a prompt to the user of the mobile device to obtain a product code for the vended product to validate the promotional offer. The mobile device further: obtains the product code for the vended product; transmits the product code to the server; and, in response: receives promotion validation information from the server; and displays the promotion validation information indicating whether the respective promotion offer was validated.

WO 2016/123545 A1

Petitioner Exhibit 1002-1072

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2016 (04.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/123545 A1

(51) International Patent Classification:
G06Q 30/02 (2012.01) *G06Q 30/06* (2012.01)
G06Q 20/18 (2012.01)

(21) International Application Number:
PCT/US2016/015763

(22) International Filing Date:
29 January 2016 (29.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/611,065 30 January 2015 (30.01.2015) US
14/614,336 4 February 2015 (04.02.2015) US

(71) Applicant: **PAYRANGE, INC.** [US/US]; 700 NE Multomah Street, Suite 1400, Portland, OR 97232 (US).

(72) Inventor: **PATEL, Paresh, K.**; 700 NE Multomah Street, Suite 1400, Portland, OR 97232 (US).

(74) Agents: **CRISMAN, Douglas J.** et al.; Morgan Lewis & Bockius LLP, 2 Palo Alto Square, 3000 El Camino Real, Suite 700, Palo Alto, CA 94306 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD AND SYSTEM FOR PROVIDING OFFERS FOR AUTOMATED RETAIL MACHINES VIA MOBILE DEVICES

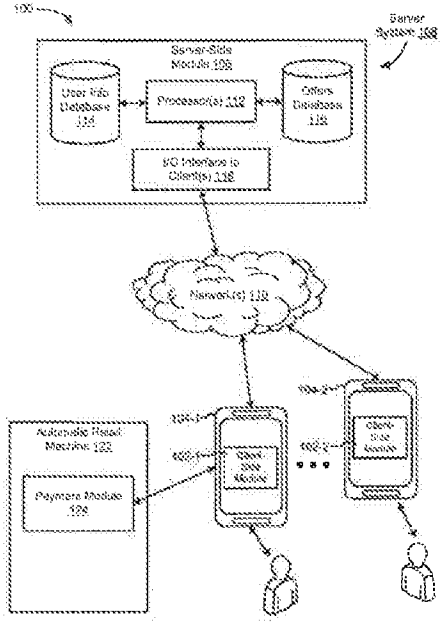


Figure 1

(57) Abstract: A mobile device with a display, processor(s), and memory: displays promotional offers; detects a user input selecting one of the promotional offers; and initiates performance of a transaction with an automatic retail machine to purchase a product stocked by the automatic retail machine. The mobile device also: receives a transaction completion notification from the payment module indicating that the product corresponding to the selected promotional offer was vended by the automatic retail machine; and, in response to receiving the transaction completion notification, provides a prompt to the user of the mobile device to obtain a product code for the vended product to validate the promotional offer. The mobile device further: obtains the product code for the vended product; transmits the product code to the server; and, in response: receives promotion validation information from the server; and displays the promotion validation information indicating whether the respective promotion offer was validated.

WO 2016/123545 A1

Petitioner Exhibit 1002-1073

METHOD AND SYSTEM FOR PROVIDING OFFERS FOR AUTOMATED RETAIL MACHINES VIA MOBILE DEVICES

TECHNICAL FIELD

[0001] The present application relates to the field of payment processing systems, and in particular, to a mobile-device-to-machine payment processing system over a non-persistent network connection.

BACKGROUND

[0002] Vending machines (or more broadly "automatic retail machines"), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g., water, juice, coffee, and soda) and edible food products/items (e.g., snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0003] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0004] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he/she desires, (3) insert payment (e.g., coins, bills, or payment cards), and (4) input his/her selection into the payment accepting unit using a user interface (e.g., a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

Petitioner Exhibit 1002-1074

[0005] As the number of people with Internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension. There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

SUMMARY

[0006] In some implementations, a method of providing and handling promotional offers for an automatic retail machine is performed at a mobile device (e.g., the mobile device 104, Figures 1-2) with a display, one or more processors, and memory. The method includes: displaying one or more promotional offers on the display; detecting a user input selecting a respective promotional offer of the one or more promotional offers; and initiating performance of a transaction with an automatic retail machine coupled with a payment module, where the transaction corresponds to purchase of a product stocked by the automatic retail machine. The method also includes: receiving a transaction completion notification from the payment module, where the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine; and, in response to receiving the transaction completion notification, providing a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer. The method further includes: obtaining the product code for the vended product; after obtaining the product code, transmitting the product code to the server; and, in response to transmitting the product code: receiving promotion validation information from the server; and displaying the promotion validation information on the display, where the promotion validation information indicates whether the respective promotion offer was validated.

[0007] In some implementations, a mobile device (e.g., the mobile device 104, Figures 1-2) includes a display, one or more processors, and memory storing one or more programs for execution by the one or more processors, the one or more programs include instructions for performing, or controlling performance of, the operations of any of the methods described herein. In some implementations, a non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device (e.g., the mobile device 104, Figures 1-2) with one or more processors and a display, cause the computing device to perform, or control performance of, the operations of any of the methods described herein. In some

Petitioner Exhibit 1002-1075

implementations, a mobile device (e.g., the mobile device 104, Figures 1-2) includes means for performing, or controlling performance of, the operations of any of the methods described herein.

[0008] (A1) In some implementations, a method is performed at a mobile device including a display, one or more processors, and memory. The method includes: displaying one or more promotional offers on the display; detecting a user input selecting a respective promotional offer of the one or more promotional offers; and initiating performance of a transaction with an automatic retail machine coupled with a payment module. In some implementations, the transaction corresponds to purchase of a product stocked by the automatic retail machine. The method also includes: receiving a transaction completion notification from the payment module, wherein the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine. In response to receiving the transaction completion notification, the method includes: providing a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer. The method further includes: obtaining the product code for the vended product. After obtaining the product code, the method includes: transmitting the product code to the server. In response to transmitting the product code, the method includes: (i) receiving promotion validation information from the server; and (ii) displaying the promotion validation information on the display. In some implementations, the promotion validation information indicates whether the respective promotion offer was validated.

[0009] (A2) In some implementations of the method of A1, the one or more promotional offers are identified based on at least one of: a unique identifier corresponding to the payment module, at least one of a current time and date, a location of the automatic retail machine, a location of the mobile device, and a unique identifier corresponding to the user of the mobile device.

[0010] (A3) In some implementations of the method of any one A1-A2, the method includes: prior to displaying the one or more promotional offers: (i) obtaining an information packet broadcast by the payment module coupled with the automatic retail machine, the information packet including at least an authorization code and a unique identifier corresponding to the payment module; (ii) sending a transaction authorization request to a server, wherein the transaction authorization includes the authorization code and the unique

Petitioner Exhibit 1002-1076

identifier corresponding to the payment module; and, (iii) in response to the transaction authorization request, receiving authorization information from the server that includes an authorization grant token for initiating a transaction with the automatic retail machine coupled with the payment module and the one or more promotional offers from the server.

[0011] (A4) In some implementations of the method of any one of A3, performance of the transaction with the automatic retail machine coupled with the payment module is initiated by sending the authorization grant token to the payment module, the authorization grant token including the authorization code included in the broadcast information packet.

[0012] (A5) In some implementations of the method of any one of A1-A4, obtaining the product code further includes: (i) capturing an image of the product that includes the product code; and (ii) extracting the product code from the captured image.

[0013] (A6) In some implementations of the method of any one of A1-A5, obtaining the product code further includes: scanning the product code of the product with a scanner unit of the mobile device.

[0014] (A7) In some implementations of the method of any one of A1-A6, the promotion validation information indicates the price of the product after the application of the respective promotional offer.

[0015] (A8) In some implementations of the method of any one of A1-A7, the method further includes: after obtaining the product code, determining whether a predetermined time period has expired. In accordance with a determination that the time period has expired, the method includes: providing a notification to the user of mobile device indicating that the respective promotional offer has expired. In accordance with a determination that the time period has not expired, the method includes: transmitting the product code to the server.

[0016] (A9) In some implementations of the method of any one of A1-A8, the method includes: transmitting the transaction completion notification to the server.

[0017] (A10) In some implementations of the method of any one of A1-A9, the mobile device further includes a first transceiver associated with a short-range communication protocol and a second transceiver associated with a long-range communication protocol.

Petitioner Exhibit 1002-1077

[0018] (A11) In an additional aspect, a method is performed at a mobile device including a display, one or more processors, a short-range transceiver (e.g., a first communication unit), a long-range transceiver (e.g., a second communication unit) that is distinct from the short-range transceiver, and memory. In some implementations, the method includes: recognizing, by an application executing on the mobile device, an automatic retail machine based at least in part on a signal strength corresponding to broadcasted information from an electronic payment device coupled with the automatic retail machine. The method also includes: displaying one or more promotional offers that are associated with the automatic retail machine on the display. In some implementations, the method further includes: detecting a user input selecting a respective promotional offer of the one or more promotional offers. The method additionally includes: initiating, via the short-range transceiver, performance of a transaction with the automatic retail machine, the transaction corresponding to purchase of a product stocked by the automatic retail machine. The method also includes: receiving, via the short-range transceiver, a transaction completion notification from the electronic payment device, the transaction completion notification indicating that the product was vended by the automatic retail machine. In response to receiving the transaction completion notification, the method includes: providing a prompt instructing a user of the mobile device to obtain a product code for the vended product. The method further includes: obtaining, based on user input provided in response to the prompt, the product code for the vended product. After obtaining the product code, the method includes: transmitting, via the long-range transceiver, the product code to a server. In response to transmitting the product code: (i) receiving, via the long-range transceiver, promotion validation information from the server; and (ii) based on the promotion validation information, displaying, on the display, an indication as to whether the respective promotional offer was validated and information identifying a credit to the user after application of the respective promotional offer.

[0019] (A12) In some implementations of the method of A11, the method further includes any of the operations described in A2-A10 above.

[0020] Various advantages of the present application are apparent in light of the descriptions below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The aforementioned features and advantages of the disclosed technology as well as additional features and advantages thereof will be more clearly understood hereinafter

Petitioner Exhibit 1002-1078

as a result of a detailed description of preferred implementations when taken in conjunction with the drawings.

[0022] To describe the technical solutions in the implementations of the present disclosed technology or in the prior art more clearly, the following briefly introduces the accompanying drawings required for describing the implementations or the prior art. Apparently, the accompanying drawings in the following description show merely some implementations of the present disclosed technology, and persons of ordinary skill in the art may still derive other drawings from these accompanying drawings without creative efforts.

[0023] Figure 1 is a block diagram of a payment processing system in accordance with some implementations.

[0024] Figure 2 is a block diagram of a mobile device in accordance with some implementations.

[0025] Figure 3 is a block diagram of a server system in accordance with some implementations.

[0026] Figure 4 is a schematic block diagram of an automatic retail machine in accordance with some implementations.

[0027] Figure 5 is a block diagram of a payment module in accordance with some implementations.

[0028] Figure 6A is a perspective view of the payment module of Figure 5 (e.g., an in-line dongle adapter) in accordance with some implementations.

[0029] Figure 6B is a perspective view taken from the first end of the payment module of Figure 6A in accordance with some implementations.

[0030] Figure 6C is a perspective view taken from the second end of the payment module of Figure 6A in accordance with some implementations.

[0031] Figure 7 is a perspective view of the payment module of Figure 6A within the automatic retail machine of Figure 4 in accordance with some implementations.

Petitioner Exhibit 1002-1079

[0032] Figure 8 is a schematic flow diagram of a process for initiating a transaction in accordance with some implementations.

[0033] Figure 9 is a schematic flow diagram of a process for acknowledging a transaction in accordance with some implementations.

[0034] Figure 10A is a block diagram of an information packet broadcast by the payment module in accordance with some implementations.

[0035] Figure 10B is a block diagram of an authorization request in accordance with some implementations.

[0036] Figure 10C is a block diagram of an authorization grant token in accordance with some implementations.

[0037] Figure 10D is a block diagram of transaction information generated by the payment module in accordance with some implementations.

[0038] Figures 11A-11G illustrate exemplary user interface for displaying promotional offers in accordance with some implementations.

[0039] Figures 12A-12C illustrate a flowchart diagram of a method of providing and handling promotional offers for an automatic retail machine in accordance with some implementations.

[0040] Like reference numerals refer to corresponding parts throughout the several views of the drawings.

DESCRIPTION OF IMPLEMENTATIONS

[0041] Reference will now be made in detail to implementations, examples of which are illustrated in the accompanying drawings. In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the subject matter presented herein. But it will be apparent to one skilled in the art that the subject matter may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the implementations.

Petitioner Exhibit 1002-1080

[0042] The following clearly and completely describes the technical solutions in the implementations of the present application with reference to the accompanying drawings in the implementations of the present application. Apparently, the described implementations are merely a part rather than all of the implementations of the present application. All other implementations obtained by persons of ordinary skill in the art based on the implementations of the present application without creative efforts shall fall within the protection scope of the present application.

[0043] Figure 1 illustrates a payment processing system 100. Figures 2-5 illustrate example devices within the payment processing system 100. Figures 6A-6C and 7 show various views of the payment module 124 and the automatic retail machine 122. Figure 8 illustrates a schematic flow diagram of a process 800 for initiating a transaction within the payment processing system 100. Figure 9 illustrates a schematic flow diagram of a process 900 for acknowledging a transaction within the payment processing system 100. Figures 10A-10D illustrate data structures associated with initiating and performing transactions within the payment processing system 100. Figures 11A-11G illustrate example user interfaces for displaying promotional offers. Figures 12A-12C illustrate a flowchart diagram of a method 1200 of providing and handling promotional offers for an automatic retail machine. The user interfaces in Figures 11A-11G are used to illustrate the method in Figures 12A-12C.

EXAMPLE DEVICES AND SYSTEMS

[0044] Figure 1 is a block diagram of a payment processing system 100 in accordance with some implementations. In accordance with some implementations, the payment processing system 100 includes client-side processing 102-1, 102-2 (hereinafter "client-side modules 102") executed on a mobile device 104-1, 104-2, server-side processing 106 (hereinafter "server-side module 106") executed on a server system 108 (sometimes also herein referred to as "the server"), and a payment module 124 coupled with an automatic retail machine 122. The client-side module 102 provides client-side functionalities for the payment processing system 100 and communications with both the server-side module 106 and the payment module 124. In some implementations, an application associated with the client-side module 102 provides a user interface to the payment processing system 100 for the mobile device 104. The client-side module 102 communicates with the server-side module 106 via a long-range communication protocol (e.g., GSM, CDMA, Wi-Fi, or the like)

Petitioner Exhibit 1002-1081

through one or more networks 110, and the client-side module 102 communicates with the payment module 124 via a short-range communication protocol (e.g., near-field communication (NFC), BLUETOOH, BLUETOOH low-energy (BLE), or the like). The server-side module 106 provides server-side functionalities for the payment processing system 100 for any number of client modules 102 each residing on a respective mobile device 104.

[0045] The payment processing system 100 harnesses the connectivity of the mobile device 104 to communicate with the payment module 124, which has neither a dedicated communication connection nor a long-range communication transceiver. As such, the mobile device 104 acts as a relay between the payment module 124 and the server system 108. Furthermore, leveraging the connectivity of the mobile device 104 helps to keep costs down from the point of view of the operator of the automatic retail machine 122.

[0046] In some implementations, the server-side module 106 includes one or more processors 112, a user information database 114, an offers database 116, and an input and output (I/O) interface to one or more clients 118. The I/O interface to one or more clients 118 facilitates the client-facing input and output processing for the server-side module 106. In some implementations, the one or more processors 112 authorize transaction requests, determine promotional offers for a particular mobile device 104, perform transaction accounting, and acknowledge completed transactions. The user information database 114 stores information for each user of the payment processing system 100 (e.g., user ID, account credentials (user name and password), transaction history, account balance, linked credit cards and bank accounts, and/or the like), and the offers database 116 stores promotional offers provided by manufacturers, distributors, retailers, and the like.

[0047] Examples of the mobile device 104 include, but are not limited to, a handheld computer, a wearable computing device, a personal digital assistant (PDA), a tablet computer, a laptop computer, a desktop computer, a cellular telephone, a smart phone, an enhanced general packet radio service (EGPRS) mobile phone, a media player, a navigation device, a game console, a television, a remote control, a point-of-sale (POS) terminal, vehicle-mounted computer, an eBook reader, or a combination of any two or more of these data processing devices or other data processing devices.

Petitioner Exhibit 1002-1082

[0048] Examples of the one or more networks 110 include local area networks (LAN) and wide area networks (WAN) such as the Internet. One or more networks 110 are, optionally, implemented using any known network protocol, including various wired or wireless protocols, such as Ethernet, Universal Serial Bus (USB), FIREWIRE, Long Term Evolution (LTE), Global System for Mobile Communications (GSM), Enhanced Data GSM Environment (EDGE), code division multiple access (CDMA), time division multiple access (TDMA), Bluetooth, Wi-Fi, voice over Internet Protocol (VoIP), Wi-MAX, or any other suitable communication protocol.

[0049] The server system 108 is implemented on one or more standalone data processing apparatuses or a distributed network of computers. In some implementations, the server system 108 also employs various virtual devices and/or services of third party service providers (e.g., third-party cloud service providers) to provide the underlying computing resources and/or infrastructure resources of the server system 108. In some implementations, the server system 108 includes, but is not limited to, a handheld computer, a tablet computer, a laptop computer, a desktop computer, or a combination of any two or more of these data processing devices or other data processing devices.

[0050] The payment processing system 100 shown in Figure 1 includes both a client-side portion (e.g., the client-side module 102) and a server-side portion (e.g., the server-side module 106). In some implementations, data processing is implemented as a standalone application installed on the mobile device 104. In addition, the division of functionalities between the client and server portions of the payment processing system 100 can vary in different implementations. For example, in some implementations, the client-side module 102 is a thin-client that provides only user-facing input and output processing functions, and delegates all other data processing functionalities to a backend server (e.g., the server system 108). Although many aspects of the present technology are described from the perspective of the server system 108, the corresponding actions performed by the mobile device 104 would be apparent to ones skilled in the art without any creative efforts. Furthermore, some aspects of the present technology may be performed by the server system 108, the mobile device 104, or the server system 108 and the mobile device 104 cooperatively.

[0051] Figure 2 is a block diagram of the mobile device 104 associated with a user in accordance with some implementations. The mobile device 104, typically, includes one or more processing units (CPUs) 202, two or more communication devices 204, memory 206,

Petitioner Exhibit 1002-1083

and one or more communication buses 208 for interconnecting these components (sometimes called a chipset). The two or more communication devices 204 include a first transceiver associated with a short-range communication protocol (e.g., NFC, BLE, or the like) and a second transceiver associated with a long-range communication protocol (e.g., GSM, CDMA, Wi-Fi, or the like). The mobile device 104 also includes a user interface 210. The user interface 210 includes one or more output devices 212 that enable presentation of media content (e.g., text, images, audio, video, etc.), including one or more speakers and/or one or more visual displays. The user interface 210 also includes one or more input devices 214, including user interface components that facilitate user input such as a keyboard, a mouse, a voice-command input unit or microphone, a touch screen display, a touch-sensitive input pad, a gesture capturing camera, or other input buttons or controls. Furthermore, in some implementations, the mobile device 104 uses a microphone and voice recognition or a camera and gesture recognition to supplement or replace the keyboard. In some implementations, the mobile device 104 optionally includes one or more sensors 215, which provide context information as to the current state of the mobile device 104 or the environmental conditions associated with mobile device 104. The one or more sensors 215 include, but are not limited, to one or more microphones, one or more cameras, an ambient light sensor, one or more accelerometers, one or more gyroscopes, a temperature sensor, one or more motion sensors, one or more biometric/biological sensors, and so on. In some implementations, the mobile device 104 optionally includes a location detection device 217, such as a GPS (global positioning satellite) or other geo-location receiver, for determining the location of the mobile device 104.

[0052] The memory 206 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid state memory devices; and, optionally, includes non-volatile memory, such as one or more magnetic disk storage devices, one or more optical disk storage devices, one or more flash memory devices, or one or more other non-volatile solid state storage devices. The memory 206, optionally, includes one or more storage devices remotely located from the one or more processing units 202. The memory 206, or alternatively the non-volatile memory within the memory 206, includes a non-transitory computer readable storage medium. In some implementations, the memory 206, or the non-transitory computer readable storage medium of the memory 206, stores the following programs, modules, and data structures, or a subset or superset thereof:

Petitioner Exhibit 1002-1084

- operating system 216 including procedures for handling various basic system services and for performing hardware dependent tasks;
- communication module 218 for transmitting signals to and receiving signals from other devices (e.g., the server system 108 and the payment module 124) via the two or more communication devices 204;
- presentation module 220 for enabling presentation of information (e.g., a user interface for the application(s) 226 or the application associated with client-side module 102, widgets, websites and web pages thereof, and/or games, audio and/or video content, text, etc.) at the mobile device 104 via one or more output devices 212 (e.g., displays, speakers, etc.) associated with the user interface 210;
- input processing module 222 for detecting one or more user inputs or interactions from the one or more input devices 214 and interpreting the detected inputs or interactions;
- web browser module 224 for navigating, requesting (e.g., via HTTP), and displaying websites and web pages thereof;
- one or more applications 226 for execution by the mobile device 104 (e.g., games, application marketplaces, payment platforms, and/or other web or non-web based applications);
- client-side module 102, which provides client-side data processing and functionalities for the payment processing system 100, including but not limited to:
    - broadcast obtaining module 230 for receiving, via the first transceiver, an information packet broadcast by a respective payment module 124, where the information packet at least includes a unique identifier corresponding to the respective payment module 124 (i.e., the device ID) and an authorization code for initiating a transaction with an automatic retail machine 122 to which the respective payment module 124 is coupled;
    - transaction authorization module 232 for: sending, via the second transceiver, a transaction authorization request to the server system 108 including the authorization code; receiving, via the second transceiver, an authorization grant token from the server system 108, including the authorization code, for initiating a transaction with the automatic retail machine 122 to which the

Petitioner Exhibit 1002-1085

respective payment module 124 is coupled; and storing the received authorization grant token (e.g., in the user data 264);

- offer(s) module 234 for: obtaining (i.e., receiving or retrieving), via the second transceiver, promotional offers from the server system 108 (e.g., in response to sending the transaction authorization request, as part of an update to the application associated with the client-side module 102, or at another time); storing the promotional offers obtained from the server system in the offers database 266; optionally determining one or more promotional offers based on one or more of a plurality of factors (e.g., the device ID, user ID and history, current location of the mobile device 104, current time/date, and/or the like); presenting one or more promotional offers to the user of the mobile device via the one or more output devices 212 (e.g., a display); and detecting a user input selecting a respective one of the one or more promotional offers presented to the user of the mobile device 104;
- trigger detecting module 236 for detecting a trigger to initiate a transaction with the automatic retail machine 122 to which the respective payment module 124 is coupled (e.g., the trigger is a gesture or other user input by the user of the mobile device 104, entrance of the mobile device 104 into a payment zone based on the RSSI observed from the payment module 124, selection of the respective promotional offer, or the like);
- transaction initiating module 238 for initiating a transaction with the automatic retail machine 122 coupled with the respective payment module 124 by sending, via the first transceiver, the stored authorization grant token to the respective payment module 124;
- transaction completion notification receiving module 240 for receiving, via the first transceiver, a transaction completion notification from the payment module 124, where the transaction completion notification includes one or more of: transaction status information (e.g., indicating whether the transaction with the automatic retail machine 122 was successful, aborted, or failed); transaction detail information (e.g., the authorization code, the amount of the transaction, the good/product associated with the transaction, the time/date the transaction was completed, transaction error information, and/or

Petitioner Exhibit 1002-1086

the like); and optionally includes other miscellaneous information regarding the respective payment module 124 and/or the automatic retail machine 122 to which the respective payment module 124 is coupled, such as interrupted transaction information, status flags, inventory information, past hard currency transaction information, other cashless transaction information, and/or the like;

- product code processing module 242 for: providing a prompt to the user of the mobile device 104 via the one or more output devices 212 to obtain a product code for a vended product to validate the respective promotional offer; obtaining the product code for the vended product (e.g., the user of the mobile device 104 manually inputs the product code, the user of the mobile device 104 captures an image of the vended product from which the product code is extracted, the user of the mobile device 104 uses a scanner plug-in of the application associated with the client-side module 102 to obtain the product code, or the like); and either validating the product code or sending, via the second transceiver, the obtained product code to the server system 108 for validation;
- information relaying module 244 for transmitting, via the second transceiver, information from the payment module 124 to the server system 108 (e.g., the transaction status information, the transaction detail information, the other miscellaneous information regarding the respective payment module 124 and/or the automatic retail machine 122 to which the respective payment module 124 is coupled, and/or the like);
- offer validation module 246 for: receiving, via the second transceiver, promotion validation information from the server system 108; and presenting the promotion validation information to the user of the mobile device via the one or more output devices 212 (e.g., the display); and
- acknowledgment module 248 for sending, via the first transceiver, acknowledgment information to the payment module 124, where the acknowledgment information acknowledges that the server system 108 received and processed the transaction status information and the transaction detail information; and

Petitioner Exhibit 1002-1087

- client data 260 storing data associated with the payment processing system 100, including, but is not limited to:
    - user profile 262 storing information for the user of the mobile device 104, including but not limited to: a unique user identifier (i.e., a user ID), login credentials (i.e., user name or handle and password), transaction history, payment data (e.g., account balance, linked credit card or bank information, app credit or gift card balance, billing address, shipping address, etc.), contact information (e.g., email address, phone number, etc.), custom parameters for the user (e.g., age, location, hobbies, etc.), identified trends and/or likes/dislikes of the user, and/or the like;
    - user data 264 storing transaction history information, authorization grant tokens, and/or the like; and
    - offers database 266 storing promotional offers provided by manufacturers, distributors, retailers, and/or the like.

[0053] Each of the above identified elements may be stored in one or more of the previously mentioned memory devices, and corresponds to a set of instructions for performing a function described above. The above identified modules or programs (i.e., sets of instructions) need not be implemented as separate software programs, procedures, modules or data structures, and thus various subsets of these modules may be combined or otherwise re-arranged in various implementations. In some implementations, the memory 206, optionally, stores a subset of the modules and data structures identified above. Furthermore, the memory 206, optionally, stores additional modules and data structures not described above.

[0054] Figure 3 is a block diagram illustrating the server system 108 in accordance with some implementations. The server system 108, typically, includes one or more processing units (CPUs) 112, one or more communication devices 304 (e.g., including the I/O interface to one or more clients 118), memory 306, and one or more communication buses 308 for interconnecting these components (sometimes called a chipset). The memory 306 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid state memory devices; and, optionally, includes non-volatile memory, such as one or more magnetic disk storage devices, one or more optical disk storage devices, one or more flash memory devices, or one or more other non-volatile solid state

Petitioner Exhibit 1002-1088

storage devices. The memory 306, optionally, includes one or more storage devices remotely located from the one or more processing units 112. The memory 306, or alternatively the non-volatile memory within the memory 306, includes a non-transitory computer readable storage medium. In some implementations, the memory 306, or the non-transitory computer readable storage medium of the memory 306, stores the following programs, modules, and data structures, or a subset or superset thereof:

- operating system 310 including procedures for handling various basic system services and for performing hardware dependent tasks;
- network communication module 312 for transmitting signals to and receiving signals from mobile devices 104 via the one or more communication devices 304;
- server-side module 106, which provides server-side data processing and functionalities for the payment processing system 100, including but not limited to:
    - transaction authorization module 314 for: receiving a transaction request from a respective mobile device 104, where the transaction request includes a device ID associated with a respective payment module 124 and an authorization code; and validating the transaction request;
    - encryption/decryption module 316 for: identifying an encryption/decryption key linked to the device ID for the respective payment module 124; decrypting the authorization code with the identified encryption/decryption key; and encrypting the authorization grant token with the identified encryption/decryption key;
    - offer determining module 318 for determining one or more promotional offers based on one or more of a plurality of factors (e.g., the device ID included in the transaction request, the user ID and history associated with the user of the respective mobile device 104, current location of the respective mobile device 104, current time/date, and/or the like);
    - transmitting module 320 for: transmitting, in accordance with a determination that the transaction request is validated, an authorization grant token and the one or more promotional offers to the respective mobile device 104; and transmitting acknowledgment information once a transaction is completed to the respective mobile device 104;

Petitioner Exhibit 1002-1089

- receiving module 322 for receiving information from the respective mobile device 104, including but not limited to: a product code and a corresponding selected promotional offer, the transaction status information for a respective transaction, the transaction detail information for the respective transaction, and/or the other miscellaneous information;
- offer validation module 324 for: validating a promotional offer based on a received product code, transaction status information, and/or transaction detail information; and sending, in accordance with a determination that the promotional offer is validated, promotion validation information to the respective mobile device 104;
- accounting module 326 for debiting an account balance or charging a linked credit card or bank account according to the transaction detail information; and
- acknowledgment module 328 for sending acknowledgment information to the respective mobile device 104 for relay to the respective payment module 124;

* server data 340 storing data for the payment processing system 100, including but not limited to:
  - user information database 114 storing stores information for each user of the payment processing system 100, including but not limited to: a unique user identifier (i.e., a user ID), login credentials (i.e., user name or handle and password), transaction history, payment data (e.g., account balance, linked credit card or bank information, app credit or gift card balance, billing address, shipping address, etc.), contact information (e.g., email address, phone number, etc.), custom parameters for the user (e.g., age, location, hobbies, etc.), identified trends and/or likes/dislikes of the user, and/or the like;
  - offers database 116 storing promotional offers provided by manufacturers, distributors, retailers, and/or the like; and
  - payment module database 342 storing information for each payment module 124 of the payment processing system 100, including but not limited to: a unique payment module identifier (i.e., a device ID), an encryption/decryption key, and/or the like.

Petitioner Exhibit 1002-1090

[0055] Each of the above identified elements may be stored in one or more of the previously mentioned memory devices, and corresponds to a set of instructions for performing a function described above. The above identified modules or programs (i.e., sets of instructions) need not be implemented as separate software programs, procedures, or modules, and thus various subsets of these modules may be combined or otherwise re-arranged in various implementations. In some implementations, the memory 306, optionally, stores a subset of the modules and data structures identified above. Furthermore, the memory 306, optionally, stores additional modules and data structures not described above.

[0056] In some implementations, at least some of the functions of the server system 108 are performed by the mobile device 104, and the corresponding sub-modules of these functions may be located within the mobile device 104 rather than the server system 108. In some implementations, at least some of the functions of mobile device 104 are performed by the server system 108, and the corresponding sub-modules of these functions may be located within the server system 108 rather than the mobile device 104. The mobile device 104 and the server system 108 shown in Figures 2-3, respectively, are merely illustrative, and different configurations of the modules for implementing the functions described herein are possible in various implementations.

[0057] Figure 4 is a schematic block diagram illustrating the automatic retail machine 122 in accordance with some implementations. For example, the automatic retail machine 122 is a vending machine or kiosk that dispenses an item or product (e.g., snacks, other foodstuffs, school supplies, drinks, tickets, and the like) in response to user payment for and selection of the item or product. The automatic retail machine 122 includes: a controller 402; a power supply 404; memory 406; a user interface 408; one or more optional sensors 414; a multi-drop bus (MDB) 416; and a dispenser 424.

[0058] In some implementations, the controller 402 is a microcontroller, microprocessor, CPU, FPGA, ASIC, or the like that manages the functions of the automatic retail machine 122. The power supply 404 is a connection to an external power source (e.g., AC or DC) or a connection to an internal power source (e.g., a battery). In some implementations, the power supply 404 further includes one or more of a power converter and/or inverter, a rectifier, a power conditioner, or the like for providing power to the various components of the automatic retail machine 122. The memory 406 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid

Petitioner Exhibit 1002-1091

state memory devices; and, optionally, includes non-volatile memory, such as one or more magnetic disk storage devices, one or more optical disk storage devices, one or more flash memory devices, or one or more other non-volatile solid state storage devices. In some implementations, the memory 406 stores an operating system and instructions for carrying out the functions and processes of the automatic retail machine 122 (e.g., dispensing items, tracking inventory, temperature control, power control, and the like). In some implementations, the memory 406 also stores configuration data and DEX (data exchange) data corresponding to the inventory of the automatic retail machine 122 and transactions performed with the automatic retail machine 122.

[0059] The user interface 408 includes one or more output devices 410 that enable presentation of information (e.g., text, images, audio, video, etc.), for example, one or more speakers and/or one or more visual displays. The user interface 408 also includes one or more input devices 412, including user interface components that facilitate user input and selection of items such as a microphone, a keypad, a touch screen display, a gesture capturing camera, or other input buttons or controls. The one or more optional sensors 414 include, but are not limited, to one or more microphones, one or more cameras, an ambient light sensor, one or more accelerometers, one or more gyroscopes, a temperature sensor, one or more motion sensors, one or more biometric/biological sensors, and so on.

[0060] In some implementations, a variety of payment devices are coupled with the MDB 416 including any combination of one or more cashless payment devices 418 (e.g., credit card reader(s)) for accepting cashless payments, one or more bill validators 420 for accepting and validating bills, and one or more coin accepters 422 for accepting coins and providing change. In some implementations, the dispenser 424 is an electromechanical system (e.g., motors, actuators, and the like) for dispensing or vending items or products stocked by the automatic retail machine. 122 For example, a user inserts a bill into the bill validator(s) 420 and is credited with an amount of money equal to the bill. Continuing with this example, the one or more output devices 410 (e.g., a display) shows the credited amount, and the user selects an item via the one or more input devices 412 (e.g., using a keypad or a sequence of button presses). Subsequently, the controller 402 sends signals to the dispenser 424 to dispense the selected product, and the dispenser dispenses or vends the selected product.

Petitioner Exhibit 1002-1092

[0061] Figure 5 is a block diagram illustrating the payment module 124 in accordance with some implementations. In some implementations, the payment module 124 is an in-line adapter dongle with male and female connectors that couples with the multi-drop bus (MDB) of the respective automatic retail machine 122 as shown in Figures 6B-6C and 7. For example, the payment module is connected in-line into the MDB 416 in Figure 4. The payment module 124, typically, includes one or more processing units (CPUs) 512, a communication device 504 (e.g., a transceiver associated with a short-range communication protocol such as NFC, BLE, or the like), memory 506, and one or more communication buses 508 for interconnecting these components (sometimes called a chipset). The memory 506 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid state memory devices; and, optionally, includes non-volatile memory, such as one or more magnetic disk storage devices, one or more optical disk storage devices, one or more flash memory devices, or one or more other non-volatile solid state storage devices. The memory 506, optionally, includes one or more storage devices remotely located from one or more processing units 512. The memory 506, or alternatively the non-volatile memory within the memory 506, includes a non-transitory computer readable storage medium. In some implementations, the memory 506, or the non-transitory computer readable storage medium of the memory 506, stores the following programs, modules, and data structures, or a subset or superset thereof:

- operating system 510 including procedures for handling various basic system services and for performing hardware dependent tasks;
- communication module 512 for transmitting signals to and receiving signals from mobile devices 104 via the communication device 504;
- transaction-processing module 514, including but not limited to:
    - broadcasting module 516 for: broadcasting an information packet to zero or more client devices 104 within the communication zone of the payment module 124 (i.e., BLE range), where the information packet at least includes a unique identifier corresponding to the payment module 124 (e.g., the device ID) and an authorization code for initiating a transaction with the automatic retail machine 122 to which the payment module 124 is coupled; and storing broadcast authorization codes in authorization database 532;

Petitioner Exhibit 1002-1093

- encryption/decryption module 518 for: encrypting the authorization code with an encryption/decryption key that corresponds to the payment module 124; and decrypting the authorization grant token with the encryption/decryption key;
- transaction sniffing module 520 for: detecting signals associated with hard currency transactions and/or other cashless transactions not associated with the payment processing system 100 (e.g., credit card transactions); and storing information associated with said hard currency transactions and/or other cashless transactions (e.g., in the other information database 536);
- validating module 522 for validating a transaction by checking the authorization code from the decrypted authorization grant token against previously broadcast authorization codes stored in the authorization database 532;
- transaction processing module 524 for: causing, in accordance with a determination that the transaction is validated, the automatic retail machine 122 to vend a product or perform a service; and storing transaction detail information in the transaction database 534; and
- acknowledgement module 526 for deleting transaction detail information from the transaction database 534 in accordance with a determination that the corresponding transaction is acknowledged by the server system 108; and

* data 530 storing data, including but not limited to:
  - authorization database 532 storing previously broadcast authorization codes;
  - transaction database 534 storing transaction detail information for transactions processed by the payment module 124; and
  - other information database 536 storing miscellaneous information regarding the payment module 124 and/or the automatic retail machine 122 coupled with the payment module 124 such as status flags, inventory information, past hard currency transaction information, other cashless transaction information, and/or the like.

[0062] Each of the above identified elements may be stored in one or more of the previously mentioned memory devices, and corresponds to a set of instructions for

Petitioner Exhibit 1002-1094

performing a function described above. The above identified modules or programs (i.e., sets of instructions) need not be implemented as separate software programs, procedures, or modules, and thus various subsets of these modules may be combined or otherwise re-arranged in various implementations. In some implementations, the memory 506, optionally, stores a subset of the modules and data structures identified above. Furthermore, the memory 506, optionally, stores additional modules and data structures not described above.

[0063] Figures 6A-6C show various views of the payment module 124 of Figure 5 in accordance with some implementations. The payment module 124 is a relatively low cost hardware component that is pre-configured to work with the industry standard multi-drop bus (MDB). On machines without MDB technology, the payment module 124 can be configured or designed to work with other serial protocols or activate a switch (e.g., a cherry switch mechanism). For example, see U.S. Patent Application No. 14/458,192, entitled "Method and System for Retrofitting an Offline-Payment Operated Machine to Accept Electronic Payments," which is incorporated by reference in its entirety. In essence, the payment module 124 simulates establishing payment on the automatic retail machine 122 in much the same manner as other alternative forms of payment (e.g., cash).

[0064] The payment module 124 is preferably designed to be used as an adapter dongle for in-line insertion within, for example, the MDB of the automatic retail machine 122 (e.g., a vending machine). The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the MDB with connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g., a coin mechanism). The MDB male and female adapters 612, 614 of the MDB may be separated (as shown in Figures 6B-6C). The payment module 124 in Figures 6A-6C has a male adapter 602 and a female adapter 604. The payment module 124 may be plugged (inserted) in serial ("in-line") with the MDB. For example, the MDB female adapter 614 may be connected to the male adapter 602 of the payment module 124, and the MDB male adapter 612 may be connected to the female adapter 604 of the payment module 124. The resulting in-line configuration is shown in Figure 7. It should be noted that the payment module 124 is designed to allow pass-through communications so that if the mobile-device-to-machine payment processing system is not enabled (e.g., for a particular purchase or simply turned off) the MDB functions as though the payment module 124 is not there and the automatic retail machine 122 can function normally.

Petitioner Exhibit 1002-1095

In Figure 7, the automatic retail machine 122 includes a display 722 showing user selections, current credit, and the like. In Figure 7, the automatic retail machine 122 also includes a touch-screen display 724 and buttons 726 for selecting a product.

USER INTERFACES AND RELATED PROCESSES

[0065] Figure 8 is a schematic flow diagram of a process 800 for authenticating a user to perform a transaction in the payment processing system 100 in accordance with some implementations. In some implementations, the payment processing system 100 includes one or more payment modules 124 (e.g., each associated with a respective automatic retail machine 122 such a vending machine for dispensing goods and/or services), one or more mobile devices 104, and the server 108. Each of the one or more mobile devices 104 executes an instance of the client-side module 102 (e.g., as an application) as a foreground or background process to access and communicate with other devices (e.g., the server 108 and the payment modules 124) in the payment processing system 100. The server 108 manages the payment processing system 100 and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the one or more payment modules 124. For brevity, the process 800 will be described with respect to a respective payment module 124 and a respective mobile device 104 within the payment processing system 100.

[0066] The payment module 124 broadcasts (802), via a short-range communication capability (e.g., BLE), an information packet. The information packet at least includes an authorization code and a unique identifier associated with the payment module 124 (i.e., the device ID). In some implementations, the information packet further includes a current firmware version of the payment module 124 and one or more status flags corresponding to one or more states of the payment module 124 and/or the automatic retail machine 122. The information packet is further discussed below with reference to Figure 10A.

[0067] In some implementations, the payment module 124 sends out a unique authorization code every X seconds (e.g., 100 ms, 200 ms, 500 ms, etc.). In some implementations, the unique authorization codes are randomly or pseudo-randomly generated numbers. In some implementations, the payment module 124 initializes a random number and then the authorization codes are sequential counts from this random number. In such implementations, the payment module 124 stores the earliest valid (unexpired) counter without a need to store every valid authorization code. In some implementations, the

Petitioner Exhibit 1002-1096

authentication code included in the broadcast information packet is a hash value of the randomly or pseudo-randomly generated number or the sequential number.

[0068] In some implementations, the payment module 124 stores broadcast authorization codes (e.g., in authorization database 542, Figure 5) until a received authorization grant token matches one of the stored authorization codes and subsequently deletes the matching authorization code. In some implementations, the broadcast authorization codes are one-time use codes whereby a broadcast authorization code may only be used by one mobile device 104 before it is invalidated and/or deleted to prevent re-play attacks. In some implementations, the payment module 124 stores previously broadcast authorization codes for a predetermined amount of time (e.g., Y minutes) after which time an authorization code expires and is deleted. In some implementations, the authorization code is encrypted with a shared secret key known by the server system 108 but unique to the payment module 124.

[0069] The mobile device 104 receives the broadcast information packet, and the mobile device 104 sends (804), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization request to the server system 108. For example, an application associated with the client-side module 102 is executed as a foreground or background process on the mobile device 104. The application is used for accessing the payment processing system 100. In this example, the application receives the broadcast information packet when the mobile device 104 is within the communication zone of the payment module 124 (i.e., BLE range) and either automatically sends the authorization request to the server system 108 or sends the authorization request to the server system 108 when the mobile device 104 is within the authorization zone of the payment module 124.

[0070] In some implementations, the broadcast information packet includes a baseline authorization zone threshold (i.e., an authorization zone criterion) indicating a baseline received signal strength indication (RSSI) that the mobile device 104 (or the application associated with the client-side module 102) is required to observe from the payment module 124 before being within the authorization zone of the payment module 124. In some implementations, the mobile device 104 (or the application associated with the client-side module 102) offsets the baseline authorization zone threshold based on the reception strength its short-range communication capability (e.g., BLE radio/transceiver) and/or other similar factors. In some implementations, the authorization request at least includes the authorization

Petitioner Exhibit 1002-1097

code which was included in the broadcast information packet, an identifier associated with the user of the mobile device 104 or the user account under which the user of the mobile device 104 is logged into the application (i.e., user ID), and the identifier associated with the payment module 124 (i.e., device ID). In some implementations, the authentication code included in the authorization request is a hash value in cleartext. The authorization request is further discussed below with reference to Figure 10B.

[0071] After receiving the authorization request, the server system 108 processes (806) the authorization request. In some implementations, the server system 108 identifies a shared secret key based on the device ID and decrypts the authorization code included in the authorization request with the identified shared secret key. The server system 108 determines whether the user associated with the user ID in the authorization request has sufficient funds in his/her account for the payment processing system to perform a transaction at the automatic retail machine 122 to which the payment module 124 corresponding to the device ID is coupled.

[0072] The server system 108 sends (808), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization grant token to the mobile device 104. In some implementations, the server system 108 does not send the authorization grant token if the authorization code in the authorization request cannot be decrypted with the shared secret key corresponding to the payment module 124 (e.g., the authorization code is corrupted or hacked). In some implementations, the server system 108 does not send the authorization grant token if the user associated with the user ID in the authorization request does not have sufficient funds in his/her account or has exceeded a predefined daily limit. In some implementations, in addition to the authorization grant token (or lack thereof if the authorization is declined), the server system 108 sends a message directly to the mobile device 104 which is not encrypted with the shared secret key corresponding to the payment module 124. After receiving the message, the mobile device 104 displays an appropriate message to the user such as sufficient funds, transaction authorized, insufficient balance, or declined authorization. In some implementations, the server system 108 sends an authorization grant token for an amount equal to zero; in which case, the payment module 124 interprets this as a declined or failed authorization which can result for any number of reasons including, but not limited to, insufficient balance or credit. In some implementations,

Petitioner Exhibit 1002-1098

the mobile device 104 stores the authorization grant token (e.g., in the user data 264) until a trigger condition is detected.

[0073] The mobile device 104 receives the authorization grant token, and, subsequently, the mobile device 104 detects (810) a trigger condition. In some implementations, the mobile device 104 (or the application) detects the trigger condition via the hand-free mode (e.g., upon entrance into the payment zone of the payment module 124) or manual mode (e.g., interacting with the user interface of the application to initiate a transaction with the payment accepting unit associated with the payment module 124).

[0074] In some implementations, the trigger condition is satisfied when the mobile device 104 detects a user input on the user interface displayed by the mobile device 104. For example, with reference to Figure 11A, a transaction is initiated between the user of the mobile device 104 and the 8th floor snack machine when the mobile device 104 detects an upward swipe gesture originating from region 1120 of the user interface 1108. In another example, with reference to Figure 11D, a transaction is initiated between the user of the mobile device 104 and the 8th floor snack machine when the mobile device 104 detects selection of Offer A 1152 with contact 1166.

[0075] In some implementations, the trigger condition is satisfied when the mobile device 104 observes an RSSI from a respective automatic retail machine that is greater than or equal to the payment zone criterion. For example, once the mobile device 104 is within the payment zone, a transaction between the respective automatic retail machine and the user of the mobile device 104 is automatically initiated. In some implementations, after the RSSI observed from the respective retail machine is greater than or equal to the payment zone criterion, the mobile device 104 prompts the user to provide a transaction confirmation, which when detected serves to satisfy the trigger condition. For example, once the mobile device 104 is within the payment zone, the mobile device 104 provides a prompts to the user, such as an audible prompt, displayed notification, or vibration, to confirm his/her intention to initiate a transaction with the respective retail machine. Continuing with this example, the user may confirm his/her intention to initiate the transaction with the respective retail machine by flicking the mobile device 104 towards the automatic retail machine, shaking the mobile device, providing an audible command, or performing a touch input/gesture on the displayed user interface.

Petitioner Exhibit 1002-1099

[0076] In some implementations, unused authorization grants (e.g., if there was no trigger condition or it expired) are canceled by the mobile device 104 by sending a cancellation message to the server system 108 corresponding to the unused authorization grant. In some implementations, the server system 108 denies or limits the number of authorization grants sent to the mobile device 104 until it has received transaction information or cancellation of authorization outstanding authorization grants sent to the mobile device 104.

[0077] In response to detecting the trigger condition, the mobile device 104 sends (812), via the short-range communication capability (e.g., BLE), the authorization grant token to the payment module 124. Subsequently, the automatic retail machine 122 displays credit to the user (e.g., via one of the displays 722 or 724 shown in Figure 7) and the user interacts with the input mechanisms of the automatic retail machine 122 (e.g., via the buttons 726 or a touch screen display 724 shown in Figure 7) to purchase products and/or services.

[0078] It should be understood that the particular order in which the process in Figure 8 has been described is merely exemplary and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods and/or processes described herein (e.g., the process 900 and the method 1200) are also applicable in an analogous manner to the process 800 described above with respect to Figure 8.

[0079] Figure 9 is a schematic flow diagram of a process 900 for processing acknowledgment information in the payment processing system 100 in accordance with some implementations. In some implementations, the payment processing system 100 includes one or more payment modules 124 (e.g., each associated with a respective automatic retail machine 122 such a vending machine for dispensing goods and/or services), one or more mobile devices 104, and the server 108. Each of the one or more mobile devices 104 executes an instance of the client-side module 102 (e.g., as an application) as a foreground or background process to access and communicate with other devices (e.g., the server 108 and the payment modules 124) in the payment processing system 100. The server 108 manages the payment processing system 100 and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the one or more payment modules 124. For brevity,

Petitioner Exhibit 1002-1100

the process 900 will be described with respect to a respective payment module 124 coupled with a respective automatic retail machine 122 and a respective mobile device 104 in the payment processing system 100. In the process 900, the payment module 124 receives first acknowledgment information for a first transaction via the mobile device 104 that initiated the first transaction.

[0080] The payment module 124 obtains (902) a first notification indicating completion of a first transaction from the automatic retail machine 122. For example, after the process 800 in Figure 8, the user of the mobile device 104 selects a product to purchase from the automatic retail machine 122 by interacting with one or more input mechanisms of the automatic retail machine 122 (e.g., he buttons 726 or a touch screen display 724 shown in Figure 7), and the automatic retail machine 122 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 124 obtains a notification from the machine of the completed transaction. In some implementations, the notification includes the amount of the transaction and (optionally) machine status information associated with the automatic retail machine 122 such as inventory information as to one or more products of the automatic retail machine 122 and/or the like.

[0081] After obtaining the first notification, the payment module 124 generates (904) first transaction information based on the first notification, and the payment module 124 stores the first transaction information. In some implementations, the transaction information includes a transaction ID for the first transaction, a device ID corresponding to the payment module 124, a user ID corresponding to the mobile device 104, transaction status information indicating that the first transaction is complete, and the transaction amount indicated by the first notification. In some implementations, the payment module 124 retains the authorization code included in the original broadcasted packet and/or the authorization grant token and includes the authorization code in the first transaction information. In some implementations, the authorization code is encrypted with a secret key corresponding to the payment module 124, which is shared with the server system 108 but not the mobile device 104. In some implementations, the first transaction information further includes other information such as the machine status information included in the first notification or transaction information corresponding to previous interrupted transaction(s). See Figure 10D and the accompanying text for further discussion regarding the transaction information 1050.

Petitioner Exhibit 1002-1101

[0082] The payment module 124 sends (906), via a short-range communication capability (e.g., BLE), the first transaction information to the mobile device 104.

[0083] The mobile device 104 sends (908), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), the first transaction information to the server system 108.

[0084] The server system 108 processes (910) the first transaction information. For example, the server system 108 debits the account of the user associated with the user ID in the first transaction information in the amount indicated by the first transaction information.

[0085] The server system 108 sends (912), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), first acknowledgment information to the mobile device 104. In some implementations, the first acknowledgment information acknowledges that the server system 108 received the first transaction information. In some implementations, the first acknowledgment information includes the user ID, the device ID, the transaction ID, and (optionally) the authorization grant included in the transaction information (e.g., the authorization code 1058, Figure 10D).

[0086] After receiving the first acknowledgement information, the mobile device 104 sends (914), via a short-range communication capability (e.g., BLE), the first acknowledgment information to the payment module 124.

[0087] After receiving the first acknowledgment information, the payment module 124 deletes (916) the stored first transaction information.

[0088] It should be understood that the particular order in which the process in Figure 9 has been described is merely exemplary and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods and/or processes described herein (e.g., the process 800 and the method 1200) are also applicable in an analogous manner to the process 900 described above with respect to Figure 9.

[0089] Figure 10A is a block diagram of an information packet 1000 broadcast by the payment module 124 (e.g., in step 802 of the process 800 in Figure 8) in accordance with

Petitioner Exhibit 1002-1102

some implementations. In some implementations, the information packet 1000 at least includes: device ID 1002 and authorization code 1004. In some implementations, the information packet 1000 additionally includes: a current firmware version 1006; one or more status flags 1008; and zone criteria information 1010.

[0090] In some implementations, the device ID 1002 is a unique identifier corresponding to the payment module 124 that broadcast the information packet 1000.

[0091] In some implementations, the authorization code 1004 is a hash value in cleartext. In some implementations, the payment module 124 randomly or pseudo-randomly generates a number or determines a sequential number (*See* step 802 of the process 800 in Figure 8) and performs a predetermined hash function (e.g., SHA-256) on the number to produce the hash value as the authorization code 1004. In some implementations, the authorization code 1004 is a unique code that is encrypted with a secret encryption key corresponding to the payment module 124. The secret encryption key is shared with the server system 108, which enables the server system 108 to decrypt the authorization code 1004 and encrypt the authorization grant token but not the mobile device 104. In some implementations, the encryption between server system 108 and payment module 124 is accomplished by two pairs of public/private keys.

[0092] In some implementations, the firmware version information 1006 identifies a current firmware version 1012 of the payment module 124. In some implementations, the firmware version information 1006 also includes update status information 1014 indicating one or more packets received by the payment module 124 to update the firmware or one or more packets needed by the payment module 124 to update the firmware.

[0093] In some implementations, the one or more status flags 1008 indicate a state of the payment module 124 and/or the automatic retail machine 122 to which the payment module 124 is coupled. In some implementations, the one or more status flags 1008 indicate a state of the payment module 124 such upload information indicator 1016 indicating that that the payment module 124 has information to be uploaded to the server system 108 (e.g., transaction information for one or more interrupted transactions). In some implementations, upload information indicator 1016 triggers the mobile device 104 to connect to payment module 124 immediately (e.g., if it has interrupted transaction information to be uploaded to the server system 108). In some implementations, the one or more status flags 1008 indicate a

Petitioner Exhibit 1002-1103

state of the automatic retail machine 122 including one or more of an error indicator 1018 (e.g., indicating that a bill and/or coin acceptor of the automatic retail machine 122 is experiencing a jam, error code, or malfunction), a currency level indicator 1020 (e.g., indicating that the level of the bill and/or coin acceptor reservoir of the automatic retail machine 122 is full or empty), and/or inventory level(s) indicator 1022 (e.g., indicating that one or more products of the automatic retail machine 122). In some implementations, the one or more status flags 1008 are error codes issued by the automatic retail machine 122 over the MDB.

[0094] In some implementations, the zone criteria information 1010 specifies an authorization zone criterion 1024 (e.g., a baseline authorization zone threshold indicating a baseline RSSI that the mobile device 104 (or the application) is required to observe before being within the authorization zone of the payment module 124) and/or a payment zone criterion 1026 (e.g., a baseline payment zone threshold indicating a baseline RSSI that the mobile device 104 (or the application) is required to observe before being within the payment zone of the payment module 124). In some implementations, the baseline authorization zone threshold and the baseline payment zone threshold are default values determined by the server system 108 or stored as variables by the application, in which case the authorization zone criterion 1024 and payment zone criterion 1026 are offsets to compensate for the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the payment module 124. Alternatively, zone criteria information 1010 includes a spread between the baseline authorization zone threshold and the baseline payment zone threshold. Thus, the mobile device 104 (or the application) determines the baseline authorization zone threshold and the baseline payment zone threshold based on the spread value and a default value for either the baseline authorization zone threshold or the baseline payment zone threshold. For example, the spread indicates -10 db and the default baseline payment zone threshold is -90 db; thus, the baseline authorization zone threshold is -80 db. Continuing with this example, after determining the baseline authorization zone threshold and the baseline payment zone threshold, the mobile device 104 (or the application) may further adjust the authorization zone threshold and/or the payment zone threshold based on the strength and/or reception of its short-range communication capability (i.e., BLE radio/transceiver).

Petitioner Exhibit 1002-1104

[0095] Figure 10B is a block diagram of an authorization request 1030 sent by the mobile device 104 to the system server 108 (e.g., in step 804 of the process 800 in Figure 8) in accordance with some implementations. In some implementations, the authorization request 1030 at least includes: a device ID 1002; a user ID 1034; and an authorization code 1004.

[0096] In some implementations, the device ID 1002 is a unique identifier corresponding to the payment module 124 that broadcast the information packet 1000 that included the authorization code 1004.

[0097] In some implementations, the user ID 1034 is a unique identifier associated with the user of the mobile device 104 sending the authorization request 1030 to the server system 108. In some implementations, the user ID 1034 is associated with the user account under which the user of the mobile device 104 is logged into the application.

[0098] In some implementations, the authorization code 1030 is the authorization code 1004 included in the information packet 1000 of that was broadcast by the payment module 124.

[0099] Figure 10C is a block diagram of an authorization grant token 1040 sent by the server system 108 to the mobile device 104 (e.g., in step 808 of the process 800 in Figure 8) in accordance with some implementations. In some implementations, in accordance with a determination that the authorization code 1036 included in the authorization request 1030 from the mobile device 104 is valid and that the user associated with the mobile device 104 has sufficient funds in his/her account for the payment processing system, the server system 108 generates the authorization grant token 1040. In some implementations, the authorization grant token 1040 at least includes: a device ID 1002; a user ID 1034; an authorized amount 1046; (optionally) an expiration period 1048; and (optionally) the authorization code 1004. In some implementations, the authorization grant token 1040 is encrypted with the shared secret key corresponding to the payment module 124.

[00100] In some implementations, the device ID 1002 is a unique identifier corresponding to the payment module 124 that broadcast the information packet 1000 that included the authorization code 1004.

Petitioner Exhibit 1002-1105

[00101] In some implementations, the user ID 1034 is a unique identifier associated with the user of the mobile device 104 that sent the authorization request 1030 to the server system 108.

[00102] In some implementations, the authorized amount 1046 indicates a maximum amount for which the user of the mobile device 104 is authorized to perform transaction(s) using the authorization grant token 1140. For example, the authorized amount 1046 is predefined by the user of the mobile device 104 or by the server system 108 based on a daily limit or based on the user's total account balance or based on a risk profile of the user associated with the user ID 1034.

[00103] In some implementations, the expiration period 1048 indicates an offset to the amount of time that the payment module 124 holds the authorization grant token 1040 valid for initiation of a transaction with the automatic retail machine 122 associated with the payment module 124. For example, the expiration period 1048 depends on the history and credit of the user of the mobile device 104 or a period predefined by the user of the mobile device 104.

[00104] In some implementations, the authorization grant token 1040 further includes the authorization code 1004 that was included in the authorization request 1030. In some implementations, when the authorization code 1004 is the hash value, the server system 108 encrypts the authorization grant token 1040 including the hashed value with the shared secret encryption key associated with the payment module 124. Subsequently, when the mobile device 104 sends the authorization grant token 1040 to the payment module 124 after detecting a trigger condition, the payment module 124 decrypts the authorization grant token 1040 using the secret key known only to the server system 108 and the payment module 124 (which authenticates the message and the authorization grant), and then matches the hash value included in the decrypted authorization grant token 1040 to previously broadcast valid (i.e., unexpired and un-used) hash values (e.g., stored authorization codes) to determine the validity of the hash value (which was known only by the payment module 124).

[00105] Figure 10D is a block diagram of transaction information 1050 generated by the payment module 124 (e.g., in step 904 of the process 900 in Figure 9) in accordance with some implementations. In some implementations, the transaction information 1050 includes: a transaction ID 1052 for the respective transaction; a device ID 1054; a user ID 1056;

Petitioner Exhibit 1002-1106

(optionally) the authorization code 1058; transaction status information 1060; the transaction detail information 1062; and miscellaneous information 1064. In some implementations, the transaction information 1050 is encrypted with the shared secret key corresponding to the payment module 124.

[00106] In some implementations, the transaction ID 1052 is a unique identifier corresponding to the respective transaction. In some implementations, the transaction ID 1052 is encoded based on or associated with the time and/or date on which and the location at which the respective transaction took place.

[00107] In some implementations, the device ID 1054 is a unique identifier corresponding to the payment module 124 that performed the respective transaction.

[00108] In some implementations, the user ID 1056 is an identifier associated with the user of the mobile device 104 that initiated the respective transaction.

[00109] In some implementations, the authorization code 1058 corresponds to the original authorization code (e.g., the auth code 1004, Figures 10A-10C) and/or authorization grant token (e.g., the auth grant token 1040, Figure 10C) that was used to initiate the respective transaction. In some implementations, the authorization code 1056 is encrypted with a unique encryption key corresponding to the payment module 124.

[00110] In some implementations, the transaction status information 1060 includes an indication whether the respective transaction was completed, not-completed, or aborted. For example, the respective transaction is incomplete if a jam occurred at the automatic retail machine 122 and the user did not receive the product associated with the respective transaction. For example, if the user walks away from the automatic retail machine 122 after money was credited for the respective transaction, the respective transaction is aborted. In another example, if respective transaction times out after a predetermined time period because the user failed to select a product at the automatic retail machine 122, the respective transaction is aborted. In another example, if the user actuates a bill or coin return mechanism of the automatic retail machine 122, the respective transaction is aborted.

[00111] In some implementations, the transaction detail information 1062 indicates the amount of the respective transaction or the amount of each of multiple transactions (e.g., in a multi-vend scenario). In some implementations, the transaction detail information 1062 also

Petitioner Exhibit 1002-1107

indicates other information related to the respective transaction such as the items dispensed by the automatic retail machine 122 and the type of transaction (e.g., coins, bills, credit card, manual mode, hands-free mode, etc.).

[00112] In some implementations, the miscellaneous information 1064 includes other information related to the payment module 124 and/or the automatic retail machine 122 to which the payment module 124 is coupled. For example, the miscellaneous information 1064 includes a verification request to the server system 108 in order to implement new firmware. In another example, the miscellaneous information 1064 includes transaction information from one or more previous interrupted transactions. In another example, the miscellaneous information 1064 includes transaction information for one or more past hard currency transactions and/or other cashless transactions (e.g., paid with a credit card or bank card at the automatic retail machine 122). In another example, the miscellaneous information 1064 includes inventory information as to one or more products of the automatic retail machine 122.

[00113] Attention is now directed towards implementations of user interfaces ("UIs") and associated processes that may be implemented on a mobile device 104 with zero or more speakers 1102, zero or more microphones 1104, and a display 1106. For example, the display 1106 is a touch screen (sometimes also herein called a "touch screen display") enabled to receive one or more contacts and display information (e.g., media content, websites and web pages thereof, and/or user interfaces for application(s) 326). Figures 11A-11G illustrate exemplary user interfaces for facilitating displaying promotional offers in accordance with some implementations.

[00114] Although some of the examples that follow will be given with reference to inputs on a touch screen (where the touch sensitive surface and the display are combined), in some implementations, the device detects inputs on a touch-sensitive surface that is separate from the display. In some implementations, the touch sensitive surface has a primary axis that corresponds to a primary axis on the display. In accordance with these implementations, the device detects contacts with the touch-sensitive surface at locations that correspond to respective locations on the display. In this way, user inputs detected by the device on the touch-sensitive surface are used by the device to manipulate the user interface on the display of the device when the touch-sensitive surface is separate from the display. It should be

Petitioner Exhibit 1002-1108

understood that similar methods are, optionally, used for other user interfaces described herein.

[00115] Additionally, while the following examples are given primarily with reference to contacts (e.g., finger inputs such as finger contacts, finger tap gestures, finger swipe gestures, etc.), it should be understood that, in some implementations, one or more of the contacts are replaced with input from another input device (e.g., a mouse-based, stylus-based, or physical button-based input). For example, a swipe gesture is, optionally, replaced with a mouse click (e.g., instead of a contact) followed by movement of the cursor along the path of the swipe (e.g., instead of movement of the contact). As another example, a tap gesture is, optionally, replaced with a mouse click while the cursor is located over the location of the tap gesture (e.g., instead of detection of the contact followed by ceasing to detect the contact) or depression of a physical button. Similarly, when multiple user inputs are simultaneously detected, it should be understood that multiple computer mice are, optionally, used simultaneously, or a mouse and finger contacts are, optionally, used simultaneously.

[00116] Figures 11A-11G show user interface 1108 displayed on respective mobile device 104 (e.g., a mobile phone associated with a user) for an application associated with the payment processing system 100; however, one skilled in the art will appreciate that the user interfaces shown in Figures 11A-11G may be implemented on other similar computing devices. The user interfaces in Figures 11A-11G are used to illustrate the processes described herein, including the method described with respect to Figures 12A-12C. One of ordinary skill in the art will appreciate that the following user interfaces are merely examples. Moreover, one of ordinary skill in the art will appreciate that additional affordances and/or user interface elements, or that fewer affordances and/or user interface elements may be used in practice.

[00117] Figure 11A illustrates the mobile device 104 displaying a transaction initiation screen 1110 for 8th floor snack machine. In Figure 11A, the transaction initiation screen 1110 includes a sequence of indicators 1116 showing that 8th floor snack machine is one of three automatic retail machines with which the user is authorized to initiate a transaction. For example, the user of the mobile device 104 is able to access the second of the three automatic retail machines by performing a left-to-right swipe gesture on the user interface 1108 (or alternatively a right-to-left swipe gesture) and the first second the three automatic retail machines by performing a right-to-left swipe gesture on the user interface 1108 (or

Petitioner Exhibit 1002-1109

alternatively a left-to-right swipe gesture). The user of the mobile device 104 is able to access settings and/or a home screen of the application by selecting affordance 1112 (e.g., with a tap gesture), and the user of the mobile device 104 is able to refresh the transaction initiation screen 1110 by selecting affordance 1114 (e.g., with a tap gesture).

[00118] Figure 11A also shows that the user of the mobile device 104 has a prepaid balance of $100.00. The user of the mobile device 104 is able to initiate a transaction with the 8th floor snack machine by performing an upward swipe gesture originating from region 1120 of the transaction initiation screen 1110. The user of the mobile device 104 is able to access special promotional offers by selecting "Special Offers" region 1122 (e.g., with a tap gesture), and the user of the mobile device 104 is able to "like" or favorite the 8th floor snack machine by selecting affordance 1124 (e.g., with a tap gesture). Figure 11A also illustrates the mobile device 104 detecting contact 1140 at a location corresponding to "Special Offers" region 1122.

[00119] Figure 11B illustrates the mobile device 104 displaying a special offers screen 1130 for the 8th floor snack machine. In Figure 11B, the special offers screen 1130 includes: a first region that corresponds to "Offer A" 1152 on product A accompanied by image A of product A; a second region that corresponds to "Offer B" 1154 on product A accompanied by image A of product A; and a third region that corresponds to "Offer C" 1156 on product B accompanied by image B of product B. The special offers screen 1130 also includes refresh affordance 1151, which, when activated (e.g., via a tap gesture), causes the special offers screen 1130 to be refreshed. In Figure 11B, none of Offers A, B, C are currently selected. The user of the mobile device 104 is able to select "Offer A" 1152 by performing a gesture (e.g., a tap gesture) on selection affordance 1153. Similarly, the user of the mobile device 104 is able to select "Offer B" 1154 by performing a gesture (e.g., a tap gesture) on selection affordance 1155 or "Offer C" 1156 by performing a gesture (e.g., a tap gesture) on selection affordance 1157. The user of the mobile device 104 is also able to dismiss or delete any of Offers A, B, or C by performing a right-to-left swipe gesture (or a left-to right swipe gesture in other implementations) in a corresponding region. Figure 11B also illustrates the mobile device 104 detecting a right-to-left swipe gesture within the second region corresponding to "Offer B" 1154 with contact 1160 moving from a first location 1162-a to a second location 1162-b.

[00120] In some implementations, the special offers screen 1130 further includes a fourth region corresponding to "No Selected Offer." For example, the user of the mobile

Petitioner Exhibit 1002-1110

device 104 may view the promotional offers on the special offers screen 1130 but not wish to apply any of them to a future transaction with the 8th floor snack machine. As such, the user of the mobile device 104 may select the "No Selected Offer" region (e.g., with a tap gesture), and, in response, the mobile device 104 re-displays the transaction initiation screen 1110 as shown in Figure 11A.

[00121] Figure 11C illustrates the mobile device 104 displaying delete affordance 1164 within the second region corresponding to "Offer B" 1154 in response to detecting the right-to-left swipe gesture in Figure 11B. The delete affordance 1164, when activated, (e.g., via a tap gesture), causes "Offer B" 1154 to be deleted from the special offers screen 1130. Figure 11C also illustrates mobile device 104 detecting contact 1166 at a location corresponding to delete affordance 1164.

[00122] Figure 11D illustrates the mobile device 104 ceasing to display "Offer B" 1154 within the special offers screen 1130 in response to detecting selection of delete affordance 1164 in Figure 11C. Figure 11D also illustrates mobile device 104 detecting contact 1168 at a location corresponding to selection affordance 1153 for "Offer A" 1152. Alternatively, in some implementations, the user of the mobile device may not wish to apply any of the offers to a future transaction with the 8th floor snack machine. As such, the user may select the affordance 1112 (e.g., with a tap gesture) or perform a predefined gesture on the special offers screen 1130 to re-display the transaction initiation screen 1110 as shown in Figure 11A.

[00123] Figure 11E shows that selection affordance 1153 is selected in response to detecting selection of selection affordance 1153 in Figure 11D. In some implementations, a transaction with the 8th floor snack machine is automatically initiated in response to detecting selection of selection affordance 1153 in Figure 11D. In other implementations, after detecting selection of selection affordance 1153 in Figure 11D, the mobile device 104 re-displays the transaction initiation screen 1110 (as shown in Figure 11A) and the transaction with the 8th floor snack machine is initiated in response to detecting upward swipe gesture originating from region 1120 of the transaction initiation screen 1110.

[00124] Figure 11F illustrates the mobile device 104 displaying a product code screen 1170, which prompts the user of the mobile device 104 to obtain the product code (e.g., UPC code, SKU, or the like) for product A so as to validate Offer A" 1152 selected in Figure 11D.

Petitioner Exhibit 1002-1111

The product code screen 1170 also includes a product code scanner window 1172 for capturing an image of product A and/or scanning the product code of product A. In Figure 11F, UPC code 1174 (e.g., the product code) of product A (e.g., a candy bar), which is in the field of view of a camera of the mobile device 104, is shown within the product code scanner window 1172. For example, the user of the mobile device 104 is able to capture the image of product A (including the UPC code 1174 within the current field of view) or scan the UPC code 1174 by tapping within product code scanner window 1172, issuing an audible command, depressing a predetermined physical button of the mobile device 104, or the like. Figure 11F also shows that the user of the mobile device 104 has a prepaid balance of $99.00, which is $1.00 less than the amount shown in Figures 11A-11E due to purchase of product A.

[00125] Figure 11G illustrates the mobile device 104 displaying an offer validation screen 1180. In some implementations, the mobile device 104 displays the offer validation screen 1180 after the user completes the transaction with the 8th floor snack machine and the server validates the product code information (e.g., the UPC scanned in Figure 11F). In Figure 11G, the offer validation screen 1180 indicates that the "Offer A" 1152 was validated and that the user's balance was credited $0.25. Figure 11G also shows that the user of the mobile device 104 has a prepaid balance of $99.25, which is $0.25 more than the amount shown in Figure 11G due to validation of the "Offer A" 1152 and a credit of $0.25 for the "Offer A" 1152.

[00126] Figures 12A-12C illustrate a flowchart diagram of a method 1200 of providing and handling promotional offers for an automatic retail machine in accordance with some implementations. In some implementations, method 1200 is performed by a mobile device with a display, one or more processors, and memory. For example, in some implementations, method 1200 is performed by mobile device 104 (Figures 1-2) or a component thereof (e.g., the client-side module 102, Figures 1-2). In some implementations, method 1200 is governed by instructions that are stored in a non-transitory computer readable storage medium and the instructions are executed by one or more processors of the mobile device. Some operations in the method 1200 are, optionally, combined and/or the order of some operations is, optionally, changed.

[00127] In some implementations, the payment processing system 100 (Figure 1) includes the mobile device 104, which performs the method 1200, a server system 108, and a payment module 124 coupled with an automatic retail machine 122. An instance of the client-

Petitioner Exhibit 1002-1112

side module 102 (e.g., as an application) is executed on the mobile device 104 as a foreground or background process to access and communicate with other devices (e.g., the server 108 and the payment module 124) in the payment processing system 100. The server 108 manages the payment processing system 100 and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the payment module 124.

[00128] In some implementations, prior to displaying the one or more promotional offers, the mobile device (1202): obtains an information packet broadcast by a payment module coupled with a automatic retail machine, where the information packet at least includes an authorization code and a unique identifier corresponding to the payment module; send a transaction authorization request to a server, where the transaction authorization includes the authorization code and the unique identifier corresponding to the payment module; and, in response to the transaction authorization request, receive authorization information from the server that includes an authorization grant token for initiating a transaction with the automatic retail machine coupled with the payment module and the one or more promotional offers from the server. As discussed in the process 800, the mobile device 104 or a component thereof (e.g., the broadcast obtaining module 230, Figure 2) receives the information packet broadcast by the payment module 124 which at least includes an authorization code and an identifier associated with the payment module 124. Subsequently, the mobile device 104 or a component thereof (e.g., the transaction authorization module 232, Figure 2) sends the authorization code to the server 108 to pre-authorize a transaction with the automatic retail machine 122 to which the payment module 124 is coupled. In accordance with a determination that the server 108 pre-authorizes the potential transaction, the mobile device 104 or a component thereof (e.g., the transaction authorization module 232, Figure 2) receives an authorization grant token for performing a transaction with the automatic retail machine 122. In some implementations, the mobile device 104 stores the authorization grant token (e.g., in user data 265, Figure 2) until a trigger condition for initiating the transaction with the automatic retail machine 122 is detected (e.g., by the trigger detecting module 236, Figure 2). In some implementations, the trigger condition is satisfied when the mobile device 104 detects a user input on the user interface displayed by the mobile device 104. For example, with reference to Figure 11A, a transaction is initiated between the user of the mobile device 104 and the 8th floor snack machine when the mobile device 104 detects an upward swipe gesture originating from region 1120 of the user interface 1108. In another example, with reference to Figure 11D, a transaction is

Petitioner Exhibit 1002-1113

initiated between the user of the mobile device 104 and the 8th floor snack machine when the mobile device 104 detects selection of Offer A 1152 with contact 1166.

[00129] In some implementations, the mobile device further includes (1204) a first transceiver associated with a short-range communication protocol and a second transceiver associated with a long-range communication protocol. The mobile device communicates with the payment module via the first transceiver, and the mobile device communicates with the server via the second transceiver. For example, the short-range communication protocol is BLE, NFC, or the like, and the long-range communication protocol is GSM, CDMA, Wi-Fi, or the like.

[00130] The mobile device displays (1206) one or more promotional offers on the display. In some implementations, the mobile device 104 only displays promotional offers for products which the user has a sufficient balance. For example, a soda costs $2.00 and there is a promotion for $0.50 off, however, the user has a balance of only $1.00. In this example, the mobile device forgoes displaying the promotion for the soda. Figure 11B, for example, shows the mobile device 104 displaying special offers screen 1130 for the 8th floor snack machine. In Figure 11B, the special offers screen 1130 includes: a first region that corresponds to "Offer A" 1152 on product A accompanied by image A of product A; a second region that corresponds to "Offer B" 1154 on product A accompanied by image A of product A; and a third region that corresponds to "Offer C" 1156 on product B accompanied by image B of product B. Alternatively, in some implementations, a respective one of the one or more promotional offers is applied automatically after the user completes a transaction, and the mobile device prompts the user to provide the product code corresponding to the respective promotion. In some implementations, one or more advertisements are displayed in place of the one or more selectable promotional offers.

[00131] In some implementations, one of the one or more promotional offers is a "reward" for a product or service that is not associated with the automatic retail machine 122 (i.e., an out-of-band offer). For example, if the user purchases a particular product, he/she will receive a link via email for a free download (e.g., a song, video, etc.), in-app credit (e.g., $2.00 for purchases within a digital media marketplace or a $2.00 credit for in-app purchases for a game), or the like. This may or may not require validation of product. For example, buy any product now from this machine and get a link to a $1.00 off coupon via email or text for a case of soda from a retail store. In some implementations, the offer might be an "additional

Petitioner Exhibit 1002-1114

sale" this is an out-of-band offer. For example, purchase XYZ Cola now, and get a case of XYZ Cola from a store for only $1.50 with a coupon to be mailed to your email address. In another example, purchase ABC Chips now, and get a special discount offer to buy a cool T-shirt for $5.00. In this example, $5.00 is added to transaction price and the user is sent an email regarding redemption and shipping of the cool the T-shirt.

[00132] In some implementations, the user is able to dismiss or delete offers and the mobile device 104 sends this information to the server 108 for analytics purposes. In one example, Figure 11C shows the mobile device 104 displaying delete affordance 1164 within the second region corresponding to "Offer B" 1154 in response to detecting the right-to-left swipe gesture in Figure 11B. Continuing with this example, Figure 11D shows the mobile device 104 ceasing to display "Offer B" 1154 within the special offers screen 1130 in response to detecting selection of delete affordance 1164 in Figure 11C.

[00133] In some implementations, the one or more promotional offers are identified (1208) based on at least one of: a unique identifier corresponding to the payment module, at least one of the current time and date, a location of the automatic retail machine, a location of the mobile device, and a unique identifier corresponding to the user of the mobile device. In some implementations, the server 108 or a component thereof (e.g., offer determining module 328, Figure 3) determines/identifies the one or more promotional offers based on the current time/date, current location, device ID associated with the payment module, user ID associated with the user of the mobile device, and the like. In some implementations, the mobile device 104 or a component thereof (e.g., the offer(s) module 234, Figure 2) determines/identifies the one or more promotional offers from a pre-stored collection of offers based on the current time/date, current location, device ID associated with the payment module, user ID associated with the user of the mobile device, and the like. For example, the mobile device 104 identifies the one or more promotional offers from the offers database 266 which includes offers sent by the server 108 at a prior time such as a part of an update to the application.

[00134] In some implementations, the promotional offers are identified based on the products stocked in the automatic retail machine 122 or past behavior (e.g., previous offers selected by the user, previous offers deleted by the user, previous offers not selected by the user, etc.). For example, side-by-side are separate snack and soda vending machines. The user buys a soda first. Then, when the user goes to transact with the snack machine, the user is presented with an offer for a particular product (e.g., to enable cross promotions between

Petitioner Exhibit 1002-1115

soda and snack distributors). Alternatively, the offers could be based on what a user did not select from the soda machine or offers that were actively deleted before.

[00135] In some implementations, the provider of the server 108 and payment module 124 manages a promotion marketplace to facilitate placing of promotional offers by manufacturers and distributors of products and to also facilitate competition between various product manufacturers and distributors. For example, a distributor or manufacturer of a product may place a promotional offer for $0.25 off on a particular item in all applicable community colleges in California on Thursdays between 2:00 and 4:00 PM PDT. In another example, a distributor or manufacturer of a product may place a promotional offer for 50% off on the product on the day the product expires (e.g., to sell perishable sandwiches or the like) for all applicable automatic retail machines. In some implementations, cross-promotional offers or complex promotional offers may also be placed whereby a user gets a credit (e.g., a rebate) for purchasing a particular drink and snack combination where each are manufactured or distributed by different entities.

[00136] In some implementations, a promotional offer on all items in automatic retail machines on a entity's campus (essentially a subsidy) is only available to select users. For example, all attorneys and staff at a law firm are given a subsidized rate on snacks but cleaning persons do not benefit from said subsidized rate. In another example, all full-time employees are given a subsidized rate on snacks but temporary workers do not benefit from said subsidized rate.

[00137] In some implementations, variable pricing is enacted whereby the base price of items changes and promotion offers may be added in addition to the variable pricing scheme. For example, a distributer wishes to decrease the price on all items in applicable machines during the off-peak hours (e.g., 9:00 PM – 6:00 AM). Therefore, after a transaction is completed, the server 108 will only charge a user the decreased price, and, after the server processes and accounts for the transaction, transaction acknowledgment information displayed at the mobile device 104 will indicate that the user was only charged the decreased price and not the price shown at the automatic retail machine 122.

[00138] The mobile device detects (1210) a user input selecting a respective promotional offer of the one or more promotional offers. For example, the user input is a touch input, voice input, or the like. Figure 11D, for example, shows the mobile device 104

Petitioner Exhibit 1002-1116

detecting selection of selection affordance 1153 for "Offer A" 1152, and Figure 11E shows that selection affordance 1153 is selected in response to detecting selection of selection affordance 1153 in Figure 11D. In some implementations, the respective promotional offer is a negative one, such as a donation to AIDS research, that adds a selected amount to the user's next transaction. Alternatively, in some implementations, the respective promotional offer is a negative one whereby the transaction is rounded up to the nearest dollar, where additional amount is donated to a Cancer research foundation.

[00139] The mobile device initiates (1212) performance of a transaction with an automatic retail machine coupled with a payment module, where the transaction corresponds to purchase of a product stocked by the automatic retail machine. In some implementations, the transaction is initiated in response to selection of the respective promotional offer (i.e., one-click transaction initiation process). For example, a transaction with the 8th floor snack machine is automatically initiated in response to detecting selection of selection affordance 1153 in Figure 11D. In other implementations, after the user selects an offer the user performs an action to initiate a transaction with the automatic retail machine (i.e., a two-step transaction initiation process). For example, after detecting selection of selection affordance 1153 in Figure 11D, the mobile device 104 re-displays the transaction initiation screen 1110 (as shown in Figure 11A) and the transaction with the 8th floor snack machine is initiated in response to detecting upward swipe gesture originating from region 1120 of the transaction initiation screen 1110.

[00140] In some implementations, performance of the transaction with the automatic retail machine coupled with the payment module is initiated (1214) by sending the authorization grant token to the payment module, where the authorization grant token includes the authorization code included in the broadcast information packet. In some implementations, initiating performance of the transaction includes the mobile device 104 or a component thereof (e.g., the transaction initiating module 238, Figure 2) sending the stored authorization grant token to the payment module 124 for payment and the user manually selects a product using the user interface of the automatic retail machine 122. As such, the automatic retail machine 122 knows nothing about the selected promotional offer – it only knows that the user sent it a payment. For example, the automatic retail machine 122 returns transaction and product information that is passed to the mobile device 104 by the payment module 124 but it cannot determine or state in any way if it is a product that corresponds to

Petitioner Exhibit 1002-1117

the offer. For example, the transaction completion notification indicates "I vended E3 for $1.00".

[00141] The mobile device receives (1216) a transaction completion notification from the payment module, where the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine. In some implementations, the mobile device 104 or a component thereof (e.g., the transaction completion notification receiving module 240, Figure 2) receives transaction completion notification (e.g., the transaction status information, the transaction detail information, the other miscellaneous information regarding the respective payment module 124 and/or the automatic retail machine 122 to which the respective payment module 124 is coupled, and/or the like) from the payment module 124 after the user manually selects a product using the user interface of the automatic retail machine 122. In some implementations, the transaction completion notification includes the good/service associated with the transaction, the current inventory of the automatic retail machine 122, information associated with one or more previous cash transactions, information associated with one or more interrupted transactions handled by the payment module 124, and/or other information associated with the automatic retail machine 122 such as error or maintenance states. In some implementations, the payment module 124 sends an error message in place of the transaction completion notification when the transaction is aborted or an error occurs during the transaction such as unavailability of a requested good/service or a vending jam.

[00142] In response to receiving the transaction completion notification, the mobile device provides (1218) a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer. In some implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) displays a scanning interface for capturing the product code of the vended item after receiving the transaction completion notification. Figure 11F, for example, shows the mobile device 104 displaying a product code screen 1170, which prompts the user of the mobile device 104 to obtain the product code (e.g., UPC code, SKU, or the like) for product A so as to validate Offer A" 1152 selected in Figure 11D. The product code screen 1170 also includes a product code scanner window 1172 for capturing an image of product A and/or scanning the product code of product A. In Figure 11F, the UPC code 1174 of product A (e.g., a candy bar), which is in the field of view of a camera of the mobile device 104, is

Petitioner Exhibit 1002-1118

shown within the product code scanner window 1172. For example, the user of the mobile device 104 is able to capture the image of product A (including the UPC code 1174 within the current field of view) or scan the UPC code 1174 by tapping within product code scanner window 1172, issuing an audible command, depressing a predetermined physical button of the mobile device 104, or the like.

[00143] In other implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) displays a pop-up message or banner notification on the display prompting the user of the mobile device 104 to manually enter or otherwise obtain the product code of the vended item. In other implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) provides an audible tone, a vocal prompt, or a sequence of tactile/haptic vibrations prompting the user of the mobile device 104 to enter or otherwise obtain the product code of the vended item.

[00144] The mobile device obtains (1220) the product code for the vended product. For example, the user enters the barcode character-by-character, scans the barcode, or simply captures an image of the barcode. In some implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) receives the product code.

[00145] In some implementations, obtaining the product code further comprises (1222): capturing an image of the product that includes the product code; and extracting the product code from the captured image. In some implementations, obtaining the product code further comprises (1224): scanning the product code of the product with a scanner unit of the mobile device. For example, the user of the mobile device 104 is able to access a product code capture plug-in from within the application associated with the payment processing system 100 (e.g., the product code processing module 242, Figure 2) which enables the user to capture an image of the product with the product code in the field of view or scan the product code of the product. In this example, the mobile device 104 extracts the product code from the captured image and sends the extracted product code to the server 108 or, alternatively, the mobile device 104 sends the captured image to the server 108 where the product code is extracted. In another example, the user of the mobile device 104 is able to manually enter the product code from within the application (e.g., via a virtual keypad) or via a website associated with the payment processing system 100.

Petitioner Exhibit 1002-1119

[00146] After obtaining the product code, the mobile device transmits (1226) the product code to the server. In response to transmitting the product code, the mobile device: receives promotion validation information from the server; and displays the promotion validation information on the display, where the promotion validation information indicates whether the respective promotion offer was validated. In some implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) either validates the obtained product code or sends the obtained product code to the server 108 for validation. In some implementations, the mobile device 104 or a component thereof (e.g., the information relaying module 244, Figure 2) sends the transaction completion notification or a portion thereof to the server 108 regardless of whether the user follows the prompt and the mobile device 104 ultimately obtains the product code. In some implementations, the server 108 determines whether conditions for the respective promotional offer have been based on the transaction and the product code. For example, the server 108 determines whether the proper product code was obtained for the respective promotional offer, whether the respective promotional offer has expired, whether the user has fulfilled a buy N items get one free condition, whether the user has fulfilled cross-promotion condition, and/or the like. In some implementations, the offer is validated and applied by the server 108 to the user's account.

[00147] In some implementations, the mobile device 104 of a component thereof (e.g., the offer validation module 246, Figure 2) receives and displays the promotion validation information. For example, the promotion validation information indicates whether the offer was validated and an updated user balance/transaction listing. Figure 11G, for example, shows the mobile device 104 displaying an offer validation screen 1180, which indicates that the "Offer A" 1152 was validated and that the user's balance was credited $0.25. Figure 11G also shows that the user of the mobile device 104 has a prepaid balance of $99.25, which is $0.25 more than the amount shown in Figure 11G due to validation of the "Offer A" 1152 and a credit of $0.25 for the "Offer A" 1152. For example, when the user gets a fifth purchased product free and the product that was the subject of the instant transaction was only the first item purchased, the promotion validation information indicates that the user must buy 3 more of the product before he/she gets a free product. In some implementations, the promotion validation information includes a coupon for a product or service that is not associated with the automatic retail machine 122 For example, the user is emailed a coupon for $5 off an amusement park for purchasing a soda.

Petitioner Exhibit 1002-1120

[00148] In some implementations, after obtaining the product code, the mobile device determines (1228) whether a predetermined time period has expired. In accordance with a determination that the time period has expired, the mobile device provides a notification to the user of mobile device indicating that the respective promotional offer has expired. In accordance with a determination that the time period has not expired, the mobile device transmits the product code to the server. In some implementations, the predetermined time period corresponds to the time between (A) initiating performance of the transaction or prompting for the product code, (B) obtaining the product code or some other time period. For example, the mobile device 104 must receive the product code within 5 minutes of the prompt or within 5 minutes of initiation of the transaction. In some implementations, this may occur hours or even days later. In some implementations, a predetermined proximity between a first location where the transaction was initiated and a second location where the product code was obtained is used in addition to or in place of the predetermined time period.

[00149] In some implementations, the application associated with the payment processing system 100 has a coupon plug-in whereby the user of the mobile device 104 is able to scan a coupon after completing a transaction for a product and also scan the product code of the product to get a post hoc rebate for the transaction.

[00150] In some implementations, the promotion validation information indicates (1230) the price of the product after the application of the respective promotional offer. For example, the mobile device 104 displays the total deducted from the user's account or charged to the user's linked bank card after application of the promotional offer to the base purchase price included in the notification completion information. Figure 11G, for example, shows that the user of the mobile device 104 has a prepaid balance of $99.25, which is $0.25 more than the amount shown in Figure 11G due to validation of the "Offer A" 1152 and a credit of $0.25 for the "Offer A" 1152.

[00151] In some implementations, the mobile device transmits (1232) the transaction completion notification to the server. In some implementations, the mobile device 104 or a component thereof (e.g., the information relaying module 244, Figure 2) sends the transaction completion notification (e.g., the transaction status information, the transaction detail information, the other miscellaneous information regarding the respective payment module 124 and/or the automatic retail machine 122 to which the respective payment module 124 is coupled, and/or the like) or a portion thereof to the server 108 prior to sending the product

Petitioner Exhibit 1002-1121

code or along with the product code. In some implementations, the transaction completion notification or a portion thereof is sent to the server 108 regardless of whether the user follows the prompt and the mobile device ultimately obtains the product code.

[00152] It should be understood that the particular order in which the operations in Figures 12A-12C have been described is merely exemplary and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods and/or processes described herein (e.g., the processes 800 and 900) are also applicable in an analogous manner to method 1200 described above with respect to Figures 12A-12C.

[00153] While particular implementations are described above, it will be understood it is not intended to limit the application to these particular implementations. On the contrary, the application includes alternatives, modifications and equivalents that are within the spirit and scope of the appended claims. Numerous specific details are set forth in order to provide a thorough understanding of the subject matter presented herein. But it will be apparent to one of ordinary skill in the art that the subject matter may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the implementations.

Petitioner Exhibit 1002-1122

WHAT IS CLAIMED IS:

1. A method, comprising:

at a mobile device including a display, one or more processors, and memory:

displaying one or more promotional offers on the display;

detecting a user input selecting a respective promotional offer of the one or more promotional offers;

initiating performance of a transaction with an automatic retail machine coupled with a payment module, wherein the transaction corresponds to purchase of a product stocked by the automatic retail machine;

receiving a transaction completion notification from the payment module, wherein the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine;

in response to receiving the transaction completion notification, providing a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer;

obtaining the product code for the vended product;

after obtaining the product code, transmitting the product code to the server; and,

in response to transmitting the product code:

receiving promotion validation information from the server; and

displaying the promotion validation information on the display, wherein the promotion validation information indicates whether the respective promotion offer was validated.

2. The method of claim 1, wherein the one or more promotional offers are identified based on at least one of: a unique identifier corresponding to the payment module, at least one of a current time and date, a location of the automatic retail machine, a location of the mobile device, and a unique identifier corresponding to the user of the mobile device.

3. The method of any one of claims 1-2, further comprising:

prior to displaying the one or more promotional offers:

obtaining an information packet broadcast by the payment module coupled with the automatic retail machine, wherein the information packet at least includes an authorization code and a unique identifier corresponding to the payment module;

Petitioner Exhibit 1002-1123

sending a transaction authorization request to a server, wherein the transaction authorization includes the authorization code and the unique identifier corresponding to the payment module; and,

in response to the transaction authorization request, receiving authorization information from the server that includes an authorization grant token for initiating a transaction with the automatic retail machine coupled with the payment module and the one or more promotional offers from the server.

4. The method of claim 3, wherein performance of the transaction with the automatic retail machine coupled with the payment module is initiated by sending the authorization grant token to the payment module, wherein the authorization grant token includes the authorization code included in the broadcast information packet.

5. The method of claim 1, wherein obtaining the product code further comprises:

capturing an image of the product that includes the product code; and

extracting the product code from the captured image.

6. The method of claim 1, wherein obtaining the product code further comprises:

scanning the product code of the product with a scanner unit of the mobile device

7. The method of any one of claims 1, 2, and 4-6, wherein the promotion validation information indicates the price of the product after the application of the respective promotional offer.

8. The method of any one of claims 1, 2, and 4-6, further comprising:

after obtaining the product code, determining whether a predetermined time period has expired;

in accordance with a determination that the time period has expired, providing a notification to the user of mobile device indicating that the respective promotional offer has expired; and,

in accordance with a determination that the time period has not expired, transmitting the product code to the server.

9. The method of any one of claims 1, 2, and 4-6, further comprising:

transmitting the transaction completion notification to the server.

Petitioner Exhibit 1002-1124

10. The method of any one of claims 1, 2, and 4-6, wherein the mobile device further includes a first transceiver associated with a short-range communication protocol and a second transceiver associated with a long-range communication protocol.

11. A mobile device, comprising:

a display;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for performing the method of any one of claims 1-10.

12. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with a display and one or more processors, cause the computing device to perform the method of any one of claims 1-10.

Petitioner Exhibit 1002-1125

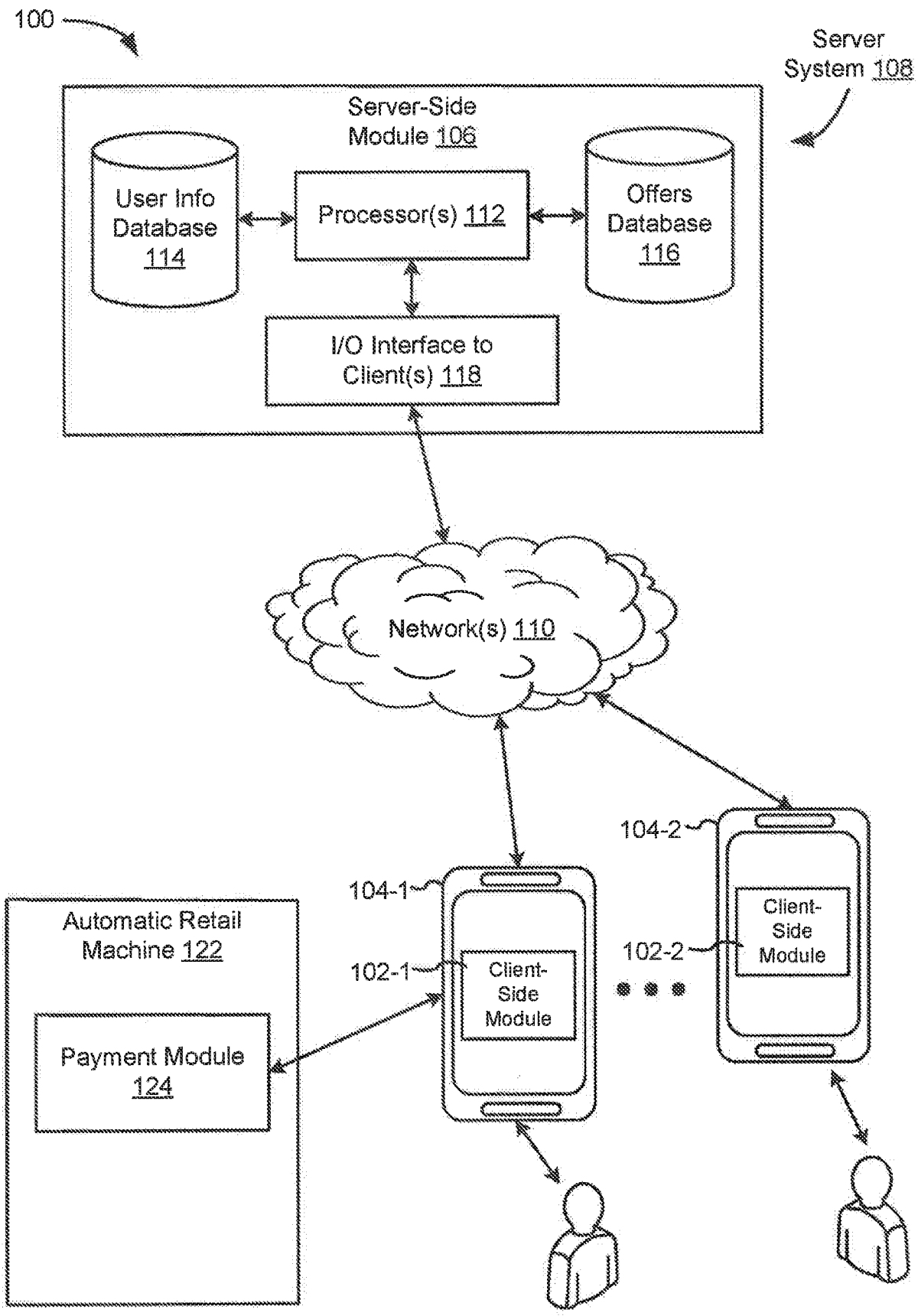


Figure 1 Petitioner Exhibit 1002-1126

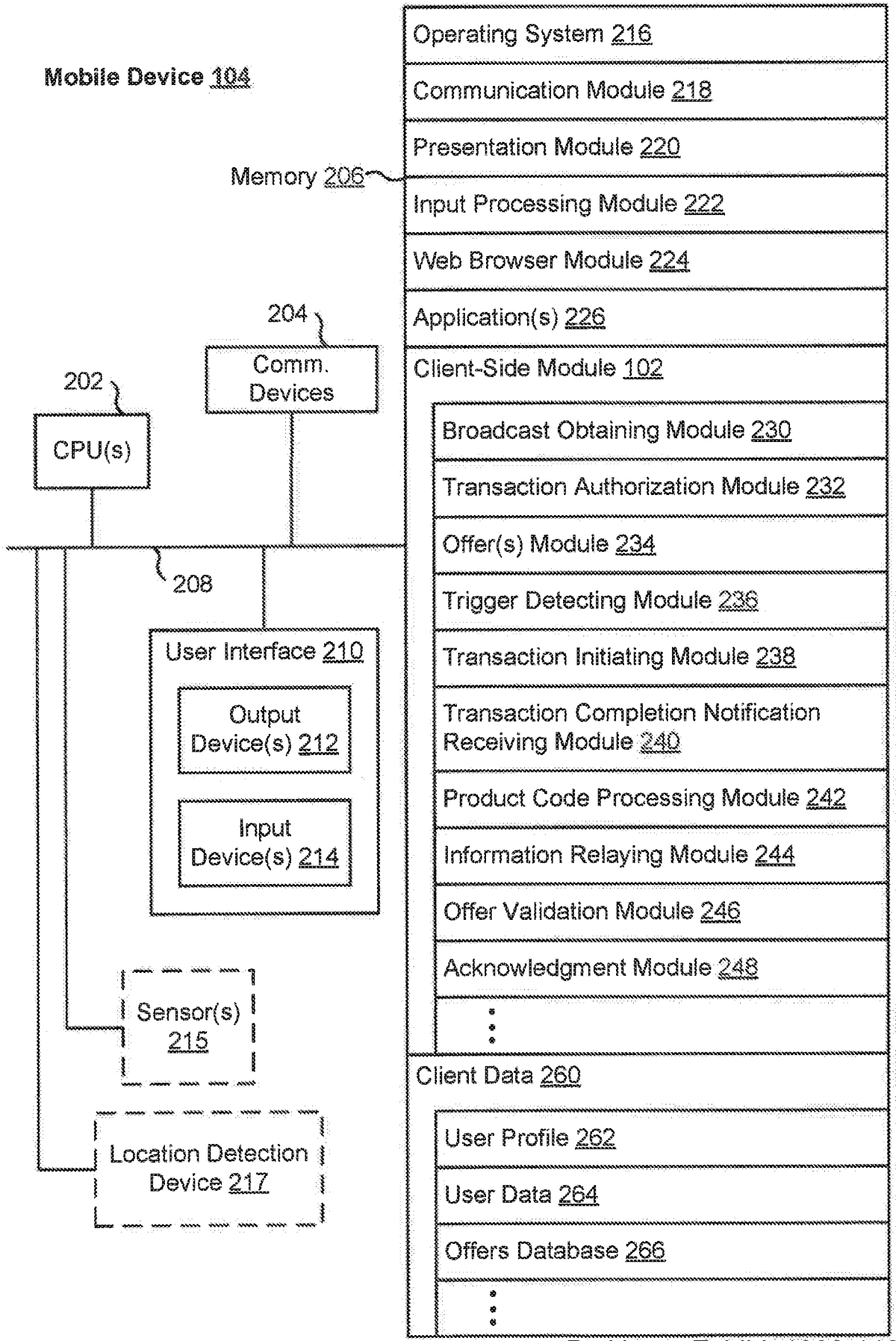


Figure 2

Petitioner Exhibit 1002-1127

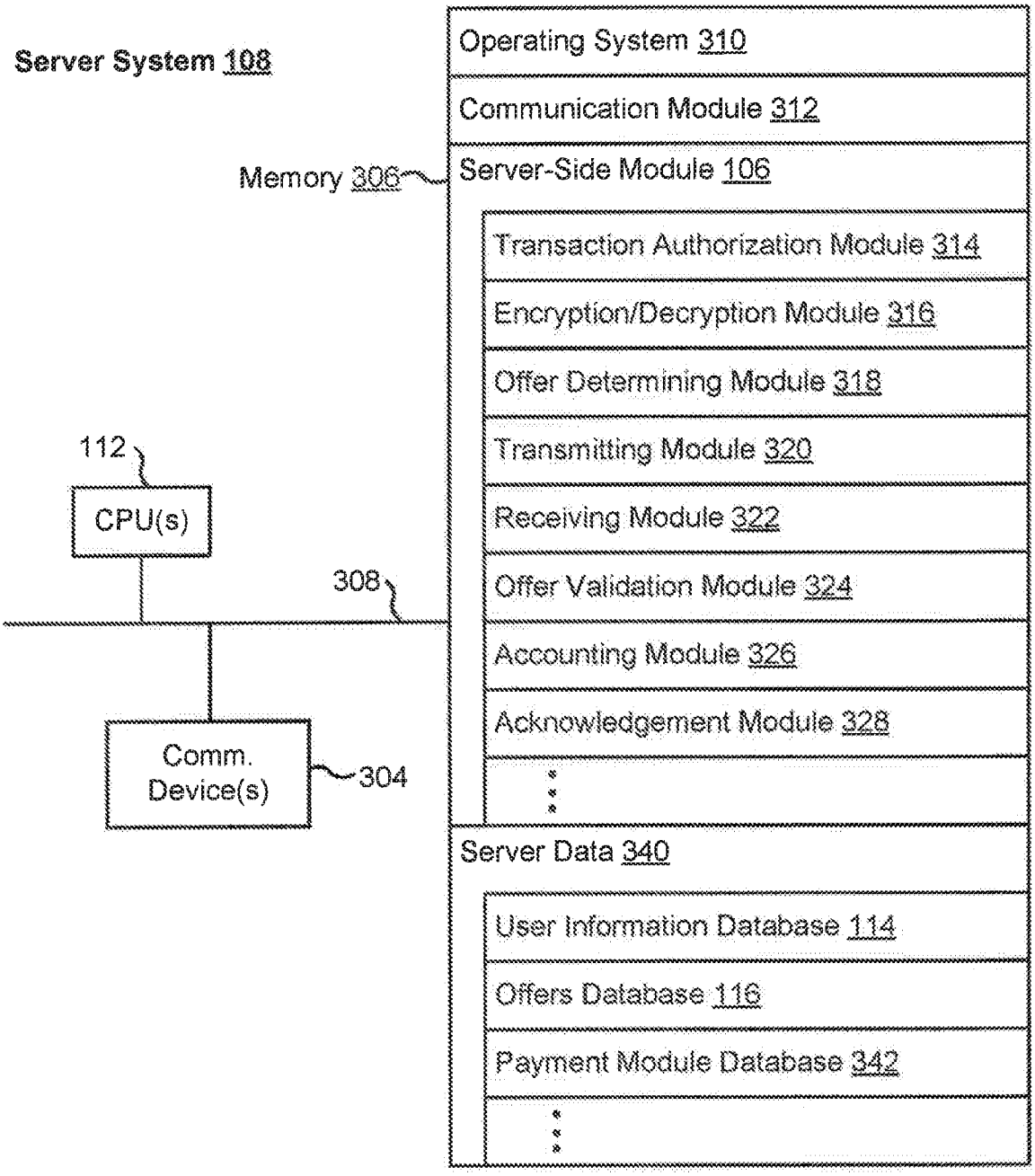

Server System 108
Operating System 310
Communication Module 312
Memory 306
Server-Side Module 106
Transaction Authorization Module 314
Encryption/Decryption Module 316
Offer Determining Module 318
Transmitting Module 320
Receiving Module 322
Offer Validation Module 324
Accounting Module 326
Acknowledgement Module 328
112
CPU(s)
308
Comm. Device(s)
304
Server Data 340
User Information Database 114
Offers Database 116
Payment Module Database 342

Figure 3

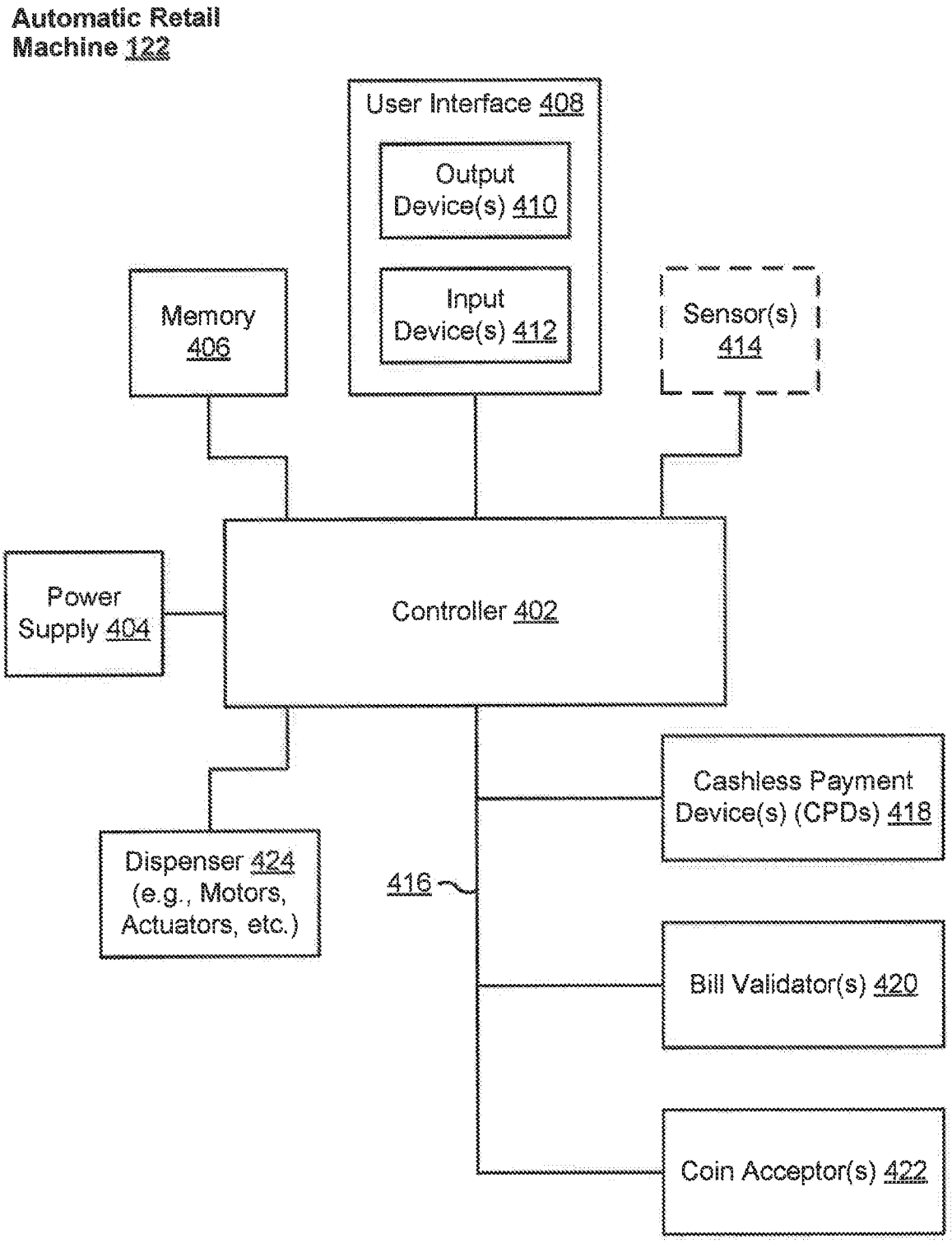

Automatic Retail Machine 122
User Interface 408
Output Device(s) 410
Input Device(s) 412
Memory 406
Sensor(s) 414
Power Supply 404
Controller 402
Dispenser 424 (e.g., Motors, Actuators, etc.)
416
Cashless Payment Device(s) (CPDs) 418
Bill Validator(s) 420
Coin Acceptor(s) 422

Figure 4

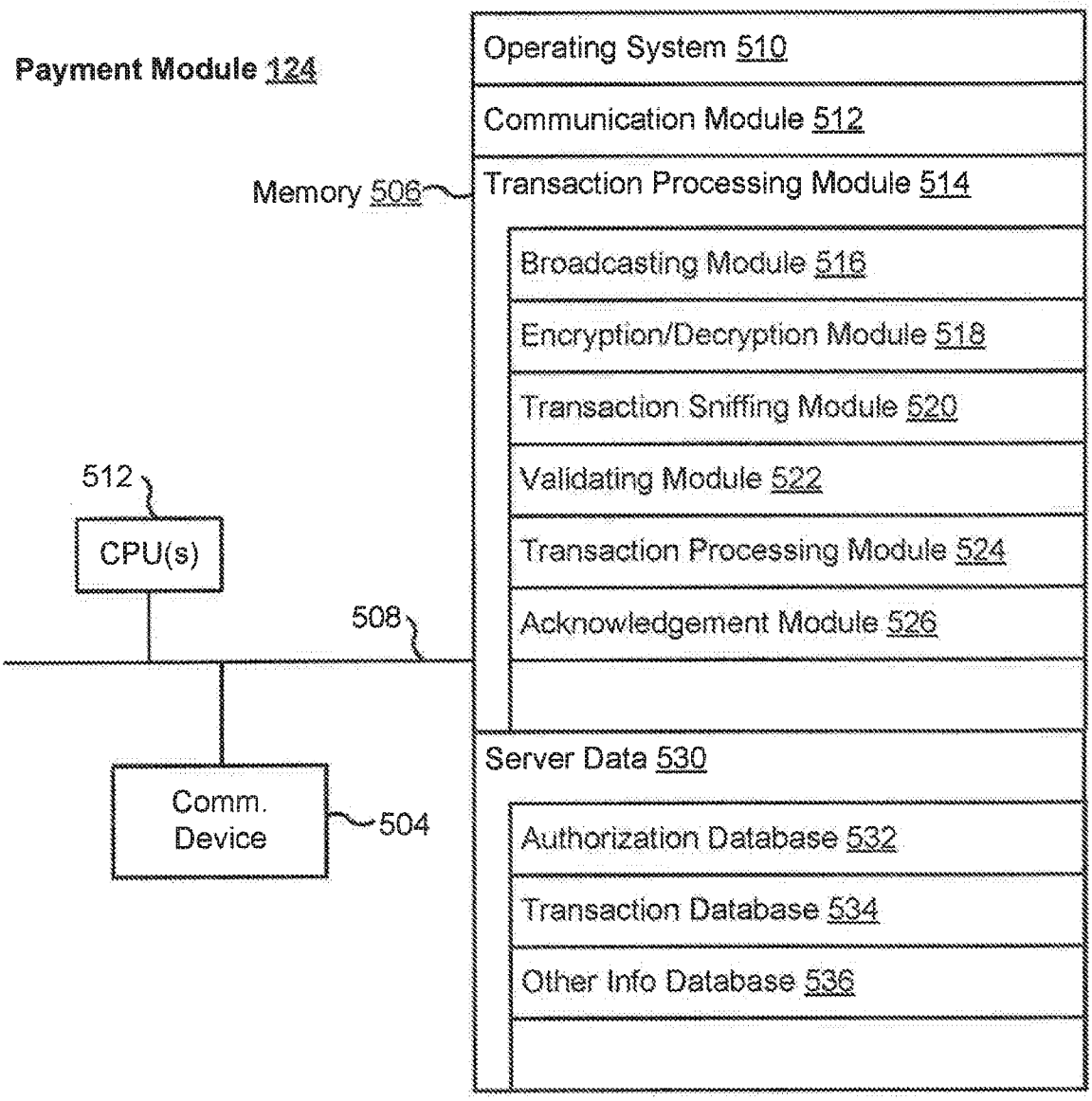

Payment Module 124
Operating System 510
Communication Module 512
Memory 506
Transaction Processing Module 514
Broadcasting Module 516
Encryption/Decryption Module 518
Transaction Sniffing Module 520
Validating Module 522
Transaction Processing Module 524
Acknowledgement Module 526
512
CPU(s)
508
Server Data 530
Comm. Device
504
Authorization Database 532
Transaction Database 534
Other Info Database 536

Figure 5

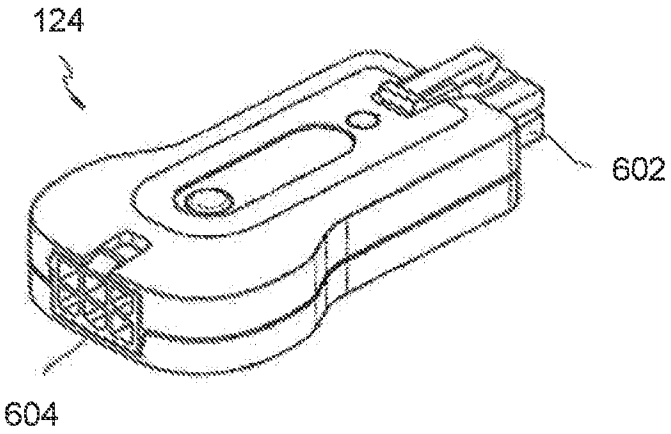


Figure 6A

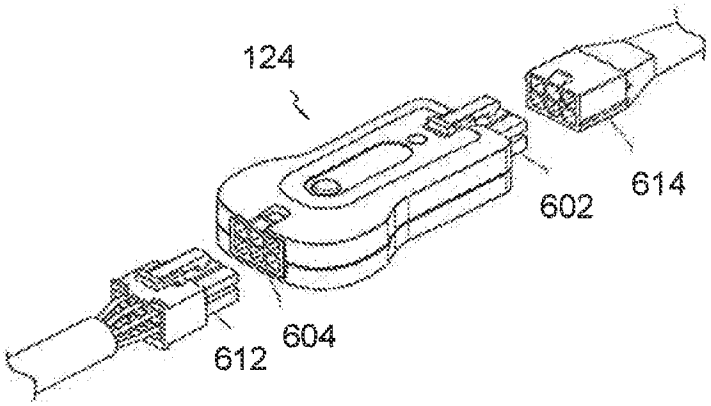
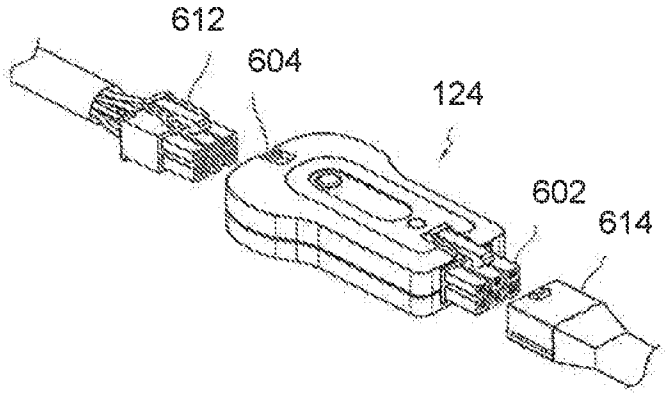
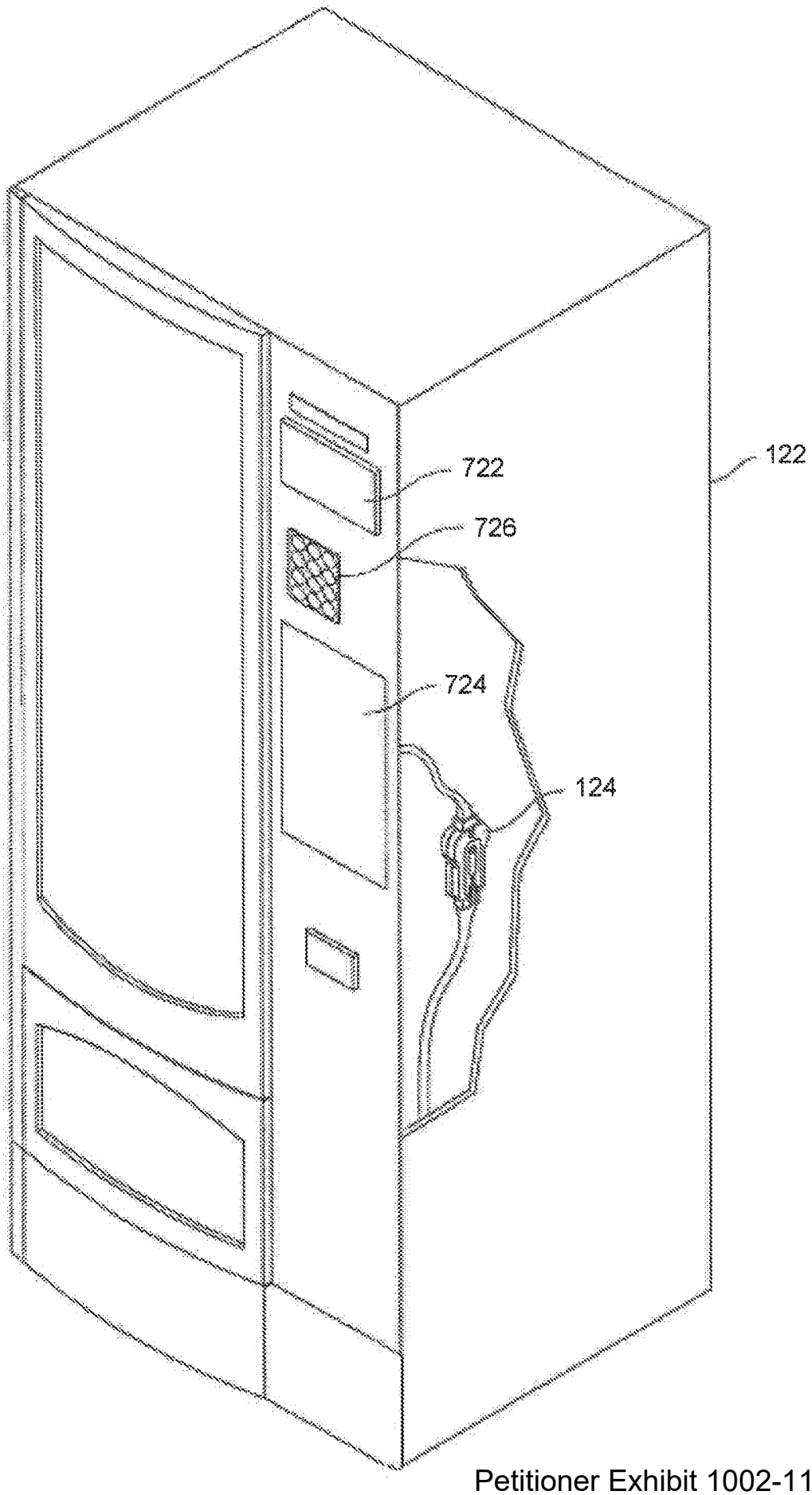


Figure 6B





Petitioner Exhibit 1002-1132

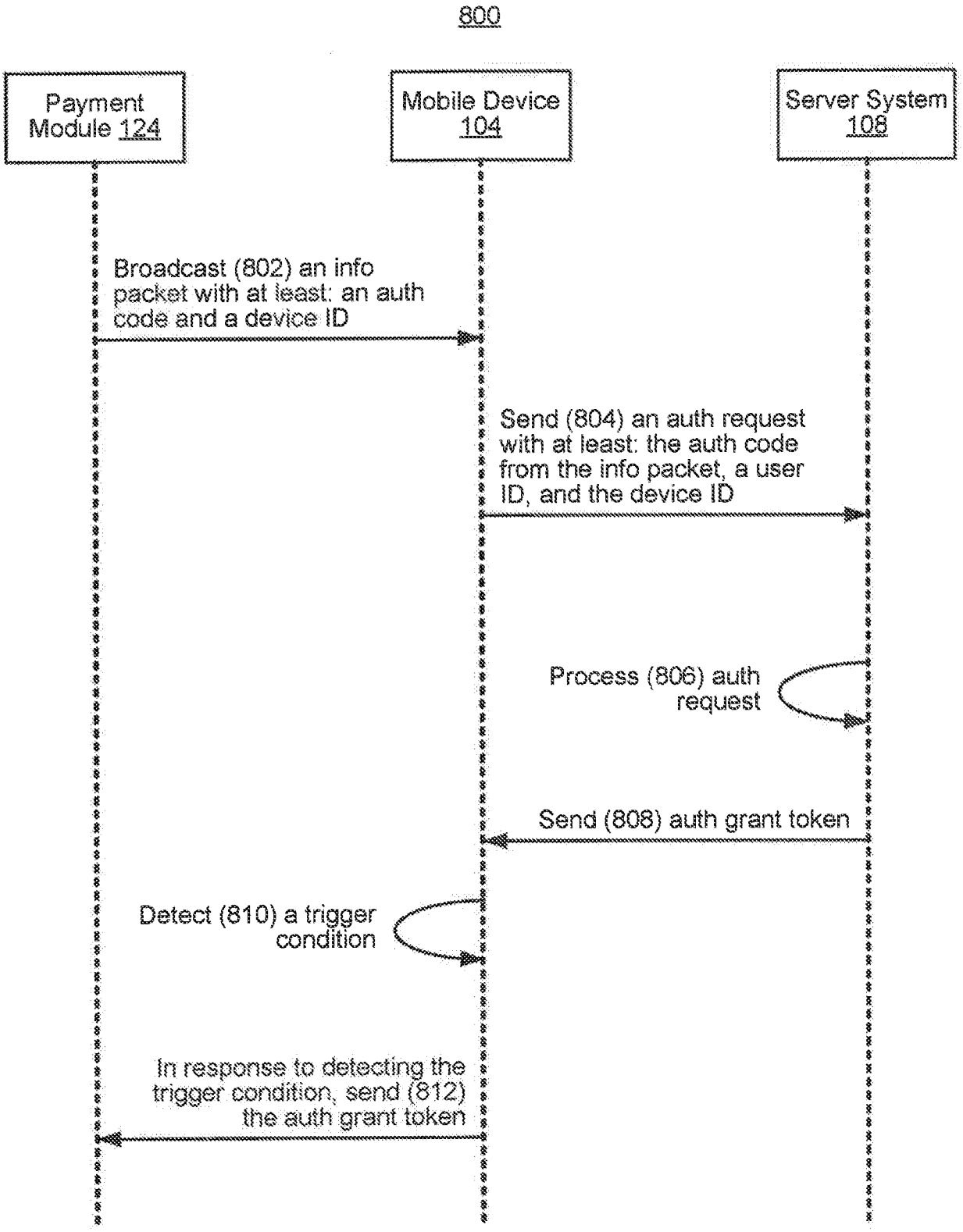

800
Payment Module 124
Mobile Device 104
Server System 108
Broadcast (802) an info packet with at least: an auth code and a device ID
Send (804) an auth request with at least: the auth code from the info packet, a user ID, and the device ID
Process (806) auth request
Send (808) auth grant token
Detect (810) a trigger condition
In response to detecting the trigger condition, send (812) the auth grant token

Figure 8

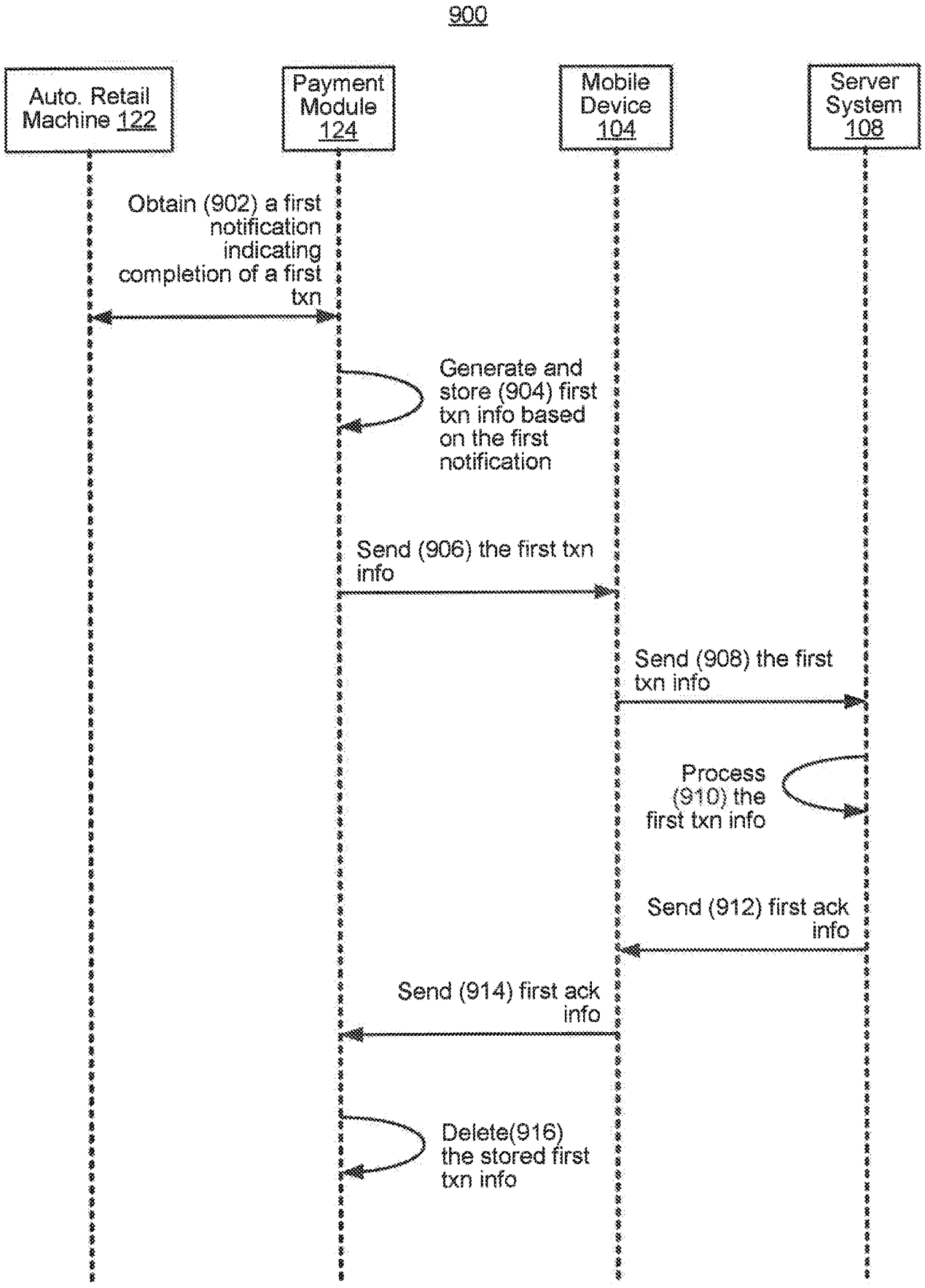


Figure 9

Petitioner Exhibit 1002-1134

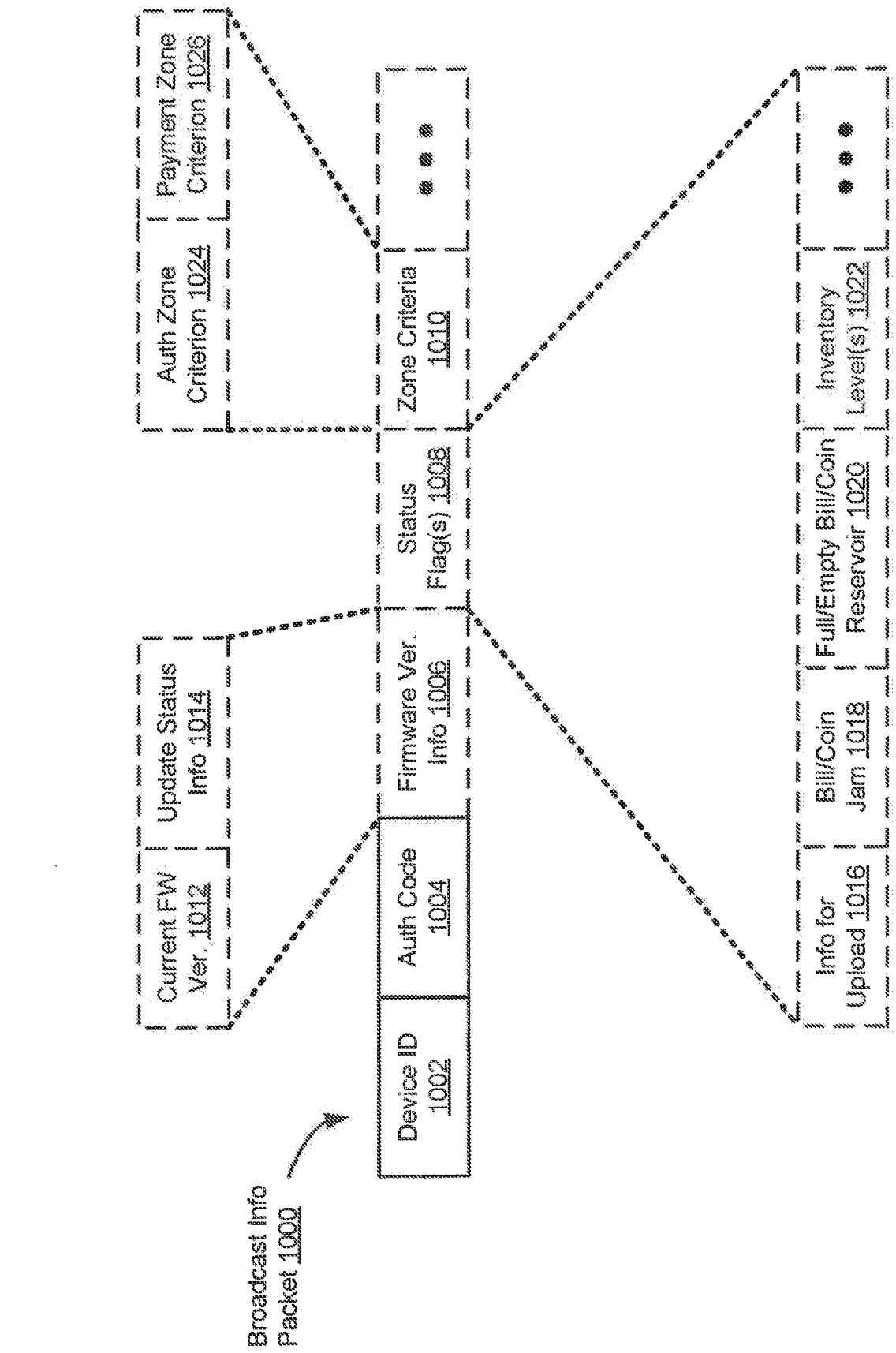

Broadcast Info Packet 1000
Device ID 1002
Auth Code 1004
Firmware Ver. Info 1006
Status Flag(s) 1008
Zone Criteria 1010
Current FW Ver. 1012
Update Status Info 1014
Auth Zone Criterion 1024
Payment Zone Criterion 1026
Info for Upload 1016
Bill/Coin Jam 1018
Full/Empty Bill/Coin Reservoir 1020
Inventory Level(s) 1022

Figure 10A

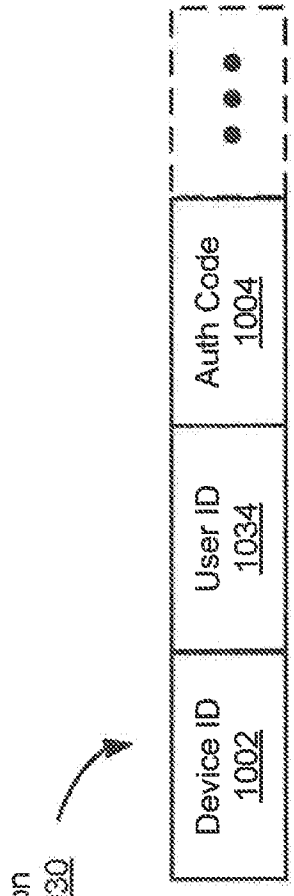


Figure 10B

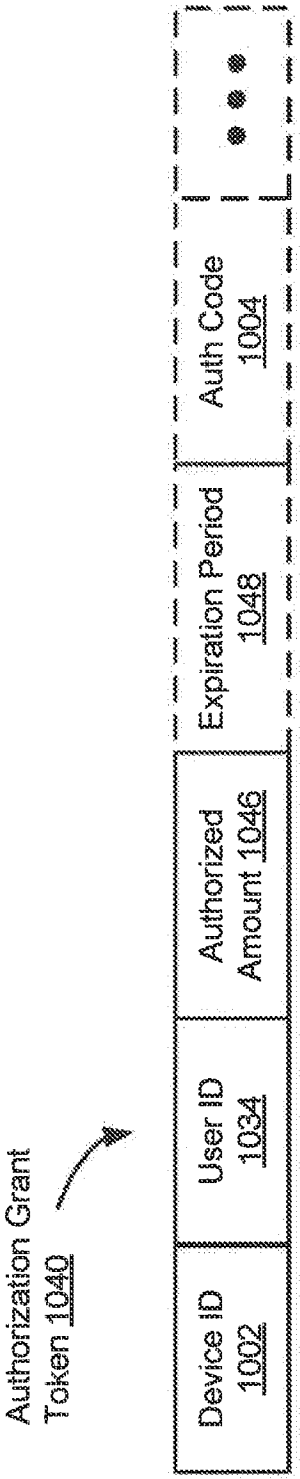


Figure 10C

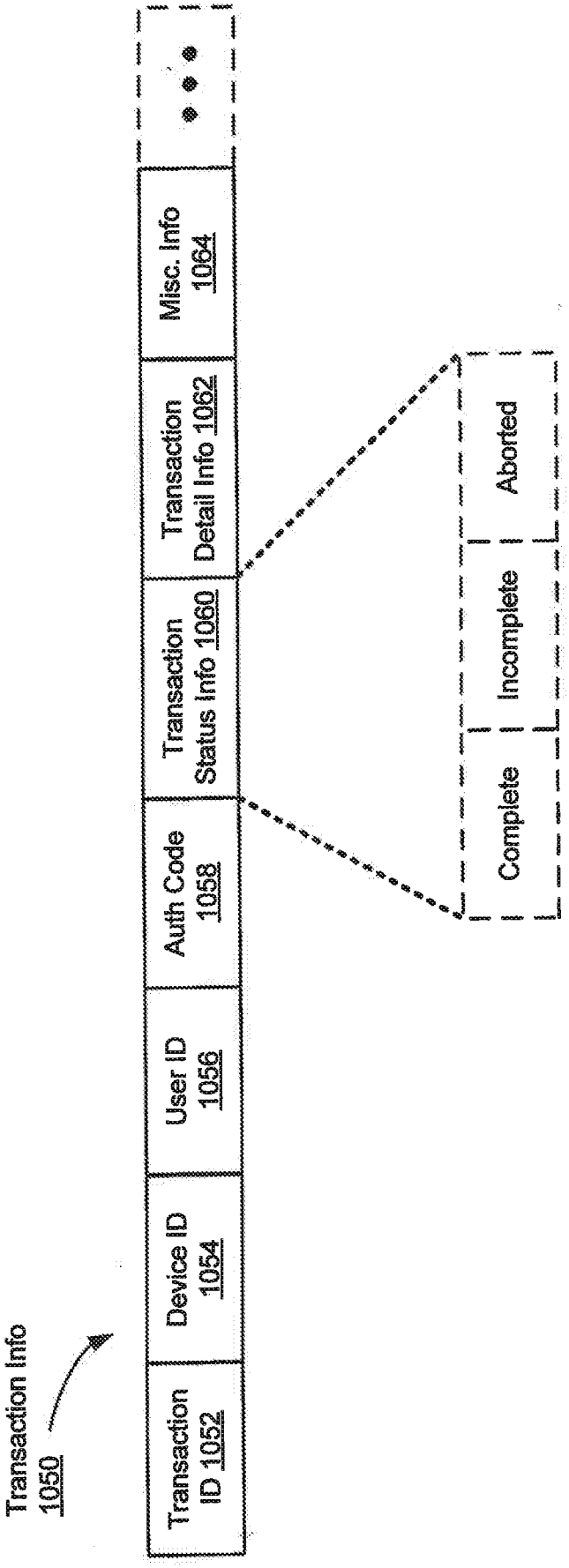
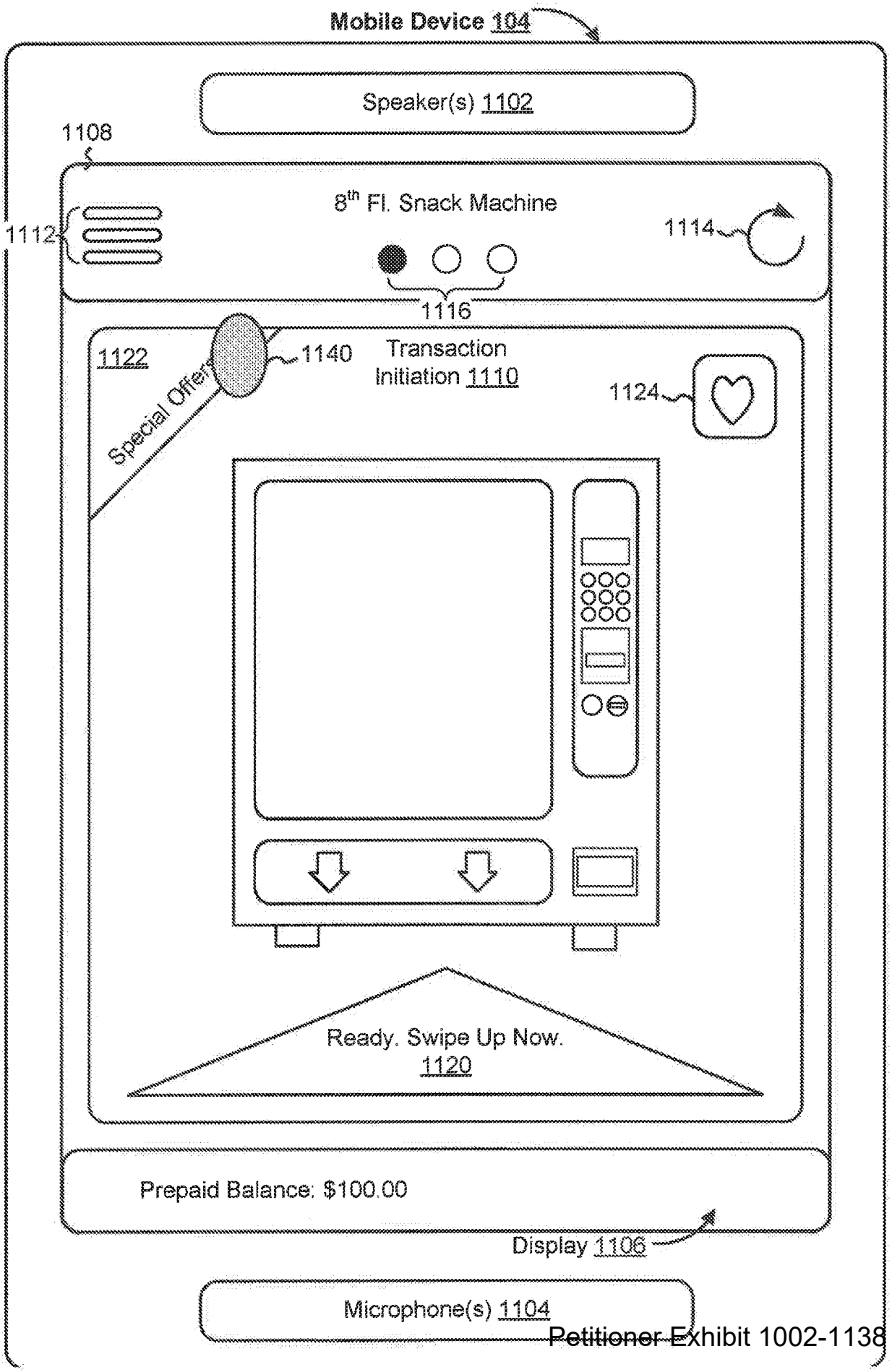
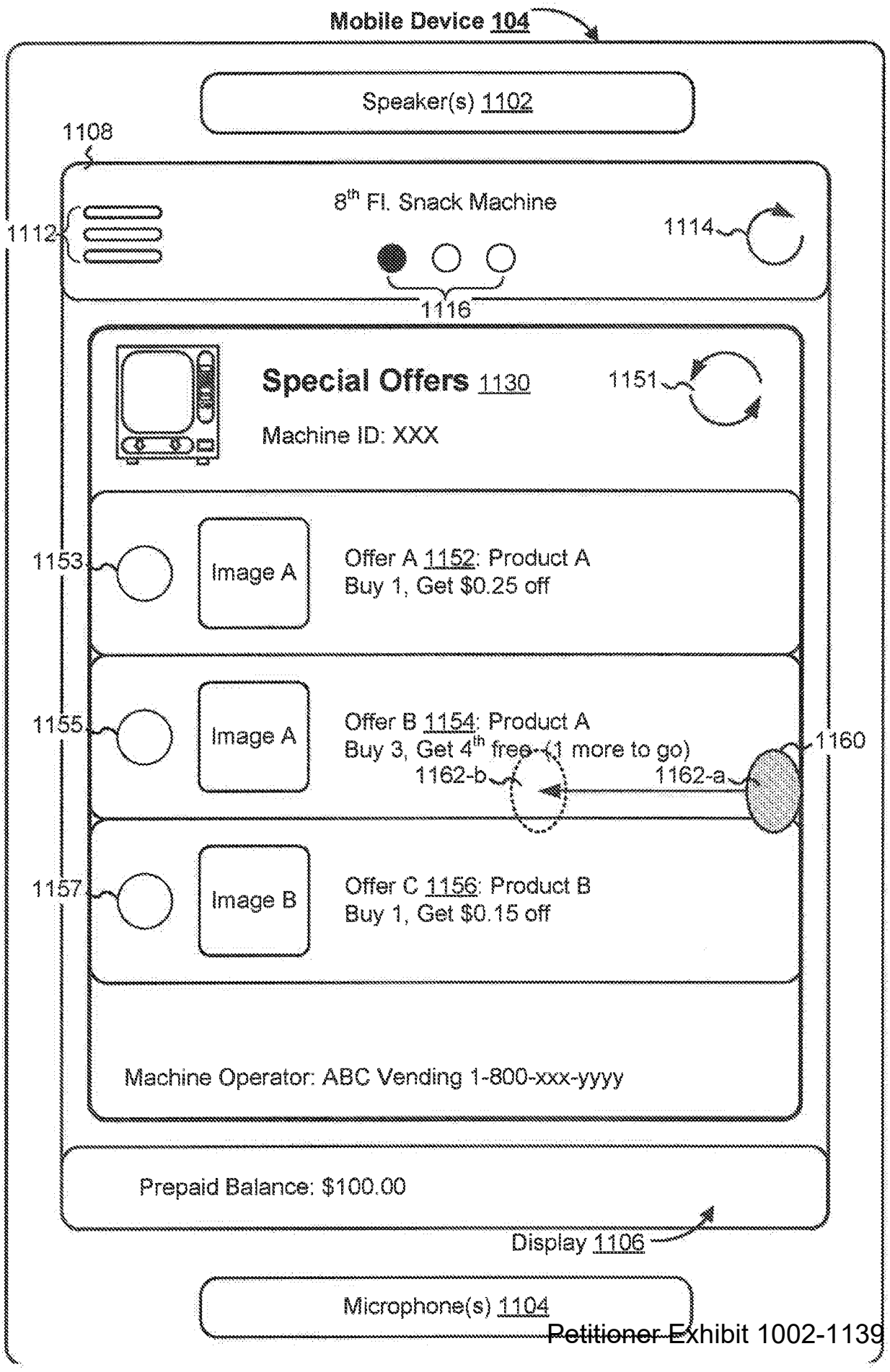
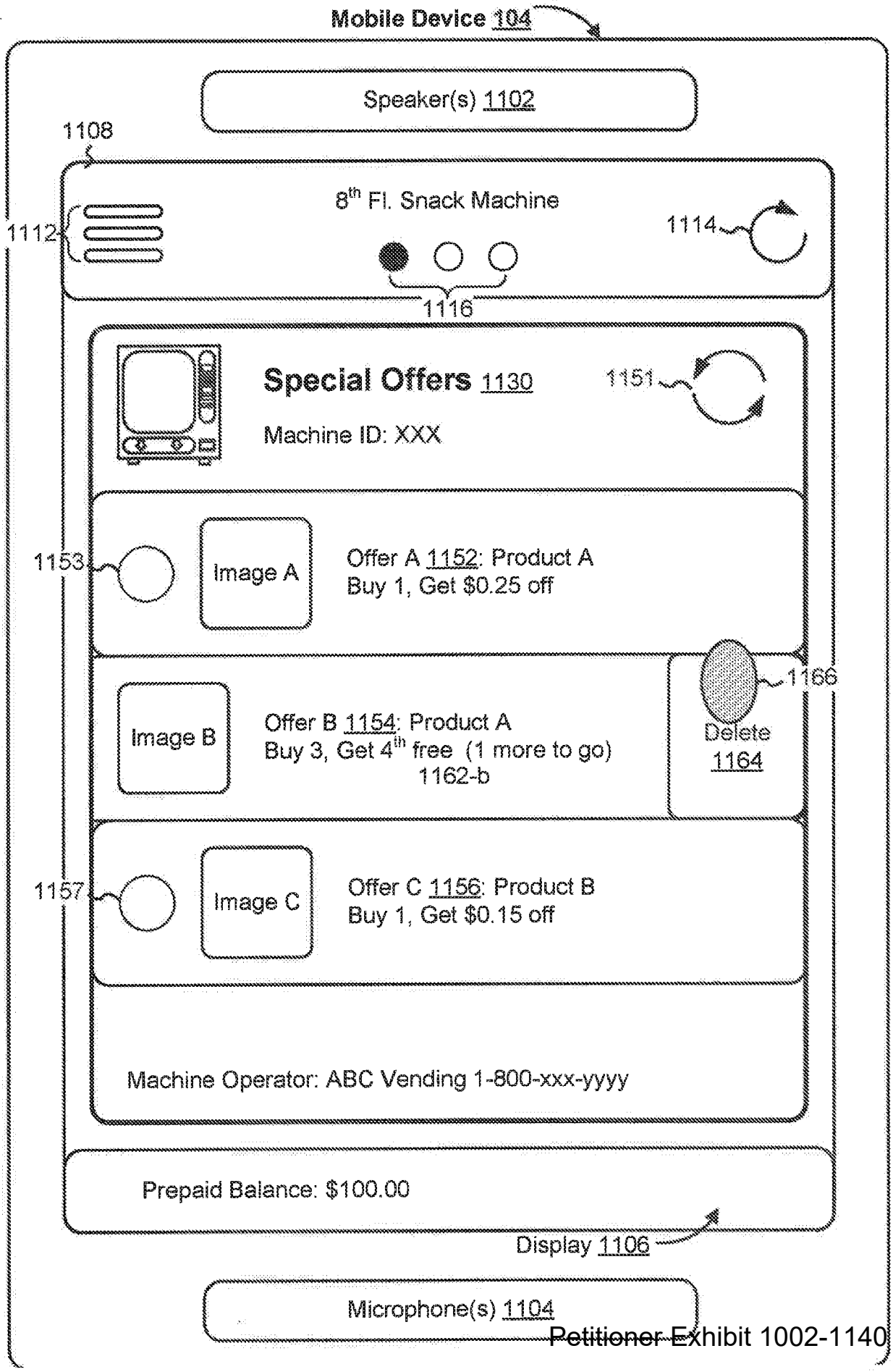

Transaction Info 1050
Transaction ID 1052
Device ID 1054
User ID 1056
Auth Code 1058
Transaction Status Info 1060
Transaction Detail Info 1062
Misc. Info 1064
Complete
Incomplete
Aborted

Figure 10D

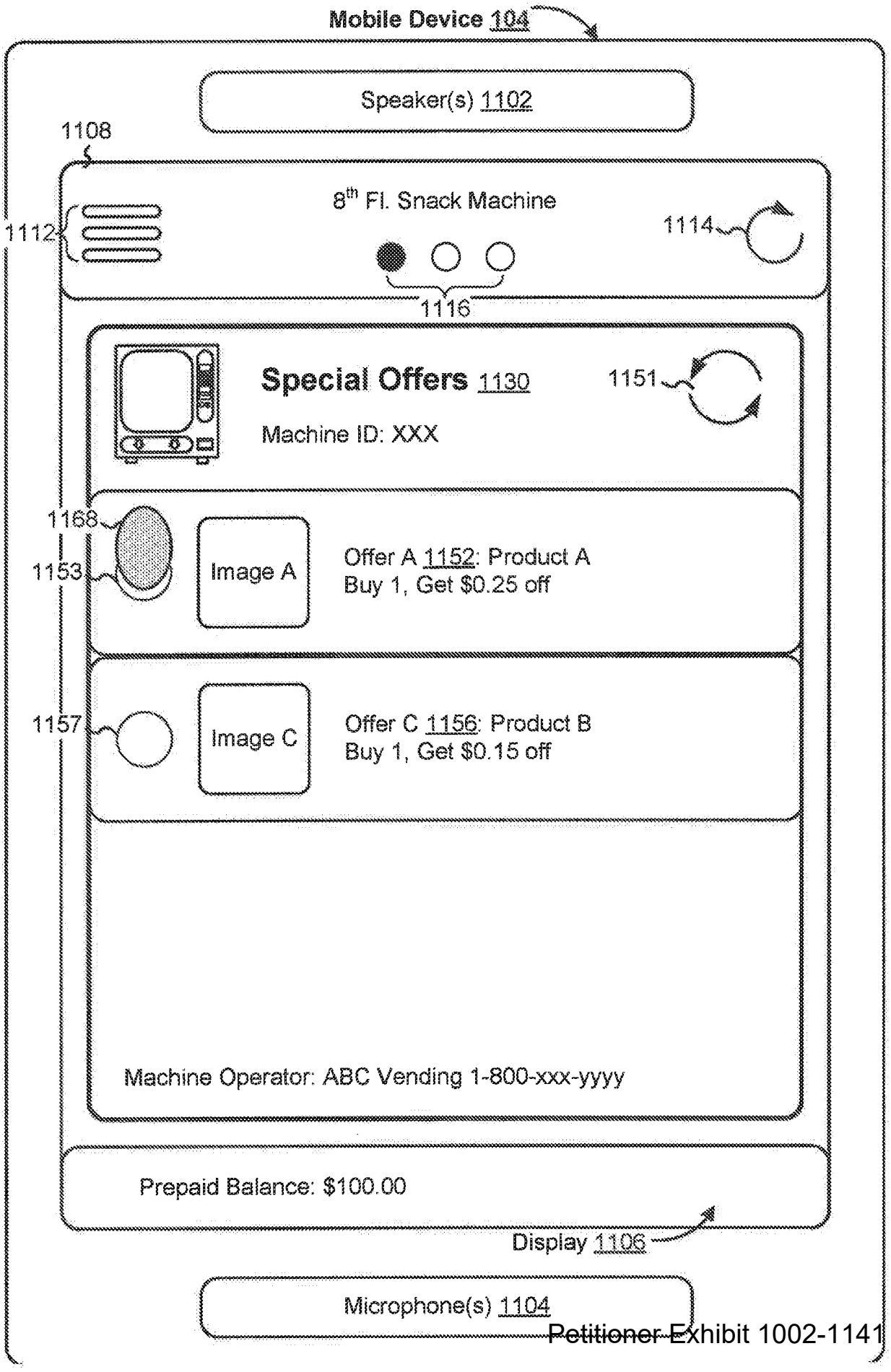

Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
1114
1116
1122
Special Offers
1140
Transaction Initiation 1110
1124
Ready. Swipe Up Now.
1120
Prepaid Balance: $100.00
Display 1106
Microphone(s) 1104

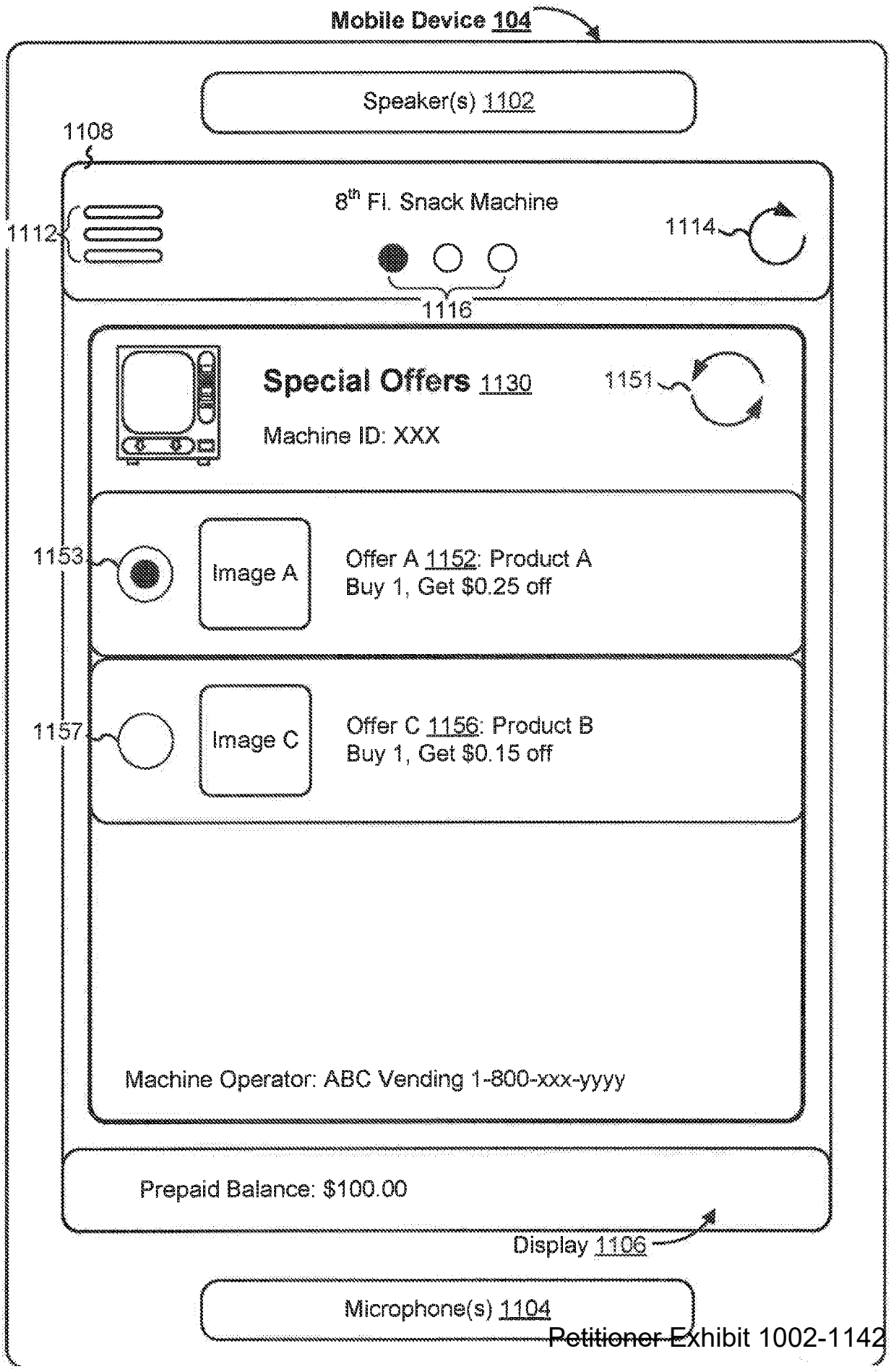


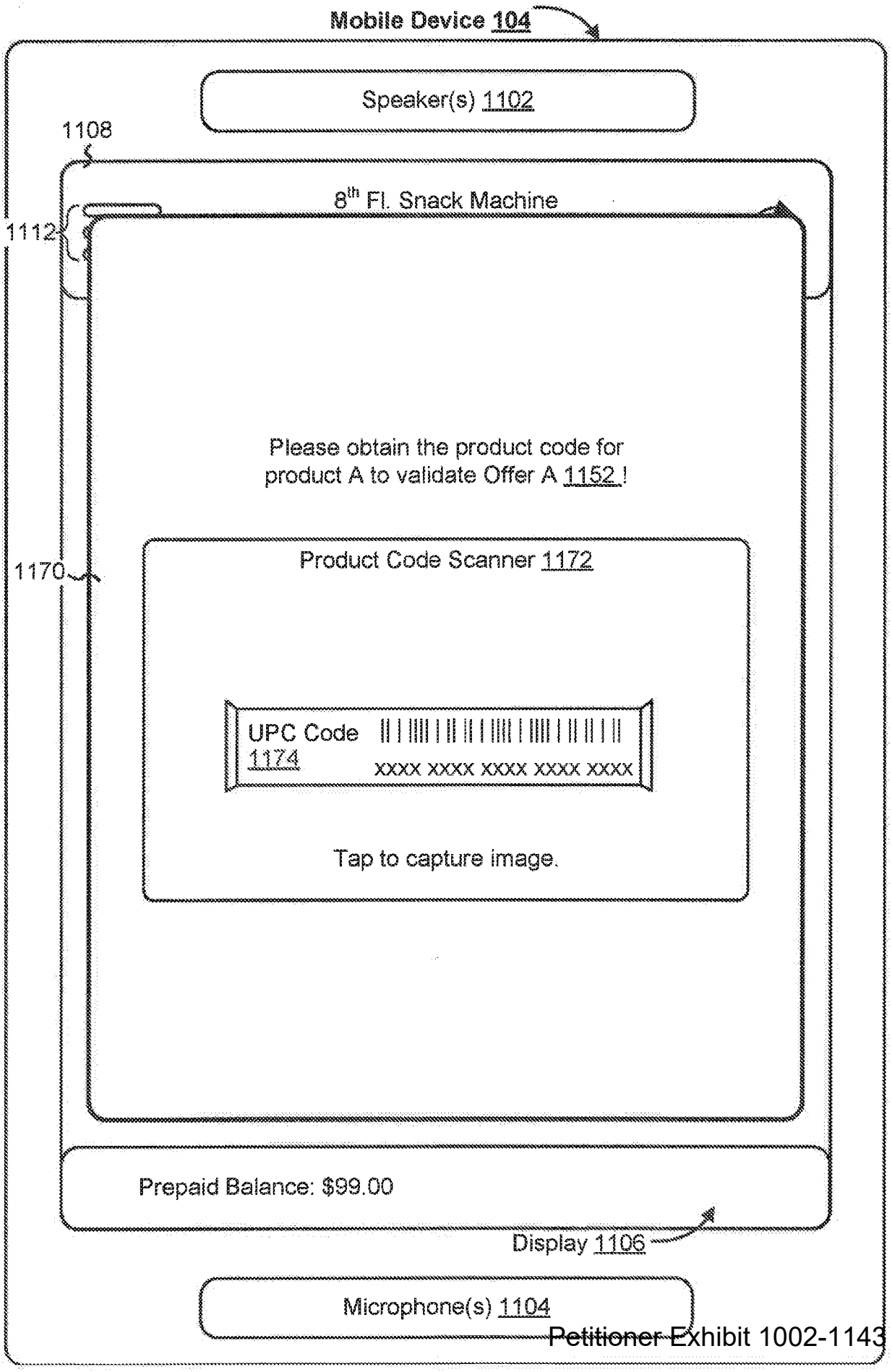
Petitioner Exhibit 1002-1139



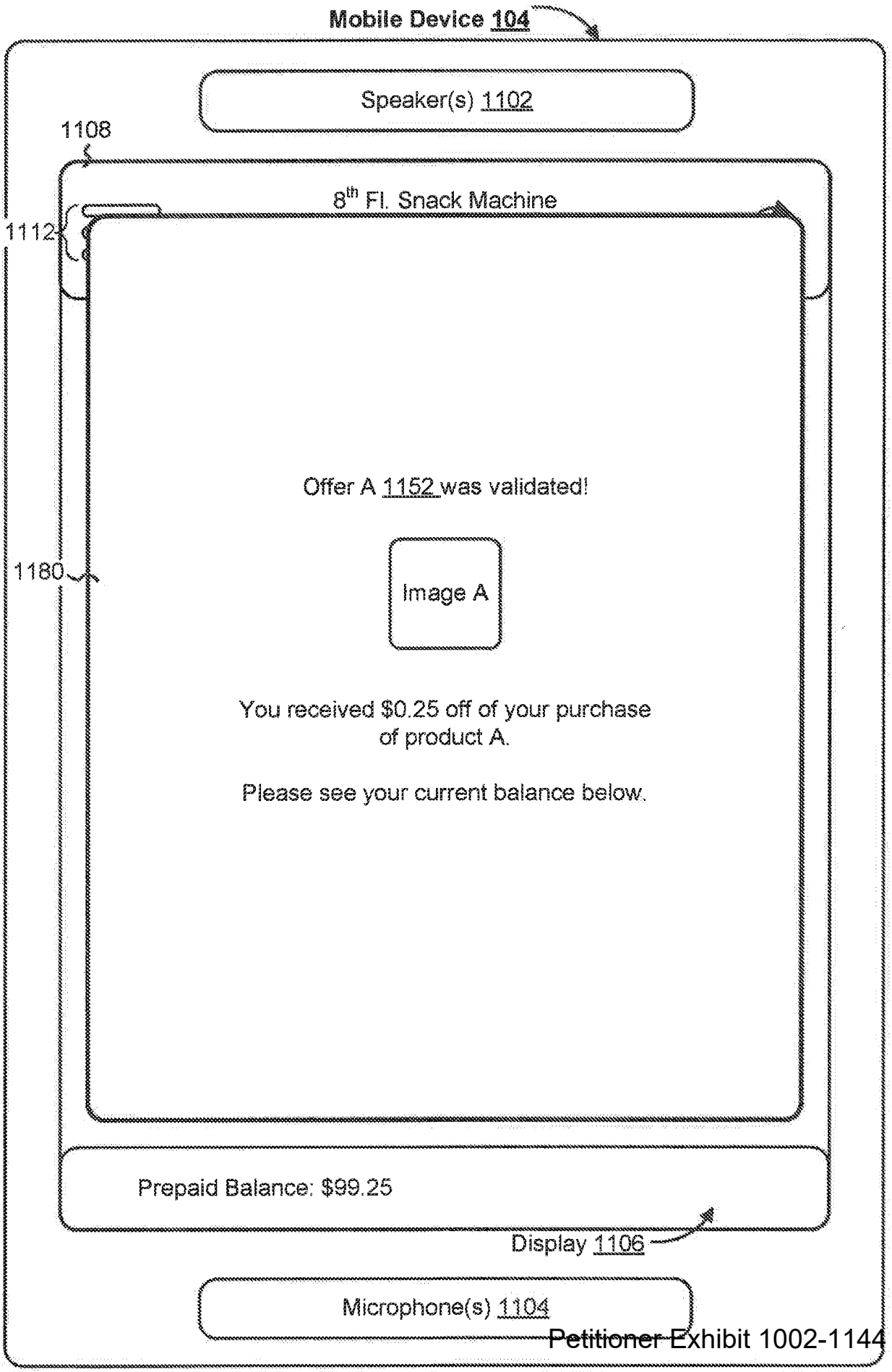
Petitioner Exhibit 1002-1140


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
1114
1116
Special Offers 1130
1151
Machine ID: XXX
1168
1153
Image A
Offer A 1152: Product A
Buy 1, Get $0.25 off
1157
Image C
Offer C 1156: Product B
Buy 1, Get $0.15 off
Machine Operator: ABC Vending 1-800-xxx-yyyy
Prepaid Balance: $100.00
Display 1106
Microphone(s) 1104


Mobile Device 104
Speaker(s) 1102
1108
1112
8th Fl. Snack Machine
1114
1116
Special Offers 1130
1151
Machine ID: XXX
1153
Image A
Offer A 1152: Product A
Buy 1, Get $0.25 off
1157
Image C
Offer C 1156: Product B
Buy 1, Get $0.15 off
Machine Operator: ABC Vending 1-800-xxx-yyyy
Prepaid Balance: $100.00
Display 1106
Microphone(s) 1104



Petitioner Exhibit 1002-1143


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
Offer A 1152 was validated!
1180
Image A
You received $0.25 off of your purchase of product A.
Please see your current balance below.
Prepaid Balance: $99.25
Display 1106
Microphone(s) 1104

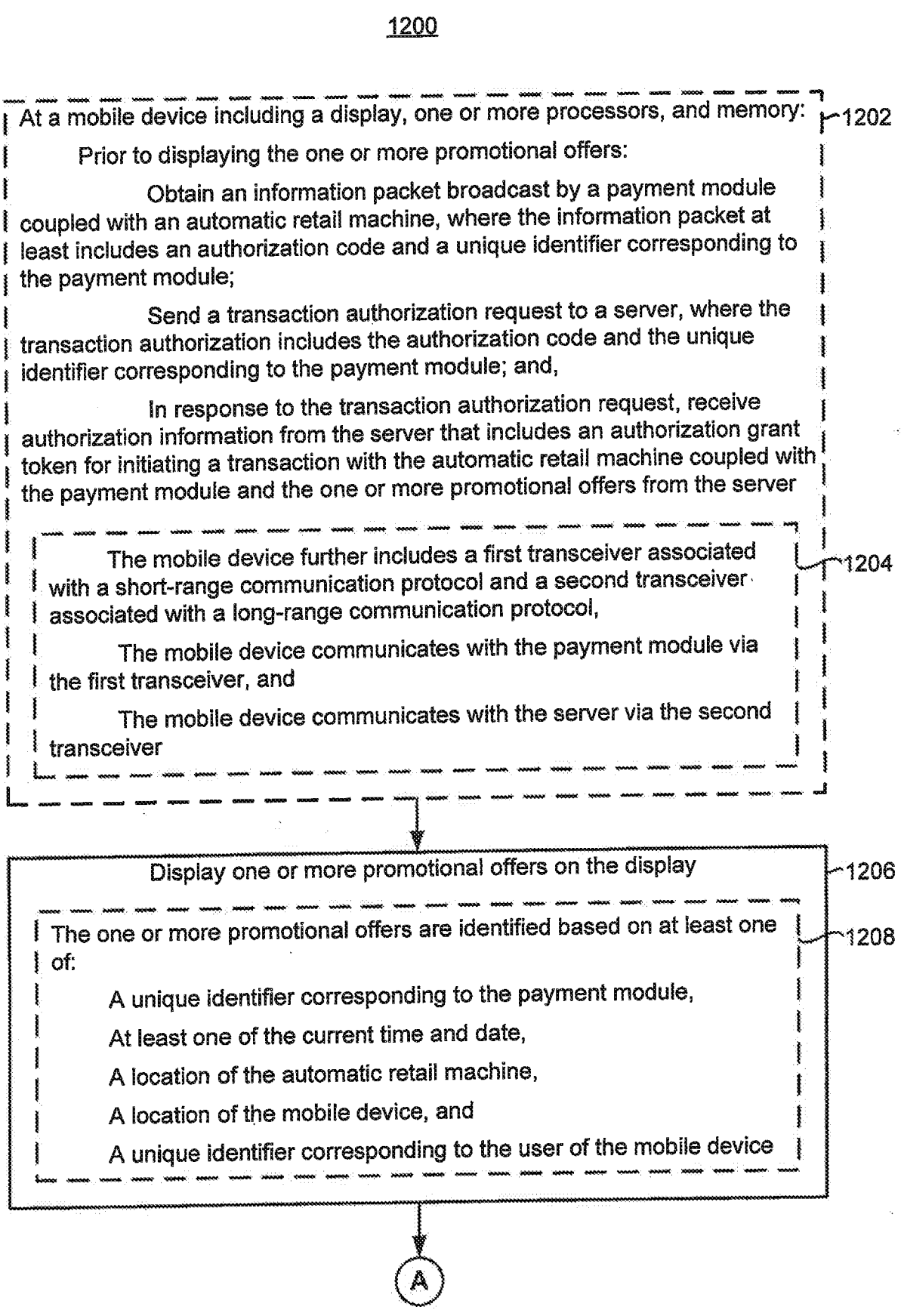


Figure 12A

Petitioner Exhibit 1002-1145

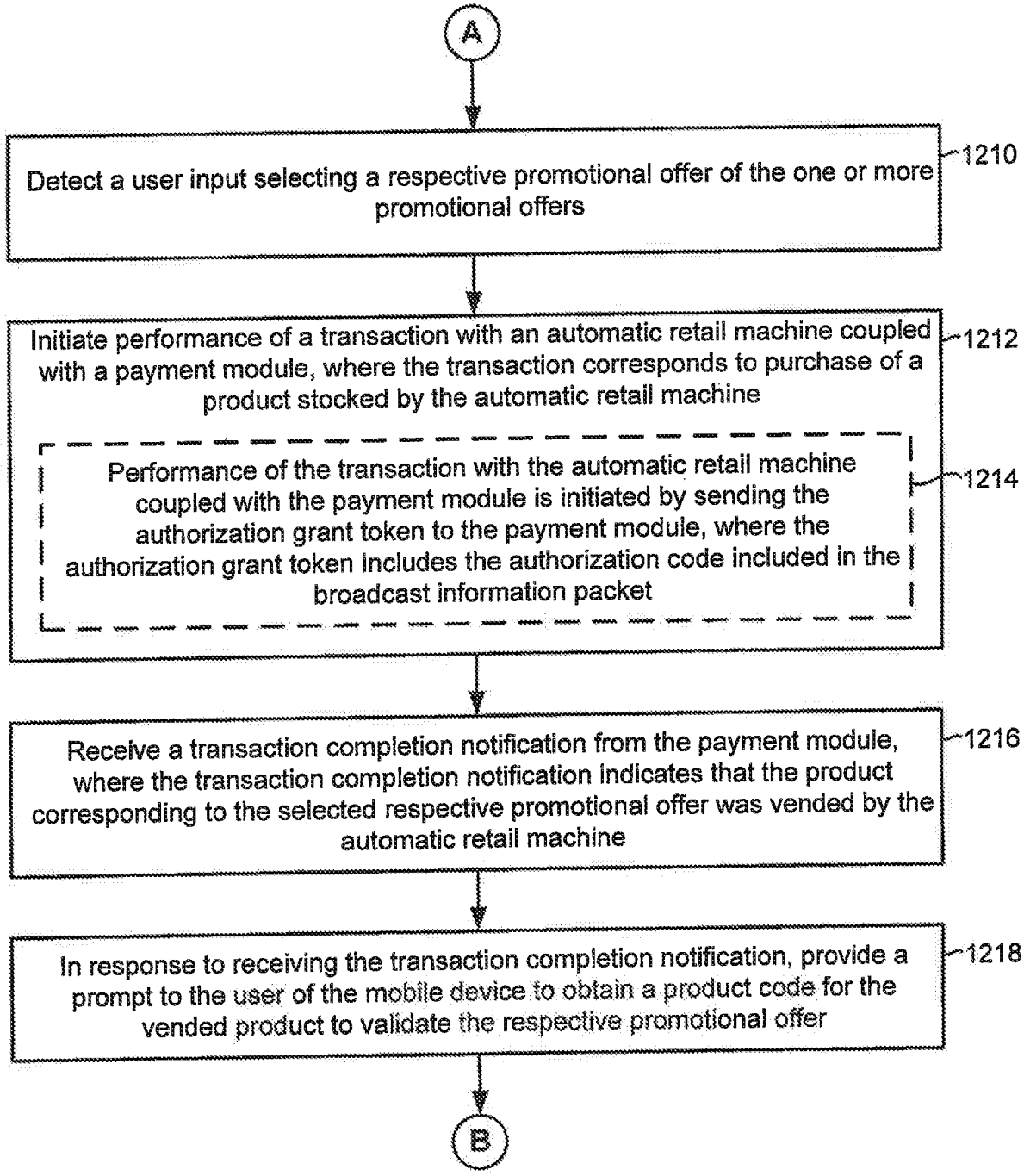

A
Detect a user input selecting a respective promotional offer of the one or more promotional offers
1210
Initiate performance of a transaction with an automatic retail machine coupled with a payment module, where the transaction corresponds to purchase of a product stocked by the automatic retail machine
1212
Performance of the transaction with the automatic retail machine coupled with the payment module is initiated by sending the authorization grant token to the payment module, where the authorization grant token includes the authorization code included in the broadcast information packet
1214
Receive a transaction completion notification from the payment module, where the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine
1216
In response to receiving the transaction completion notification, provide a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer
1218
B

Figure 12B

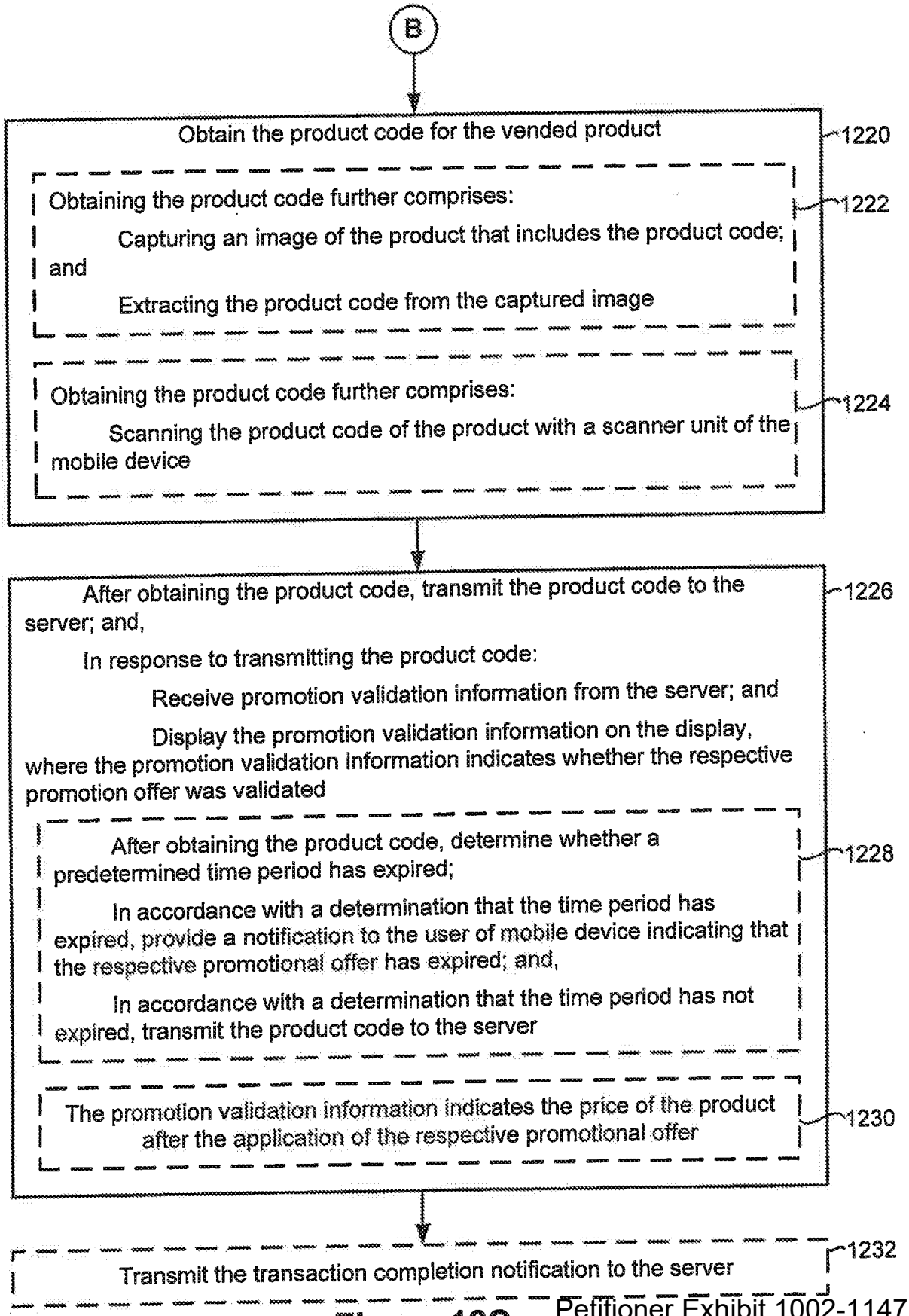


Figure 12C

Petitioner Exhibit 1002-1147

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/015763

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q30/02 G06Q20/18 G06Q30/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 8 856 045 B1 (PATEL PARESH K [US] ET AL) 7 October 2014 (2014-10-07) abstract figure 7 figure 10A figure 10C column 3, line 46 - line 64 column 10, line 38 - line 51 column 12, line 15 - line 51 column 14, line 53 - line 65 column 23, line 17 - line 25 column 28, line 52 - line 67 column 29, line 53 - line 60	1-12
A	US 2014/136301 A1 (VALDES JUAN [US]) 15 May 2014 (2014-05-15) abstract paragraph [0045] - paragraph [0061] paragraph [0062] - paragraph [0067]	1-12

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 March 2016	08/04/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040,	Mercan, Raimund

Petitioner Exhibit 1002-1148

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/015763

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8856045 B1	07-10-2014	US 8856045 B1	07-10-2014
		US 2015170130 A1	18-06-2015
		US 2015227928 A1	13-08-2015
		WO 2015095599 A1	25-06-2015
US 2014136301 A1	15-05-2014	NONE	

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 January 2017 (19.01.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/010936 A1

(51) International Patent Classification:
G06Q 20/32 (2012.01) *G06Q 40/02* (2012.01)

(21) International Application Number:
PCT/SG2016/050297

(22) International Filing Date:
27 June 2016 (27.06.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201505585T 16 July 2015 (16.07.2015) SG

(71) Applicant: **TOUREGO GLOBAL PTE. LTD.** [SG/SG]; 141 Cecil Street, #08-07 Tung Ann Association Building, Singapore 069541 (SG).

(72) Inventor: **TAN, Tie Wee**; c/o 14, Robinson Road, #08-01A, Far East Finance Building, Singapore 048545 (SG).

(74) Agent: **YUSARN AUDREY**; 24 Raffles Place, #27-01, Clifford Centre, Singapore 048621 (SG).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) Title: SYSTEM AND METHOD FOR FACILITATING REFUNDS

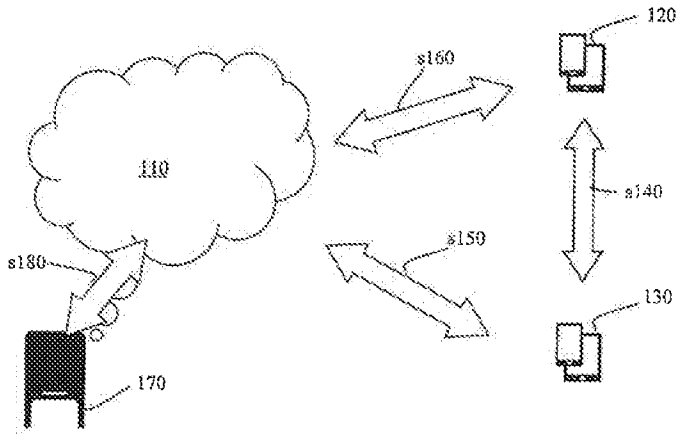


FIG. 1

(57) Abstract: A system and method for facilitating a refund to a user is disclosed. The system comprises a mobile device having means to communicate with a central processor for the generation of a refund account and a unique identifier; the unique identifier associated with the user; a computer device operable to access the unique identifier for verification upon receipt of a refund qualifying transaction associated with the user, the computer device further operable to send information relating to the refund qualifying transaction and generate a refund request upon successful verification; and the [illegible] configured to be in communication with the computer device to receive and process the refund request, the central processor further configured to generate an elec-

Petitioner Exhibit 1002-1150

WO 2017/010936 A1

SYSTEM AND METHOD FOR FACILITATING REFUNDS

FIELD OF THE INVENTION

The present invention relates to a system and method for facilitating refunds, such as but not limited to a tax refund for purchases made by tourists while travelling within their destination countries ("tourist refund").

BACKGROUND ART

The following discussion of the background to the invention is intended to facilitate an understanding of the present invention only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was published, known or part of the common general knowledge of the person skilled in the art in any jurisdiction as at the priority date of the invention.

In line with tax principle while at the same time attracting tourists, jurisdictions that levy a Value-Added Tax (VAT) or Goods and Services Tax (GST) or similar would allow individuals such as tourists to claim a tax refund on the goods purchased within a country. This tax refund would be administered upon the departure of the tourists from the country; provided certain criteria are met such as the goods are unopened, unused and exported out of the country.

The Revenue/Customs authorities of the country can administer tourist refund scheme(s), although it is increasingly popular for commercial contractors to be appointed to administer on their behalf. These commercial contractors typically work in cooperation with the Revenue/Customs authorities to ensure that the appropriate amount of tax refunds is paid out to the tourist(s). A service or commission fee will be charged which would form the bulk of the revenue model for the commercial contractor.

Two methods of administration of tourist refund schemes are currently being operated in the world. One is based on the authentication of paper forms and mandatory checks including physical checks at the point of departure by

Petitioner Exhibit 1002-1151

Revenue/Customs officials, and the other that is based on the electronic capture of transaction data by static devices at a participating retailer's shop and the use of this data to perform a risk-based selection of transactions for physical checks at the point of departure by Revenue/Customs officials.

For example, in Singapore the GST paid for purchases at the shops can be refunded via an electronic Tourist Refund Scheme (eTRS). The eTRS scheme starts when a tourist makes a purchase at a participating retailer and shows his passport at the point of purchase to prove his eligibility. Some non-exhaustive examples of the criteria that the tourist must fulfill in order to be eligible for the GST tax refund include:

i. the tourist is not a Singapore citizen or permanent resident of Singapore;

ii. the tourist had not spent more than 365 days in Singapore in the past twenty-four (24) months before the date of purchase;

iii. the tourist has not been employed in Singapore at any time in the past six (6) months before the date of purchase;

iv. the tourist is sixteen (16) years old or above at the time of purchase; and

v. the tourist is not a crew member of any aircraft or international cruise departing Singapore.

When paying for the purchases, the tourist would typically utilize a credit/debit card. Information such as the sixteen-digit primary account number (PAN) related the credit/debit card may be used as an identifier or token for tagging the purchases entitled for refund. The participating retailer (merchant) may also issue a paper eTRS Ticket to the tourist. The eTRS Ticket can also be used as a token instead of the credit/debit card.

With this token, the tourist can apply for a GST refund at the eTRS self-help kiosk before checking in at an airport or other immigration departure points such as, but not limited to, an airport or a cruise centre. If approved, the eTRS self-help kiosk would generate a Notification Slip indicating "Approved". Depending on the mode of refund selected by the tourist, the tourist can

Petitioner Exhibit 1002-1152

obtain the refund (minus a service fee) by a direct credit into a designated refund account, such as credit card account, by a bank cheque or in cash at a central refund counter using the approved Notification Slip. If not approved, the eTRS self-help kiosk would generate a Notification Slip indicating that the refund is "Not Approved". The tourist then brings his purchases to the Customs counter for physical inspection. If the goods pass Customs inspection, a Customs officer would generate a Notification Slip indicating "Approved" to replace the "Not Approved" Notification Slip. During peak hours, these could become bottlenecks in processing the departing tourists as the customs counter is limited by manpower while the self-help kiosks may be overwhelmed by the number of tourists applying for refunds. Departing tourists typically have to arrive at the immigration departure points earlier to locate these static self-help kiosks in anticipation of a queue.

Further, in order to qualify for the GST refund in Singapore, the tourist must meet certain criteria. These criteria include spending at least S$100 (including GST) that can be accumulated in up to three (3) same-day invoices or receipts from retailers bearing the same GST registration number. Also, the tourist has to depart with the goods via the airport or cruise centre within a predetermined period, such as two (2) months from the date of purchase. The tourist must also depart with the goods within twelve (12) hours after obtaining approval of the GST refund. If the tourist is departing on an international cruise (excluding cruises-to-nowhere, round-trip cruise and regional ferry) from the cruise terminal, he must declare that he is exiting Singapore and will not return via the same voyage on the same ship, using his cruise itinerary as documentary proof of departure, and commit that he will not be returning to Singapore within forty-eight (48) hours. Further additional criteria may be imposed on student pass holders.

The authorities typically require that the purchases are verified against the invoices or receipts, and the goods are unused, unopened and exported out of the country and this is done at a counter either before check in (for goods that are to be checked in) or after immigration, to ensure that the goods are exported. However, the authorities at times do a targeted check instead.

Petitioner Exhibit 1002-1153

With the proliferation of mobile devices, it is common for tourists to travel with at least one personal mobile device that may be used to connect to the internet either via a wireless fidelity (Wi-Fi) networks or mobile telecommunications networks. Hence, it is envisaged that the functions of the mobile device, in particular smartphones, can be better utilized in allowing electronic tax refunds to be facilitated through the use of a dedicated software application residing on this mobile device together with its onboard camera, geo-location module, wireless communication module (Bluetooth and Wi-Fi), alarm notifications, internet connectivity etc.

The present invention seeks to provide a system and method that alleviates the above-mentioned drawbacks or meet the above needs at least in part.

SUMMARY OF THE INVENTION

Throughout the document, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Furthermore, throughout the specification, unless the context requires otherwise, the word "include" or variations such as "includes" or "including", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

The present invention seeks to meet the needs of a tax refund system that does not rely on self-help kiosks, and enables users such as tourists to access their tax refunds efficiently and accurately. The invention proposes a system and method of administration by way of an application software installable on mobile devices to verify user identity, facilitate a completely paperless tourist tax refund experience, and enable more types of transaction data to be captured for a more complete risk-based selection.

A technical problem the invention seeks to solve relates to the bottlenecks faced by customs at peak hour. Another technical problem is associated with

Petitioner Exhibit 1002-1154

the need to verify identities of tourists and transactions, such as purchases against the invoices and receipts in a more effective and efficient manner to reduce identity and transaction frauds.

The above and other problems are alleviated at least in part and an improvement in the art is made by a system in accordance with this invention. A first advantage of the system in accordance with this invention is that the tourist refund process is completely electronic, thereby eliminating the need to deal with paper refund tickets and paper receipts. A second advantage of the system in accordance with this invention is that the tourist is able to register in their own time and convenience on their mobile devices and after logging into the system, the tourist is able to view a consolidated list of all the refund claims they have made via the system, the additional spending required in order to fulfil the minimum spending requirement, as well as the amount of intermediate value accumulated and used. Such intermediate value may be translated into a form of 'rewards points' or the like. An associated third advantage of the system in accordance with this invention is that by having an intermediate value system (in the form of rewards point or the like) that is currency agnostic, there is no need to convert currencies. This mitigates any fluctuations in the exchange rates. Such an arrangement provides more certainty to the tourist in terms of the amount of tax refund obtainable, which can be spent even before the refund was actually approved. In accordance with an aspect of the invention there comprises a system for facilitating refund to a user comprising: a mobile device having means to communicate with a central processor for the generation of a refund account and a unique identifier; the unique identifier associated with the user; a computer device operable to access the unique identifier for verification upon receipt of a refund qualifying transaction associated with the user, the computer device further operable to receive and send information relating to the refund qualifying transaction and generate a refund request upon successful verification; and the central processor operable to be in data communication with the computer device to receive or send information relating to verification of the unique identification and the refund qualifying transaction and process

Petitioner Exhibit 1002-1155

the verification or refund request, the central processor further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

In some embodiments, the refund may be a tax refund, and be in the form of an intermediate value. The intermediate value may be derived from the actual value of refund based on a conversion rate.

In some embodiments, the computer device may be a point-of-sale device, such that the point-of-sale device may be configured to directly send information relating to the refund qualifying transaction to the central processor.

In some embodiments, the generated unique identifier may be encoded as a quick response (QR) code and the computer device accesses the unique identifier by scanning the QR code displayed on the mobile device.

In some embodiments, the central processor may be operable to send the electronic ticket to a third party server for further verification of the refund qualifying transaction and confirmation of the refund.

In some embodiments, the central processor stores the information relating to the refund qualifying transaction in a database before the electronic ticket is generated and sent to the third party server.

In some embodiments, the mobile device may be operable to send an electronic notification related to a requirement being met. The requirement may be a confirmation of departure, or a Declaration of Eligibility.

In some embodiments, the mobile device may be operable to receive a notification of refund issued by a third party server once the electronic ticket is processed successfully.

Petitioner Exhibit 1002-1156

In some embodiments, the central processor is operable to receive a notification of refund issued by a third party server once the at least one electronic ticket is processed successfully and the central processor is operable to send a notification of refund to the mobile device.

In some embodiments, the unique identifier associated with the user is generated based on a passport information of the user.

In some embodiments, the unique identifier is generated after a registration process.

In some embodiments, the unique identifier is further associated with an image capture of the passport.

In some embodiments, the mobile device is integrated with the computing device.

In some embodiments, the central processor is operable to send a notification to the mobile device indicating the success or failure of the refund request.

In some embodiments, there comprises another unique identifier associated with a retailer using the computer device.

In some embodiments, the another unique identifier is generated after a registration process by the retailer.

In some embodiments, the another unique identifier is further associated with an image capture of one or more account information associated with the retailer.

In some embodiments, if the unique identifier is not accessible by the computer device, the computer device is operable to obtain an alternative identifier for verification and send the alternative identifier to the central

Petitioner Exhibit 1002-1157

processor.

In some embodiments, upon receipt of the alternative identifier, the central processor is operable to determine whether a corresponding refund account associated with the user is present and if not, the central processor is operable to generate the refund account and the unique identifier based on the alternative identifier.

In some embodiments, the central processor comprises or is in data communication with a database for storing at least one retailer list of goods and services eligible for tax refund.

In some embodiments, the central processor is operable to receive a wish-list of goods and services from the mobile device and upon receipt of the wish-list, compare the wish-list with the at least one retailer list of goods and services.

In some embodiments, when there is a match between the wish-list and the at least one retailer list, the central processor is operable to provide a matched list to the mobile device.

In some embodiments, where the electronic ticket is a provisional electronic ticket, the provisional electronic ticket comprises a plurality of electronic receipts.

In some embodiments, the provisional electronic ticket is converted to a final electronic ticket at an approved departure point.

In some embodiments, the central processor arranged in data communication with at least one third party server to retrieve information related to the identity of the user, and sends the information related to the identity of the user to the computer device.

Petitioner Exhibit 1002-1158

In some embodiments, if the refund request is not successfully processed, the central processor is arranged in data communication with another computer device provided to an authorized personnel to perform further processing.

In accordance with another aspect of the invention there is a method for facilitating a refund to a user comprising the steps of: communicating via a mobile device with a central processor for the generation of a refund account and a unique identifier, the unique identifier associated with the user; via a computer device, accessing the unique identifier for verification on receipt of a refund qualifying transaction associated with the user; generating a refund request upon successful verification; sending information relating to the refund qualifying transaction via a central processor; receiving and processing the refund request; wherein the central processor is further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

In some embodiments, the method further includes the step of converting the refund to an intermediate value after the generation of the refund.

In some embodiments, the intermediate value is derived from the actual value of refund based on a conversion rate.

In some embodiments, the method further comprises the step of exporting the information relating to the refund qualifying transaction via a point-of-sale (POS) device in data communication with the computer device, the point-of-sale device is configured to directly send information relating to the refund qualifying transaction to the central processor.

In some embodiments, the computer device accesses the unique identifier by scanning an image shown on the mobile device.

In some embodiments, the method further comprises the step of sending the electronic ticket to a government server for further verification of the refund

Petitioner Exhibit 1002-1159

qualifying transaction and confirmation of the refund.

In some embodiments, the mobile device is operable to send an electronic notification related to a requirement being met. The requirement may be a confirmation of departure. The requirement may alternatively, or in conjunction, be a Declaration of Eligibility.

In some embodiments, the generation of electronic ticket is based upon one or more requirements being met.

In some embodiments, the method further comprises a step of sending an electronic notification to the mobile device indicating the success or failure of the refund request.

In some embodiments, the method further comprises a step of obtaining an alternative identifier for verification and sending the alternative identifier to the central processor if the unique identifier is not accessible by the computer device.

In some embodiments, upon receipt of the alternative identifier, the central processor is operable to determine whether a corresponding refund account associated with the user is present and if not, the central processor is operable to generate the refund account and the unique identifier based on the alternative identifier.

In some embodiments, the central processor comprises a database for storing at least one retailer list of goods eligible for tax refund.

In some embodiments, the central processor is operable to receive a wish-list of goods from the mobile device and upon receipt of the wish-list, compare the wish-list with the at least one retailer list of goods or services.

In some embodiments, when there is a match between the wish-list and the at

Petitioner Exhibit 1002-1160

least one retailer list, the central processor is operable to provide a matched list to the mobile device.

In some embodiments, the electronic ticket is a provisional electronic ticket, the provisional electronic ticket comprises a plurality of electronic receipts. The provisional electronic ticket may be converted to a final electronic ticket at an approved departure point.

In accordance with another aspect of the invention there is a non-transitory computer readable medium containing executable software instructions thereon wherein when executed on a mobile device and/or a computer device performs the method of facilitating a refund to a user comprising the steps of: communicating via the mobile device with a central processor for the generation of a refund account and a unique identifier, the unique identifier associated with the user; accessing the unique identifier for verification via a computer device on receipt of a refund qualifying transaction associated with the user; sending information relating to the refund qualifying transaction; generating a refund request upon successful verification; and receiving and processing the refund request by a central processor, wherein the central processor is further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

The non-transitory computer readable medium may further comprises a software instruction to send an electronic notification to the mobile device indicating the success or failure of the refund request.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is the overall architecture of an embodiment of the invention showing how the various parts of the system interact;

Petitioner Exhibit 1002-1161

Fig. 2 is a flowchart of an embodiment of the invention showing how a user is taken through the system when the application is launched;

Fig. 3 is a state machine diagram of an embodiment of the invention; and

Fig. 4 and Fig. 5 show how a single MDCC device may be used for the deployment of tourist refund in accordance with other embodiments of the invention.

Other arrangements of the invention are possible and, consequently, the accompanying drawing is not to be understood as superseding the generality of the preceding description of the invention.

PREFERRED EMBODIMENTS OF THE INVENTION

Particular embodiments of the present invention will now be described with reference to the accompanying drawings. The terminology used herein is for the purpose of describing particular embodiments only and is not intended to limit the scope of the present invention. Additionally, unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art to which this invention belongs.

In accordance with an embodiment of the present invention and with reference to Fig. 1, there is a system 10 for facilitating refunds. The refund may be in the form of tax refund provided to a tourist and will be described in such a context. It is to be appreciated that the system 10 may be adapted for other types of refunds and not limited to a tax refund. The term 'refunds' include refund in an electronic medium.

The system 10 comprises a central processor 110. Central processor 110 may be in the form of one or more processors and/or servers 110 belonging to an organisation administering the tourist refunds. An example of such an organisation is the Central Refund Agency (CRA). The CRA may be a private organisation, a government organisation, or a quasi-government organisation.

Petitioner Exhibit 1002-1162

The CRA may further be in data communication with a Central Clearing House (CCH) 170 for the purpose of settlement and crediting of refund value.

The one or more servers 110 can include a cloud server or a conventional server with data communications capability. For the ease of discussion, the one or more server will hereinafter be referred to as 'server' or 'servers'. Server 110 may be connected to one or more databases (not shown). Such database(s) are operable to contain records and information relating to the tourist refunds such as name, addresses and/or pre-generated or generated unique identifiers associated with the users seeking refunds. Server 110 is also operable to generate and update refund accounts for facilitating, processing and crediting refunds.

In one embodiment, the system 10 comprises a mobile device 120, preferably endowed with communications and computing capabilities and hereinafter referred to as MDCC 120, and computing device 130 (hereinafter referred to as 'Retailer Device' 130). The Retailer Device 130 can also be an MDCC or other computing device like a desktop/laptop computer. A Point-of-Sale (POS) device/system may be in data communication with the Retailer Device 130, the data communication in wired or wireless, remotely or otherwise. Alternatively, the POS device or its associated function may be incorporated/integrated with the Retailer device 130 as a module.

To facilitate the refund process, the mobile device 120 and computing device 130 may be installed with dedicated software applications (colloquially known as 'apps'). Such dedicated software applications may be operating system (OS) such as iOS™ or Android™ specific, and/or device specific.

The software application installable on mobile device 120 provides a user interface for user registration and for retrieving or providing information for the refund process. Once installed, the software application is operable to perform at least the following functions:-

a. receive registration details entered by the user;
b. communicate with the server 110 to send the registration details;
c. receive from the server 110 a unique identifier associated with the user (tourist);
d. receive from the server 110 information related to the refund process;

Petitioner Exhibit 1002-1163

e. display notifications/alerts on the MDCC 120 relating to refund process;
f. provide user interface for user to browse or view account details;
g. search for necessary communication networks for data communication with the server 110 and the computing device 130 (if necessary); and
h. store, organise and retrieve information received from various parties.

The MDCC 120 and the Retailer Device 130 can be any mobile electronic device(s) that can connect wirelessly to Wi-Fi networks or conventional telecommunications networks such as 2G, 3G, 4G, or LTE based networks. The mobile electronic devices include, but are not limited to mobile devices like smartphones, personal digital assistant (PDA) phones and tablets. The devices include mobile devices running on iOS platforms such as the iPhone and the iPad.

The invention will next be described in the context where a user of MDCC 120 (presumably a tourist) downloads a dedicated software application (hereinafter 'software application') onto the MDCC 120 for registration with the system 10; and usage of the MDCC 120 with the installed software application for facilitating refunds.

During the first usage after downloading the dedicated software application, a registration process is initiated where the tourist is prompted to register by entering his or her registration details into the application. The tourist may enter the necessary details for registration via manual entry or via imaging the identification documents associated with the tourist, if the MDCC 120 comprises an imaging device or module such as an on-board camera. The identification documents may include passport or other approved identification papers identifying the user as a tourist. In the case of a passport that comprises a machine readable zone (for example barcode), the MDCC 120 may also be used for reading the readable zone on the passport using the on-board camera or if the MDCC 120 is installed with the necessary hardware and/or software for doing the same.

The registration process can further integrate a verification of the authenticity of passports. The registration process can also include a check against records or entries in one or more authorized databases (for example government immigration records) to ascertain the eligibility of the tourist for a

Petitioner Exhibit 1002-1164

tax refund. Such authorized databases may be public or private databases. With these verifications, the tourist may not need to carry his passport in order for the retailer to verify his tourist status, subject to regulatory acceptance of such method of verifications.

Upon receiving the registration information, the MDCC 120 next sends the registration information to the server 110 for the creation of a user account. Once the user account is created, the server 110 then replies to the MDCC 120 with a unique identifier associated with the user account, for the tourist. The unique identifier can be in the form of an assigned account number and/or encoded into a QR or Quick Response code by the server 110 or software application installed on MDCC 120. The QR code is a type of matrix barcode that is machine readable and can contain information that can quickly be translated into usable data.

Once the unique identifier is generated, the unique identifier can be accessed on the same MDCC 120 used to register the user or on any other mobile devices 120 that is compatible with the form or physical medium that the unique identifier is encoded. In this regard, the unique identifier is therefore device agnostic. Other types of machine readable codes like barcodes can also be used in place of QR codes, although these may hold less data. This QR code is tied/tagged to each and every tax refund qualifying transaction made by the tourist.

It is to be appreciated that the unique identifier may include a simple account number, and/or a combination/hybrid of one or more of the above described codes.

Once registered and a user account is in place, the tourist user may then make tax refund qualifying transactions such as tax refund qualifying purchases at one or more participating retailers.

After the tax refund qualifying purchase is made at the participating retailer, the tourist retrieves his or her unique identifier, in the form of a QR code, for display on the MDCC 120. The participating retailer uses the Retailer Device 130 to scan the QR code (s140) for verification on the eligibility for a tax refund by checking against the server 110 to ascertain if the tourist has a

Petitioner Exhibit 1002-1165

registered account and is eligible for a refund. As an example, the check will include comparing and matching entries with the server 110 and/or its associated processor(s) or database(s) to determine if the passport is a foreign passport and if the tourist is at an age eligible for refund (e.g. 16 years or older). The server 110 can also perform a check against government immigration records via the government server 170 to ascertain the eligibility of the tourist for a tax refund. Alternative ways of unique identifier accessing technology or combinations may be used. Examples of such technologies may include Near Field Communications (NFC), Bluetooth, Wi-Fi, etc. as known to a skilled person. The identification may also be manually entered into the Retailer Device 130. Such a step of verification may include checking the physical passport and the passport information/details submitted, subject to compliance with the necessary regulatory requirements.

Upon scanning of the unique identifier, the participating retailer may enter the purchase/transaction details related to the purchase made by the tourist into the Retailer Device 130. The transaction details may be manually or automatically transmitted. In the latter, the transaction details may be transmitted automatically via a cable or wirelessly from a Point-of-Sale ("POS") system and/or POS device, the POS device configured to send the information relating to the refund qualifying transaction, i.e. purchase/transaction details to the Retailer Device 130 and/or server 110. For example, to facilitate the transmission, a software driver may be installed on the POS system for detecting the Retailer Device 130 as a printer, so that the POS device can print the transaction details to the Retailer Device 130. Alternatively, software may be installed on the POS device or system to capture the transaction details from a payment screen via an Optical Character Recognition (OCR) module. In the case of an Internet-enabled POS system or device, the purchase or transaction details can be directly transmitted to the server 110 via one or more wired or wireless communication means. The transaction details may then be accessible via a web resource locator or link, such as a Uniform Resource Locator (URL).

If a paper receipt is issued for the transaction, the Retailer Device 130 may also be used to image or scan the paper receipt associated with the

Petitioner Exhibit 1002-1166

transaction for the transaction details to be extracted by an image conversion and/or recognition module, such as, for example the OCR module. Once the retailer has verified the transaction details thus captured, he can transmit the transaction details to the server 110 via the Retailer Device 130. In another embodiment, the MDCC 120 may be used in place of the Retailer Device 130 to image or scan the paper receipt associated with the transaction. Once the retailer has verified the transaction details thus captured, he can present the tourist with a retailer identifier, which can be another QR code, unique to the retailer, for scanning by the MDCC 120, as a form of retailer confirmation/receipt.

In another embodiment, if a user is unable to present his unique identifier in the form of a QR code (for example because the user has not yet registered with the server 110), the retailer may scan an alternative identifier, such as but not limited to the Tourist's passport to retrieve his account information. The scanning device may be the Retailer Device 130 or in the form of a barcode scanner or other imaging device and once the passport has been scanned, the server 110 checks if the tourist has a registered account and eligible for a refund, e.g. if passport is a foreign passport and if tourist is at an age eligible for refund (e.g. 16 years or older). The server 110 can also perform a check against third party servers or databases, such as government immigration records via the government server 170 to ascertain the eligibility of the tourist for a tax refund. If the tourist is not eligible, the server 110 prompts an authorized personnel (e.g. a cashier) to inform the tourist that he is not eligible for tourist refund. If the tourist is eligible, the server 110 checks for an existing account by comparing the scanned details with one or more databases of the server 110. If a user account already exists, the app installed on the retailer device 130 is operable to display the user profile or details for validation by the cashier. If the tourist before the cashier matches the user profile, then the cashier confirms the user (customer) identity via a user interface and proceeds to enter receipt details. If a user account does not exist for the tourist, the server 110 creates a user account and the cashier proceeds to enter receipt details.

The Retailer Device 130 (or the MDCC 120) is operable to send the unique

Petitioner Exhibit 1002-1167

identifier, as well as the transaction details like the cost, the receipt number, the date and time of the transaction, etc. (see s150) to the server 110. No transaction details can be transmitted without the necessary information associated with the unique identifier (in the form of the QR code) on the MDCC 120 (or on the Retailer Device 130). To minimize fraud, the the Retailer Device 130 can be configured (by the retailer or otherwise) to halt all communications outside of the retailer's opening hours. This would prevent unauthorised tax refunds claims from being entered into the system. The security of the system 10 can be further enhanced by a password management system that requires the cashier to log into the retailer account and may require the password to be changed regularly. Sub-accounts may also be created for individual employees of the retailer who are responsible for collecting payment and their supervisors to create a system of checks-and-balances for approving unusual tax refund claims. Prior to use, the retailer account may undergo a similar registration process as described earlier for the user (tourist) account. In some embodiments, the registration process entails the server 110 assigning or issuing retailers with user identifiers (IDs) and passwords. A manager of the retailer may create sub-accounts. Alternatively the server 110 may assign subaccounts to the retailers, who in turn have administrative rights to manage the sub-accounts. Similar to the registration of the user account, another retailer unique identifier such as a QR code may be generated and assigned to each retailer who registers for an account to participate in the system.

Based on the details sent by the participating retailer, the server 110 sends an electronic ticket for the notification of transaction. Such a notification may be in the form of an eTRS Ticket (containing the details mandated by the Revenue/Customs authorities such as a documentary ID or DOC-ID that uniquely identifies the transaction) directly to the MDCC 120, thus recording the purchase as an eTRS Transaction. The server 110 would also notify the participating retailer via the dedicated software application installed on the Retailer Device 130 of the eTRS Ticket (see s150).

The MDCC 120 is operable to image, store and organise the purchase receipts and invoices issued by the participating retailer, and link these with

Petitioner Exhibit 1002-1168

the eTRS Transaction for ease of subsequent retrieval by the tourist or by an inspector of the Revenue/Customs authorities. The server 110 will transmit the transaction details as required by the Revenue/Customs authorities to a Central Clearing House (CCH) 170 for lodgement as an eTRS Transaction 180. In another embodiment of the present invention, the server 110 can also request the CCH 170 to perform an instance of risk assessment after each transaction, and communicate 180 the risk assessment results to the server 110. If the result is such that the tourist is selected to present his or her purchases for inspection by an officer of the Revenue/Customs authorities at the point of departure from the country, the server 110 would then notify the tourist of this requirement via the software application installed on the MDCC 120 either shortly after the transaction itself and/or at the point of departure from the country (s160). This early deterrence would assist to deter potential fraudsters from trying to obtain a tax refund through fraudulent means.

With additional tax refund qualifying purchases, multiple eTRS Tickets can be sent to the MDCC 120 in the same direct way (s160).

When the tourist is leaving the country, the MDCC 120 or the dedicated software application installed on the MDCC 120 would request for confirmation of departure from the tourist. Once the tourist confirms his departure from the country, the tourist can request for a refund together with a Declaration of Eligibility (a requirement by the Singapore Revenue/Customs authorities) or other declarations as required by the Revenue/Customs authorities (s160). The tourist may be guided through the Declaration of Eligibility process by the application on the MDCC 120, which also displays the passport details of the tourist for his or her confirmation as the person making the Declaration. Purchases recorded as eTRS Transactions are also displayed for the tourist to select those for which he or she would like to submit a claim for tax refund. For those tax refundable purchases made through retailers that do not operate the application, the application on MDCC 120 can scan the paper copy of the eTRS Tickets issued by these retailers so that all the transactions are consolidated. Alternatively, the CCH 170 can also transmit electronically, the details contained in the paper eTRS Tickets, to MDCC 120, upon request by the MDCC 120 or the dedicated software

Petitioner Exhibit 1002-1169

application installed on the MDCC 120. The tourist would also confirm the preferred refund option – whether in cash or credited back to a credit/debit card or a bank account or even an electronic wallet account – and the application guides the tourist to confirm the relevant details accordingly. The preferred refund option and details may have already been entered at the point of user registration, otherwise the tourist will be prompted to do so. The tourist may also enter the necessary details via manual entry or via imaging the credit card via the on-board camera on MDCC 120, for example.

Once the various fields are completed, the application can allow the tourist to confirm the details one last time before submitting them to the server 110.

In addition to the tourist proactively initiating a request for refund, one way of reminding the tourist to submit the request for refund would be to use a location-based service, such as Global Positioning System (GPS), geo-fencing, navigation systems etc, to alert the MDCC 120 when the MDCC 120 is detected within range of a departure point installed with a location-based service device, examples of such departure points including an airport or a cruise centre. This would notify and remind the tourist to submit the request for refund. Alternatively, the application on the tourist MDCC 120 can also rely on Wi-Fi networks or cellular base stations at the airport and the cruise centre to remind the tourist when the MDCC 120 accesses these networks. Alternatively, the MDCC 120 can detect transmitters (including but not limited to Bluetooth Low Energy beacons) located at a departure point, such as an airport or a cruise centre, and trigger the application to remind the tourist. This saves the tourist the trouble of having to arrive at the airport early to locate the eTRS self-help kiosk, since the tourist can now submit the request using his or her MDCC 120.

Once the request for refund is submitted (s160) to the server 110, the CCH 170 is notified via s180 and can communicate to the server 110 as to whether the tourist has been selected for inspection by the Revenue/Customs authorities and the server 110 notifies the tourist via the MDCC 120 accordingly (s160).

Petitioner Exhibit 1002-1170

For tourists who have not been selected for inspection, they would receive a digitised Notification of Approval slip on their MDCC 120. Those who have not received a notification of approval slip and/or have been selected for inspection either at any point of purchase or after the submission of the request for refund would receive a digitised Notification of Inspection slip prompting them to proceed to a counter of the Revenue/Customs authorities for further processing. There, upon presenting the digitised eTRS tickets, invoices/receipts and notification slips stored on the tourists' MDCC 120 together with the goods purchased, passport and plane ticket, as required, an authorized personnel such as the Revenue/Customs officer or inspector updates the record stored at the CCH 170. This may be performed via a separate computing device provided to the customs officer having a dedicated software application installed thereon and arranged in data communication with the server 110 to interact with the server 110. In some embodiments, a 'customs officer' identifier in the form of a QR Code may be provided to the customs inspector to present to the tourist after the customs inspector is satisfied with the eligibility of the tourist and the purchases for a refund. Upon scanning of the QR Code, the server 110 then updates the CCH record as "Approved" and issues a Notification of Approval slip.

This Notification of approval may be in paper, or digitised and sent to their MDCC 120.

Cash refunds would be made at a Central Refund Counter (CRC) upon presentation of the Notification of Approval slips, otherwise the monies would be credited to their credit/debit card or bank account as previously indicated, or any payment platforms (e.g. Alipay™, Paypal™) for facilitating the transfer of refund monies to one or more user accounts. The tourists would then proceed to depart Singapore accordingly.

In some embodiments, instead of a cash refund, the refund value may be converted to an intermediate value. Examples of such intermediate value may be coupons, credits, points, or other electronic value etc. One embodiment of

Petitioner Exhibit 1002-1171

an intermediate value is in the form of 'rewards points'. Such a system of rewards points can also be implemented into the tourist refund process, where the rewards points can be applied towards the purchase of goods and services at participating retailers. Retailers participating in this system of rewards points can be the same ones that are accredited under the tourist refund scheme or retailers that are not accredited but can also be equipped with a Retailer Device 130. Tourists can accumulate rewards points issued by the CRA. In the conversion of tax refund to rewards points, the system may refund the full amount, less than or more than the full amount of tax levied depending on the conversion rate between the tax refund to rewards point, instead of withholding a service fee as in the traditional method, although a service fee can still be offered as an alternative. The system can offer the tourist the option to take the refund in the form of tourist refund (whether as cash or via a credit/debit card) or in the form of rewards points, by way of a prompt either at the point of purchase or at the point of departure from the country. The tourist could even be allowed to convert the tourist refund into rewards points (vice versa) at any point in time, with or without a conversion fee. There may be a point in time where the availability of a tourist refund by way of cash or credit card is reduced or even removed. The rewards points can also be tagged with an expiry date, such that they expire if not used within a certain period of time, or the rewards points may be issued without an expiry date.

With reference to Fig. 2, an embodiment of a process for facilitating a tourist refund, wherein like numerals reference like parts, is described. The process begins when the dedicated software application installed on MDCC 120 is launched (step 210). The process begins with checking whether the tourist is already registered or is a new unregistered user (step 220). If the tourist is not registered, the tourist is walked through with a registration procedure (step 230) where an electronic user account is created with the server 110 and the relevant details are captured by the dedicated software application. Backend, the system 10 performs checks against the details like the passport number, nationality, name and/or other relevant information to ensure duplicate records

Petitioner Exhibit 1002-1172

are not created. The system can also verify the authenticity of the passports based on their security features or the server 110 may be linked with one or more third party servers. These third party servers may be private, public or government databases for the checking of stolen passports, as well as checking for other eligibility criteria such as whether the user is in fact a Permanent Resident of a particular jurisdiction and does not fall under the category of 'tourist', therefore ineligible for tourist refund; or whether the user has entered Singapore on a visit pass that may not strictly fall under a 'tourist pass', such as a student pass, etc. whereupon additional criteria have to be fulfilled. For each user account, a unique identifier like a QR code is created and stored by the application, or created by the server 110 and stored by the application. This process can be integrated with the onboard camera of the mobile device 120 to scan the machine readable zone of the passport to populate the various details or even to scan the passport itself with optical character recognition, or else manual entry of the details is used. The tourist is also given the option of imaging the passport, guiding him through the process of which page to capture, so that he does not have to carry a physical passport when shopping to claim a refund.

At a participating shop, the tourist makes a purchase and the retailer enters or scans the relevant details into the point-of-sale (POS) machine (step 240). After verifying that the purchases qualify for refund and the eligibility of the tourist by checking the tourist's passport, the retailer scans the unique identifier being displayed on the user MDCC 120 by either using the issued retailer device or the retailer's own mobile device with the application installed (step 250). One method of verifying the status of the tourist would be verification upon scanning the unique identifier or QR code via an onboard camera (where available) if the retailer is using a mobile device as the retailer device 130, whereby upon receipt of the scanned information (which includes the unique identifier), the server 110 would inform the retailer device whether the user is a tourist or not, which dispenses with the need to check the physical passport. The details of the transaction are then sent to the central server 110 or a processor belonging to the central refund agency (CRA) (step

Petitioner Exhibit 1002-1173

260), and this may be further sent to CCH 170. Once verified and the records updated, confirmation of the transaction is sent (step 270) together to the retailer and an eTRS Ticket is sent to the tourist either in the application, by email or any other forms of messaging. An electronic image or document of the invoice or receipt issued by the retailer can also be stored in the mobile application for later retrieval.

With some newer POS machines, the purchase details can be transmitted to the retailer device, either wirelessly via Wi-Fi or Bluetooth, or by a cable like a USB or similar, which speeds up the process and reduces the possibility of human error. The purchase details can even be directly transmitted to the server 110 in the form of a central processor. The added security measure of requiring the unique identifier before transmitting means the possibility of non-genuine tourist transactions is reduced. The tourist or the retailer may also use his or her mobile device to image the paper receipt associated with the transaction for the transaction details to be extracted by Optical Character Recognition. The retailer may also be equipped with other devices with imaging or scanning capabilities. Where the details are captured by the tourist's device, once the retailer has verified the transaction details thus captured, he can present the tourist with an identifier, which can be another QR code, unique to the retailer, for scanning by the tourist's device, as a form of retailer confirmation.

The application (and server 110) is also able to track the fulfilment of certain jurisdictional requirements where the purchases made by the tourist are submitted to the server are logged into the system. This feature is available where the tourist images receipts and enters the necessary details relating to the transactions he made. For example, in Singapore in order to qualify for a tax refund, a minimum $100 must be spent from retailers bearing the same GST registration number and this can be accumulated in up to 3 same-day invoices or receipt, thus the application can immediately alert the user, whether tourist or retailer, if this minimum amount has been reached on the same day. This does away with the current need to check physical receipts

Petitioner Exhibit 1002-1174

and sum them up.

An additional feature of using a system of intermediate value in the form of rewards points as described in the earlier embodiment can be incorporated into the process. During the purchase (step 240), the tourist informs the retailer that he wishes to use his rewards points, and upon scanning the QR code on the tourist's MDCC (step 250), the rewards points balance is retrieved from the server and displayed to the retailer. Based on this amount and confirmation from the tourist via the tourist's MDCC (step 250) of the number of rewards points to redeem, the retailer would apply the rewards points against the purchase price accordingly and update the server (step 260). In another embodiment, during a purchase (step 240), the tourist who wishes to utilize his intermediate value in the form of rewards points may launch the software application installed on the MDCC 120 to retrieve from the server and display the rewards points balance information. The tourist can inform the retailer of his intention to use his rewards points and scan an identifier, which can be another QR code, unique to the retailer before entering and confirming the number of rewards points he wishes to use, for transmission to the server. The server can then push the number of rewards points to be thus used for display on the issued retailer device or the retailer's own mobile device with the application installed, and the retailer would apply the rewards points against the purchase price accordingly and update the server (step 260). Upon receipt of the eTRS Ticket in the application, the tourist can be prompted to choose whether to convert the amount, with or without a service charge to the CRA, into the rewards points. This raises the possibility of the tourist being able to spend his tourist refund at participating retailers even before leaving the country.

A flowchart shown in Fig. 3 describes an embodiment of how the tax refund is credited/made to the tourist when the tourist is departing the country. At a departing point such as the airport or cruise centre, the installed application on the MDCC 120 is launched by the tourist either on his own volition or reminded by notifications displayed on the mobile device 120. Such

Petitioner Exhibit 1002-1175

notifications can be triggered by detecting that the tourist is at a departure point such as the airport or cruise centre. The tourist is then prompted to confirm that he is departing the country (step 310), which triggers the system 10 (either via the installed software application or the server 110) to notify the tourist of the purchases made to date, the eTRS Tickets collected, the amount of refund available, as well as the amount of outstanding refunds which may be in the form of an intermediate value as described. The tourist also indicates how the refund is to be made, either in cash or to the credit card account that was used (based on the purchase or transaction details), or to a specified bank account or even to another different credit card account. A further prompt whether to convert the refund available may be triggered to allow the tourist to do so.

Once the list of purchases is confirmed and verified by the tourist, the tourist is guided through the various steps of completing the Declaration of Eligibility and displays the tourist's passport details for confirmation. After confirmation, the declaration of eligibility and refund claims are submitted to the server (step 320) and to the CCH and confirmation is sent to the tourist (step 330), together with either an approval Notification slip or an inspection Notification slip if the tourist has been selected for inspection. If the inspection is verified and cleared, an approval Notification slip is issued to the tourist, and based on the approval Notification slip, a refund can be obtained (step 340) either in cash at the Cash Refund Counter at the airport or cruise centre, or credited back to the specified credit/debit card or bank account. Alternatively, the tourist can also choose to obtain the refund in the form of an intermediate value such as the rewards points, especially if he plans to visit the country again sometime soon. The tourist then departs the country (step 350). The Declaration of Eligibility can be submitted together with the refund claims via the application on the mobile device, which means that process is simplified and the tourist can do so at their own convenience, e.g. while queuing to check in or clearing immigration or even in the transport on the way to the airport.

In another embodiment of the present invention and with reference to Fig. 4

Petitioner Exhibit 1002-1176

and 5, wherein like numerals reference like parts, the functions associated with the MDCC 120 and retailer device 130 may be integrated into a single MDCC device 420. Such an arrangement is advantageous in the sense that one single MDCC 420 may be utilized for the whole refund process. It is to be appreciated that either:-

the associated functions described for both mobile device 120 and computing device 130 as earlier described would have to be implemented on the MDCC 420, or

another dedicated software application incorporating essential functions for mobile device 120 and the computing device 130 would have to be installed on the MDCC 420.

In the single device arrangement, the participating retailer's premises may be equipped with a transmitter and/or receiver (including but not limited to Bluetooth Low Energy 'Bluetooth LE' beacons) 410 operable to transmit to/receive from a MDCC 420 (used interchangeably with the term 'single device') within range of the transmitter/receiver.

An example of the single device arrangement 400 is shown in Fig. 4. The arrangement 400 comprises one or more Bluetooth LE (BLE) beacons 410 installed within the retailer's shop at a designated location, such as around a cashier. The BLE beacons 410 can operate in a 'broadcast' or 'advertisement' mode to notify nearby devices of its presence via an address. The address follows a specific format, such as a predefined prefix, followed by a variable UUID, and a major, minor pair. When a user with the MDCC 420, such as a tourist is within the pre-determined range of the designated location, the MDCC 420 detects the BLE beacons 410 and prompts the user to launch his dedicated software application, or directly launches the software application without prompt once the BLE beacons 410 are detected, which can be programmed to inform the user that he is at a participating retailer based on matching and verifying the broadcast format of the BLE. The retailer specific information can then be displayed on the MDCC 420.

The user next shops and transacts at the retailer shop. Upon payment for the merchandise, the tourist requests for a tax refund. The cashier then requests

Petitioner Exhibit 1002-1177

the tourist to send the request for refund from his MDCC 420, together with the refund account number and BLE address to the server 110.

The server 110 opens a session between the user account and the retailer account. The tourist is prompted to scan the transaction receipt using the MDCC 420 via the OCR module as described in previous embodiments, or via other means including manual or POS system as described. Once scanned, the transaction details are displayed on the MDCC 420.

The tourist presents the transaction details to the cashier or other personnel authorized by the retailer. The cashier verifies the transaction details and presents a retailer identifier to the tourist. The retailer identifier may be a QR code. The retailer identifier encoded in the form of a QR code may further comprise one or more of the following information:-

i. Retailer's account number held with the server 110; and

ii. Sub-accounts created by the retailer for each authorized personnel (e.g. cashier).

The sub-accounts provide a means for identifying the cashier in case of suspected transaction activity(ies), such as collusion between cashier and tourist.

The tourist scans the retailer QR code and the software application transmits the same to the server 110 for verification.

Upon receipt of the information related to the retailer identifier, the server 110 matches the QR code with the BLE address to verify that the MDCC 420 is on site. Upon verification, the MDCC 420 transmits the transaction details to the server 110. The server 110 then runs checks on the transaction details. The checks may include (but not limited to) ensuring that the transaction details are current, i.e. with current date and time, and relate to the correct retailer.

Upon completion of the checks, the server 110 then sends the transaction details to the CCH 170. The CCH 170 then acknowledges the lodgement of the refund claim to the server 110. The server 110 generates the eTRS Ticket, assigns the DOC-ID and sends the same to MDCC 420.

With reference to Fig. 5, at the point of departure, such as an airport or cruise center, the location of the MDCC 420 is determined by the software application via GPS or other location-based services. Alternatively, the

Petitioner Exhibit 1002-1178

application on the tourist MDCC 120 can also rely on Wi-Fi networks or cellular base stations at the airport and the cruise centre for detecting the MDCC 420. Once detected, the software application guides the user through the declaration of eligibility as described earlier (see steps 310 to 350). Next the tourist confirms his departure and eligibility. The MDCC 420 then retrieves the transaction records from the server 110 for the tourist to select for refund. Once the user selects the transaction records, he is prompted to select the refund method (e.g. rewards points, direct credit into specified account etc.). Upon selection, the MDCC 420 sends the declaration of eligibility; selected refund transaction(s); and refund method to the server 110. The server 110 in turn transmits the information to the CCH 170. The CCH 170 then replies with an approval or non-approval Notification slip to the server 110, which in turn transmit the approval or non-approval Notification to the MDCC 420. If the refund is approved, the CCH 170 further instructs or informs the CRC 430 to process the refund.

Where the CCH 170 replies with the non-approval notification slip, in some embodiments the tourist may be directed to the customs officer or inspector as described in the earlier embodiment for further inspection. The customs officer may be provided with a separate computer device with a dedicated software application installed thereon to facilitate inspection by the customs officer. A 'customs officer approval' identifier in the form of a QR Code may be provided to the customs inspector to present to the tourist after the customs inspector is satisfied with the eligibility of the tourist. Upon scanning of the 'customs officer approval' QR Code, the server 110 then updates the CCH record as "Approved" and issues a Notification of Approval slip. If still not approved, the purchases will not be eligible for tax refunds.

During a purchase (step 240), the tourist who wishes to utilize his intermediate value in the form of rewards points can inform the retailer of his intention to use his rewards points. He may launch the software application installed on the MDCC 420 to retrieve from the server 110 his rewards points balance and enter and confirm the number of rewards points he wishes to use, before showing to the retailer for verification. Once the retailer has verified the

Petitioner Exhibit 1002-1179

number of rewards points to be used, he can present the tourist with a retailer identifier, which can be another QR code, unique to the retailer, for scanning by the single device 420 as a form of retailer confirmation, and the server will be updated (step 260). The retailer would apply the rewards points against the purchase price accordingly. Also, upon receipt of the eTRS Ticket in-app, the tourist can be prompted to choose whether to convert the amount, with or without a service charge to the server 110, into the rewards points. This raises the possibility of the tourist being able to spend his tourist refund at participating retailers even before leaving the country.

The single device arrangement is based on the use of a mobile device 420 and eliminates the need for a Retailer Device. Instead of issuing each retailer with a separate device, Bluetooth Low Energy (BLE) beacons (transmitters/receivers) can be placed in each retailer outlet, and each authorized personnel may access the retailer's identifier (which may be in the form of a QR code or otherwise) in a variety of ways. For example an authorized personnel such as a cashier at the retailer shop can be provided with a QR Code Staff Pass, or each retailer outlet can be provided with its own QR Code identifier. The BLE can ensure transactions only take place at participating shops and the QR Code Staff Pass or identifier acts as retailer acknowledgement that the cashier has done her checks. The BLE can also be used to push targeted retailing information to the tourist, e.g. discounts, advertisements, etc. It is to be appreciated that both the QR code and BLE may be utilized in the form of a two-layered check to ensure that the transactions take place within the retailer's shop or premise. Such a two-layered check reduces the risk of any collusion between a member of the retailer's staff and the tourist.

In some embodiments, the server 110 may be operating the system of intermediate value. In such an arrangement, the server 110 may comprise a predictive engine operable to predict which user refund account is likely to be fraudulent so as to be able to take pre-emptive action. Otherwise the system may compromise on account integrity. The predictive engine can be based on at least one criterion of user demographics (e.g. location, countries visited for a past predetermined time frame), transaction profile (e.g. value of

Petitioner Exhibit 1002-1180

transaction, type of goods, etc.), the type of identifier (e.g. credit card) used to register for a refund account, gender, nationality etc. Based on these criteria, an algorithm can be developed to run in the server 110 to pick out suspicious user accounts. For example, the predictive engine may attribute high risk weights to transactions exceeding certain value arising from certain countries. In some embodiments, in addition to identifying suspicious user accounts, the predictive engine may further be configured to data communicate and send selected details relating to the 'suspicious accounts' to the relevant authorities, which include the customs. The selected details are sent to the authorities for further follow up checks in order to provide a more targeted and focused check In other embodiments, the system 10 may refuse the registration of any requested refunds accounts deemed not to pass an initial security check based on one or more of the at least one criterion. In yet other embodiments, based on the profile identified by the predictive engine, selected users or tourists may be banned from purchasing certain tax free eligible items. In some embodiments, the predictive engine may be arranged in data communication with one or more database servers, such database servers for maintaining user information.

The above arrangements are advantageous in that more parameters for the selection of tourists for inspection are considered, compared to that considered by the CCH 170 currently. In addition, the selection performed at the servers 110 effectively provide an additional layer of check which is pre-emptive in nature, as compared to that currently done at the exit point(s) which is 'reactive'. In this regard, it is to be appreciated that the existing system performs selection at the end of a tourist's trip/visit which is deemed less efficient compared to selection performed before the tourist starts his trip. This is because based on the existing structure, the retailers would have already taken the trouble to process the eTRS transactions of a fraudster, only for the transactions to be subsequently found invalid (this is assuming the CCH is able to select the tourist for inspection) when the fraudster attempts to make a claim for a refund as he leaves the country. The above arrangements effectively prevent suspicious transactions from being performed by would-be

Petitioner Exhibit 1002-1181

fraudsters, saving time and effort for both the retailers as well as the Customs. In another embodiment, the server 110 is configured to link to at least one retailer for the provision of one or more retailer item list(s) available for sale and tax refund. In the app installed on the tourist's MDCC 120, a user interface may then be provided to the tourist which displays the retailer item list of available items for sale and/or tax refund for the tourist to view before the tourist arrives at the country and/or before he/she leaves the country. Once a wish list or checklist of selected items from a tourist is communicated to the server 110 via the app, the server 110 is operable to provide a list of retailer(s) and details of the retailers selling the one or more items, via a data push or pull mechanism that the tourist desire to purchase. The wish list and retailer list may be compared by any compare and match algorithm between the entries on the tourist's wish-list with what the retailers have to offer. The compare and match may be performed at the server 110 side or the app installed on the MDCC 120.

In the creation of the tourist's checklist, the tourist can record a plurality of parameters related to each item. Non-exhaustive examples of these parameters may include the item's name, category, quantity and recipient's name and insert short notes and images (such as pictures) related to each item. Newly created items can be added to a temporary 'pending list' which the tourist can check off to move the items to a completed list whenever a purchase is made. Interfaces for sorting the items in alphabetical or other order may also be provided to the user.

Each time the tourist creates a new item, the app is operable to retrieve a list of retailer(s) selling the item from the server 110, and then provide to the tourist, retailers that sell the item or related items. The tourist can download the names of the recommended retailers to add them to his shopping list (via an interface) or to access the retailer's profile on the app. Through the list and/or a BLE located at the retailer's outlet, the tourist can be notified by the server 110 via the app and/or the retailer that sells the item or related items whenever the tourist is near to the retailer's shop and/or send content e.g. sales voucher from the retailer to the Tourist. This is advantageous to provide

Petitioner Exhibit 1002-1182

a seamless experience for the tourist and to aid the retailers in selling their products. Further, the arrangement provides an advantageous hybrid between a pure online shopping experience and a real shopping experience where goods can be inspected before it is purchased. Amongst other advantages, the above arrangement reduces the shopping time required for a tourist to look or source for an item and whether that item is eligible for tax refund; provides an alert or other forms of notification when the tourist is nearby a retailer; and provides an informed list on prices and quality before committing to the purchase.

In some embodiments, the server 110 is operable to issue one eTRS ticket for each refund claim at each retailer store and charge a service fee for each eTRS Ticket issued. Each eTRS Ticket may comprise more than one sales receipt accumulated at the same store (GSTN), subject to one or more regulations to meet a minimum threshold eligible for refund (e.g. SGD 100). For each eTRS ticket issued, the server 110 may also be required to pay a CCH Fee of SGD 1.50.

As an alternative embodiment, instead of issuing an electronic ticket in the form of an eTRS ticket for each transaction, the server 110 is instead operable to issue a provisional eTRS for the first transaction eligible for a refund claim, and add all subsequent transaction receipts to this provisional eTRS ticket. This is akin to a batch mode process and allows multiple retailers' transactions to be combined into a single formal/final eTRS ticket. The formal eTRS ticket will be issued only when the tourist is at an approved departure point. In such a way, both the user and the service provider may save on CCH Fees because only one Refund Ticket per user per trip is issued, instead of one Refund Ticket per user, per store, per trip. This can be performed without compromising on security or authenticity, as the tourist user will have to undergo the verification step at each retailer store.

In some embodiments, users of the system, such as approved retailers, may be provided with a user interface accessible to a portal, the user interface accessible via any computer device such as, but not limited to, a mobile device. The user interface may be used to display business information related to the retailer described as follow. An example of the interface is a

Petitioner Exhibit 1002-1183

webpage. The server will retrieve and store input received from various sensors such as Bluetooth LE beacons, image capturing devices located around the retailer's shop, for purpose of tracking, monitoring, obtaining, and/or deriving one or more parameters associated with the retailer. Examples of such one or more parameters include number of shoppers in a retailer shop. Such data may be provided on a real-time or near real-time basis displayed on the user interface. The data obtained may be further analyzed to provide business intelligence information useful for the retailer. Such business intelligence information may include shopper traffic in the retailer shop, busiest period of a weekday or weekend, busiest period over one or more months, etc.

In some embodiments, the system may be linked up with other commercial databases related to cruise ship services for example, to provide users with information such as Qualifying Cruise Ships eligible for tourist refund, as well as pre-populating travel itinerary to achieve certain level of convenience for the users of the system.

The described embodiments are advantageous as they provide a three-tier checking and verification process. In particular, a first level of check/verification is performed when a user (tourist) registers with the central processor 110. The second level of check/verification is performed before or during the generation of the eTRS ticket, and the third level of check/verification is performed at the point of departure prior to the generation of an electronic notification indicating the success or failure of the refund transaction.

Further, it is to be appreciated that the capturing of detailed information at the point of user registration allows a tourist to specify a desired account for refund upfront. Such an arrangement is useful to alleviate any time pressure that a tourist may face when he is leaving the country, as he needs to complete all form of formalities prior to boarding the aircraft / cruise ship. By shifting the data collection point to prior to the tourist embarking on his trip or

Petitioner Exhibit 1002-1184

at the point of registration, precious time is saved for the tourist when he faces the most time pressure.

The above is a description of embodiments of systems and methods for facilitating refunds, in particular tax refunds to tourists in accordance with the present invention. It is envisioned that those skilled in the art can design alternative embodiments of this invention that falls within the scope of the invention. In particular, it is to be appreciated that features from various embodiment(s) may be combined to form one or more additional embodiments. Further, the following are non-exhaustive examples of features that may be combined with the described embodiments to form further embodiments that falls within the scope of the invention:-

- In the single device embodiment, the user (tourist) may send both the retailer identifier and the transaction details to the server 110 for further processing upon scanning the retailer QR code. As a pre-requisite, the server 110 will however process the transaction details if and only if the retailer identifier is verified.
- The verification or scanning of the retailer's identifier may be performed either during the refund qualifying transaction is made or after. In the former case, the transaction details are captured before the retailer identifier is scanned before transmission to the server 110. This is particularly relevant for the single device embodiment. In the latter case, the retailer identifier may be verified or scanned for purpose of opening the transaction session before either the user or an authorized representative of the retailer retrieves the transaction details.

Petitioner Exhibit 1002-1185

WE CLAIM

1. A system for facilitating refund to a user comprising:

a mobile device having means to communicate with a central processor for the generation of a refund account and a unique identifier; the unique identifier associated with the user;

a computer device operable to access the unique identifier for verification upon receipt of a refund qualifying transaction associated with the user, the computer device further operable to receive and send information relating to the refund qualifying transaction and generate a refund request upon successful verification; and

the central processor operable to be in data communication with the computer device to receive or send information relating to verification of the unique identification and the refund qualifying transaction and process the verification or refund request, the central processor further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

2. The system according to claim 1, wherein the refund is a tax refund and in the form of an intermediate value.

3. The system according to claim 2, wherein the intermediate value is derived from the actual value of refund based on a conversion rate.

4. The system according to claim 1, wherein the computer device is a point-of-sale device, the point-of-sale device is configured to directly send information relating to the refund qualifying transaction to the central processor.

5. The system according to claim 1, wherein the unique identifier is encoded as a quick response (QR) code and the computer device accesses the unique identifier by scanning the QR code displayed on the mobile device.

Petitioner Exhibit 1002-1186

6. The system according to claim 1, wherein the central processor is operable to send the electronic ticket to a third party server for further verification of the refund qualifying transaction and confirmation of the refund.

7. The system according to claim 6, wherein the central processor stores the information relating to the refund qualifying transaction in a database before the electronic ticket is generated and sent to the third party server.

8. The system according to claim 1, wherein the mobile device is operable to send an electronic notification related to a requirement being met.

9. The system according to claim 8, wherein the requirement is a confirmation of departure.

10. The system according to claim 8, wherein the requirement is a Declaration of Eligibility.

11. The system according to claim 10, wherein the mobile device is operable to receive a notification of refund issued by a third party server once the electronic ticket is processed successfully.

12. The system according to claim 1, wherein the central processor is operable to receive a notification of refund issued by a third party server once the at least one electronic ticket is processed successfully and the central processor is operable to send a notification of refund to the mobile device.

13. The system according to claim 1, wherein the unique identifier associated with the user is generated based on a passport information of the user.

14. The system according to claim 13, wherein the unique identifier is generated after a registration process by the user.

Petitioner Exhibit 1002-1187

15. The system according to claim 13, wherein the unique identifier is further associated with an image capture of the passport.

16. The system according to any one of the preceding claims, wherein the mobile device is integrated with the computing device.

17. The system according to any one of the preceding claims, wherein the central processor is operable to send a notification to the mobile device indicating the success or failure of the refund request.

18. The system according to claim 1, wherein there comprises another unique identifier associated with a retailer using the computer device.

19. The system according to claim 18, wherein the another unique identifier is generated after a registration process by the retailer.

20. The system according to claim 18, wherein the another unique identifier is further associated with an image capture of one or more account information associated with the retailer.

21. The system according to claim 1, wherein if the unique identifier is not accessible by the computer device, the computer device is operable to obtain an alternative identifier for verification and send the alternative identifier to the central processor.

22. The system according to claim 21, wherein upon receipt of the alternative identifier, the central processor is operable to determine whether a corresponding refund account associated with the user is present and if not, the central processor is operable to generate the refund account and the unique identifier based on the alternative identifier.

23. The system according to claim 2, wherein the central processor comprises a database for storing at least one retailer list of goods and

Petitioner Exhibit 1002-1188

services eligible for tax refund.

24. The system according to claim 23, wherein the central processor is operable to receive a wish-list of goods and services from the mobile device and upon receipt of the wish-list, compare the wish-list with the at least one retailer list of goods and services.

25. The system according to claim 24, wherein when there is a match between the wish-list and the at least one retailer list, the central processor is operable to provide a matched list to the mobile device.

26. The system according to claim 1, wherein the electronic ticket is a provisional electronic ticket, the provisional electronic ticket comprises a plurality of electronic receipts.

27. The system according to claim 26, wherein the provisional electronic ticket is converted to a final electronic ticket at an approved departure point.

28. The system according to claim 1, the central processor arranged in data communication with at least one third party server to retrieve information related to the identity of the user, and sends the information related to the identity of the user to the computer device

29. A method for facilitating a refund to a user comprising the steps of:

communicating via a mobile device with a central processor for the generation of a refund account and a unique identifier, the unique identifier associated with the user;

via a computer device,

accessing the unique identifier for verification on receipt of a refund qualifying transaction associated with the user;

generating a refund request upon successful verification; and

sending information relating to the refund qualifying transaction

Petitioner Exhibit 1002-1189

via a central processor,

receiving and processing the refund request;,

wherein the central processor is further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

30. The method of claim 29, further including the step of converting the refund to an intermediate value after the generation of the refund.

31. The method of claim 30 wherein the intermediate value is derived from the actual value of refund based on a conversion rate.

32. The method of claim 29 further comprising the step of exporting the information relating to the refund qualifying transaction via a point-of-sale (POS) device in data communication with the computer device, the point-of-sale device is configured to directly send information relating to the refund qualifying transaction to the central processor.

33. The method of claim 29 wherein the computer device accesses the unique identifier by scanning an image shown on the mobile device.

34. The method according to claim 29, further comprising the step of sending the electronic ticket to a government server for further verification of the refund qualifying transaction and confirmation of the refund.

35. The method according to claim 34, wherein the mobile device is operable to send an electronic notification related to a requirement being met.

36. The method according to claim 35, wherein the requirement is a confirmation of departure.

37. The method according to claim 35, wherein the requirement is a Declaration of Eligibility.

Petitioner Exhibit 1002-1190

38. The method of claim 29 wherein the generation of electronic ticket is based upon one or more requirements being met.

39. The method of claim 35 further comprising the step of sending an electronic notification to the mobile device indicating the success or failure of the refund request.

40. The method according to claim 29, further comprises a step of obtaining an alternative identifier for verification and sending the alternative identifier to the central processor if the unique identifier is not accessible by the computer device.

41. The method according to claim 29, wherein upon receipt of the alternative identifier, the central processor is operable to determine whether a corresponding refund account associated with the user is present and if not, the central processor is operable to generate the refund account and the unique identifier based on the alternative identifier.

42. The method according to claim 29, wherein the central processor comprises a database for storing at least one retailer list of goods and services eligible for tax refund.

43. The method according to claim 31, wherein the central processor is operable to receive a wish-list of goods and services from the mobile device and upon receipt of the wish-list, compare the wish-list with the at least one retailer list of goods and services.

44. The method according to claim 32, wherein when there is a match between the wish-list and the at least one retailer list, the central processor is operable to provide a matched list to the mobile device.

45. The method according to claim 29, wherein the electronic ticket is a

Petitioner Exhibit 1002-1191

provisional electronic ticket, the provisional electronic ticket comprises a plurality of electronic receipts.

46. The method according to claim 45, wherein the provisional electronic ticket is converted to a final electronic ticket at an approved departure point.

47. A non-transitory computer readable medium containing executable software instructions thereon wherein when executed on a mobile device and/or a computer device performs the method of facilitating a refund to a user comprising the steps of:

communicating via the mobile device with a central processor for the generation of a refund account and a unique identifier, the unique identifier associated with the user;

accessing the unique identifier for verification via a computer device on receipt of a refund qualifying transaction associated with the user;

sending information relating to the refund qualifying transaction;

generating a refund request upon successful verification; and

receiving and processing the refund request by a central processor,

wherein the central processor is further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

48. The non-transitory computer readable medium according to claim 47, further comprising a software instruction to send an electronic notification to the mobile device indicating the success or failure of the refund request.

49. The system of claim 1, wherein if the refund request is not successfully processed, the central processor is arranged in data communication with another computer device provided to an authorized personnel to perform further processing.

Petitioner Exhibit 1002-1192

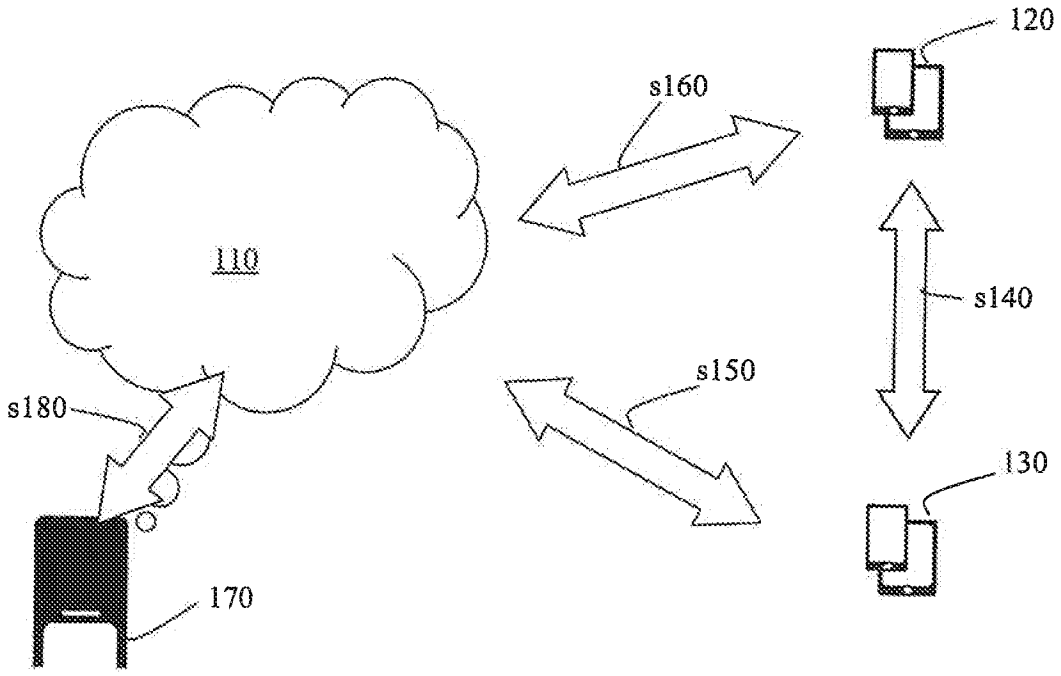


FIG. 1

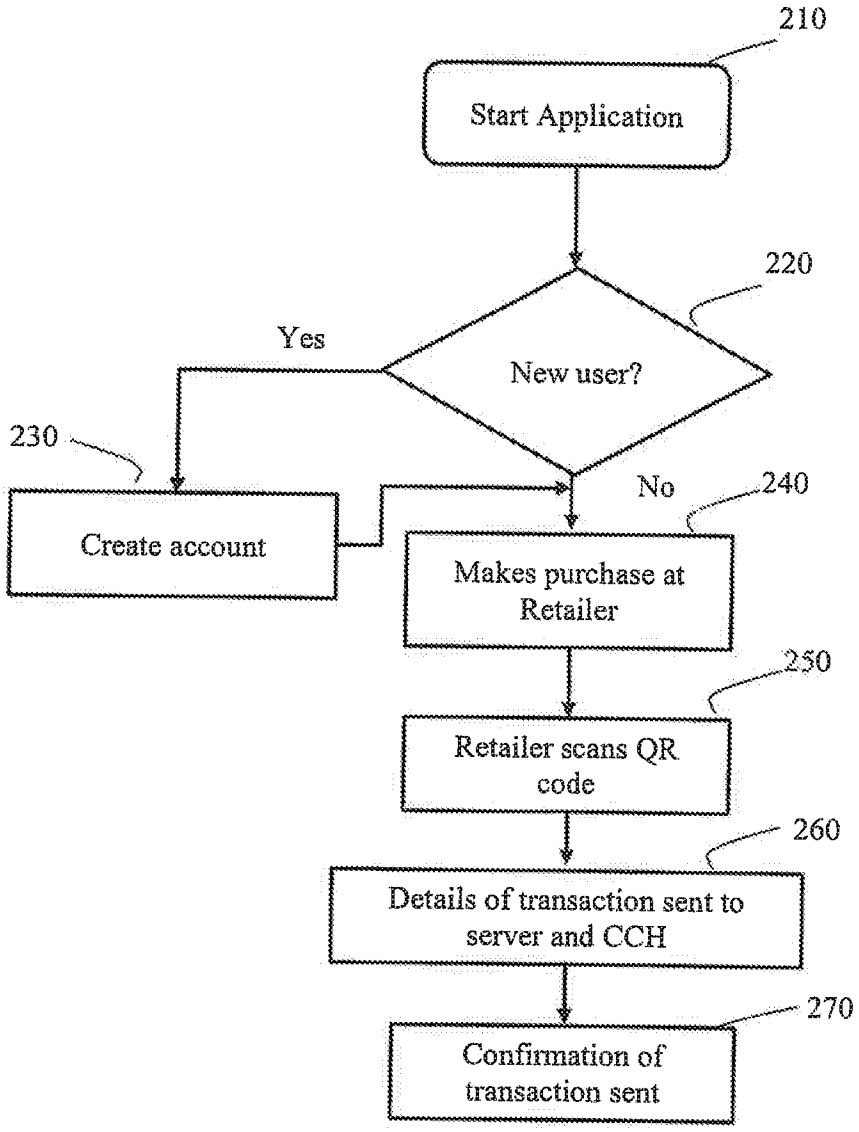

210
Start Application
220
New user?
Yes
No
230
Create account
240
Makes purchase at Retailer
250
Retailer scans QR code
260
Details of transaction sent to server and CCH
270
Confirmation of transaction sent

FIG. 2

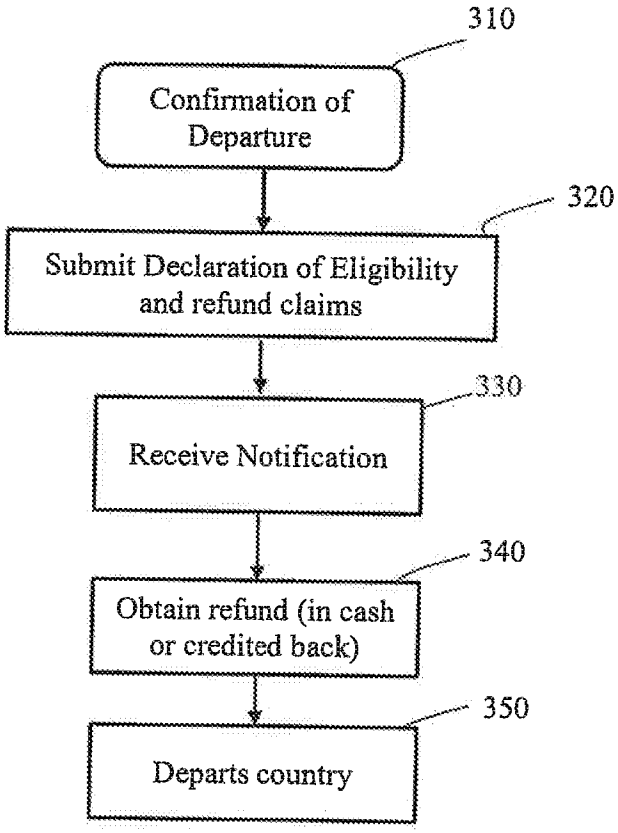

310
Confirmation of Departure
320
Submit Declaration of Eligibility and refund claims
330
Receive Notification
340
Obtain refund (in cash or credited back)
350
Departs country

FIG. 3

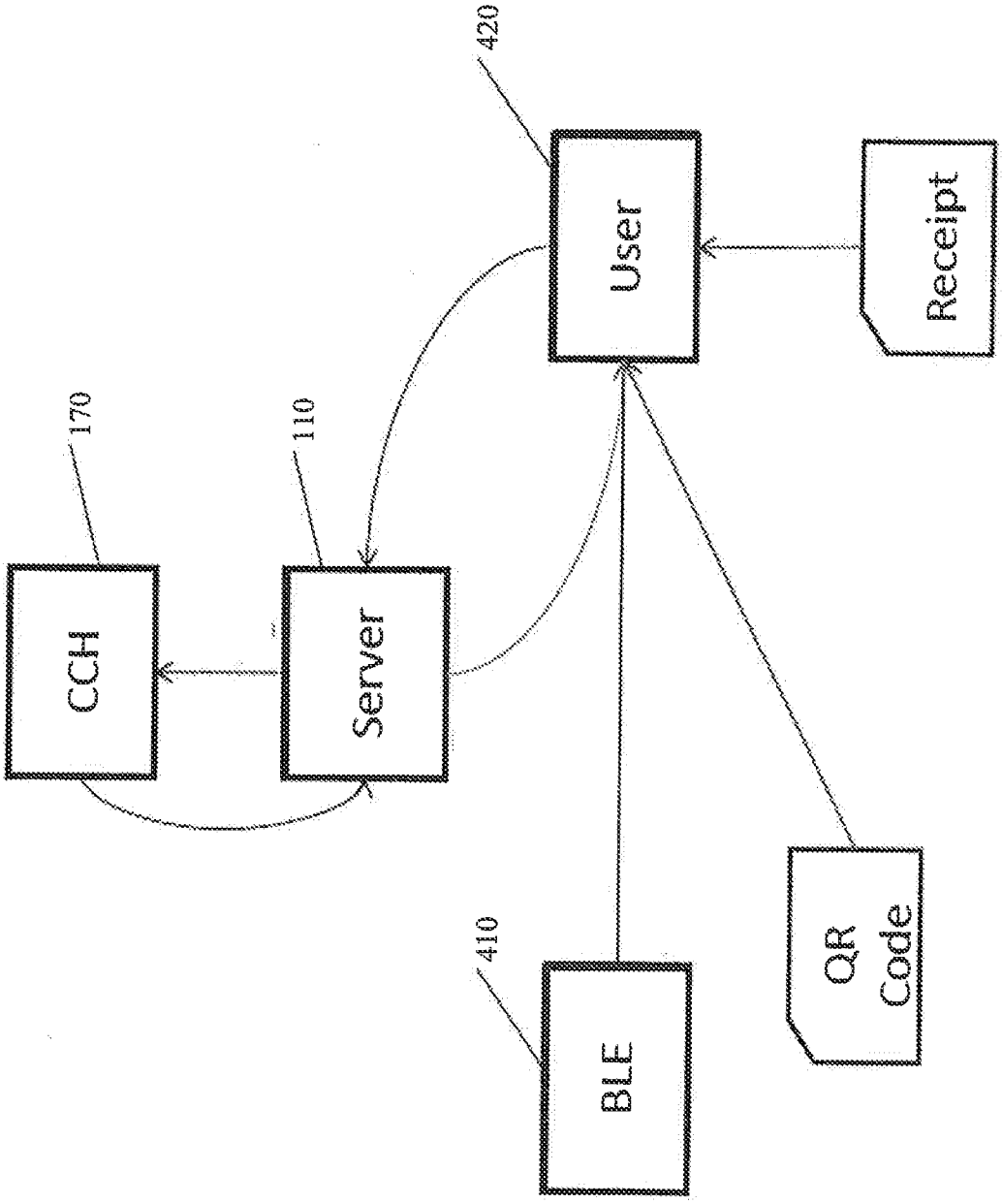


FIG. 4

Petitioner Exhibit 1002-1196

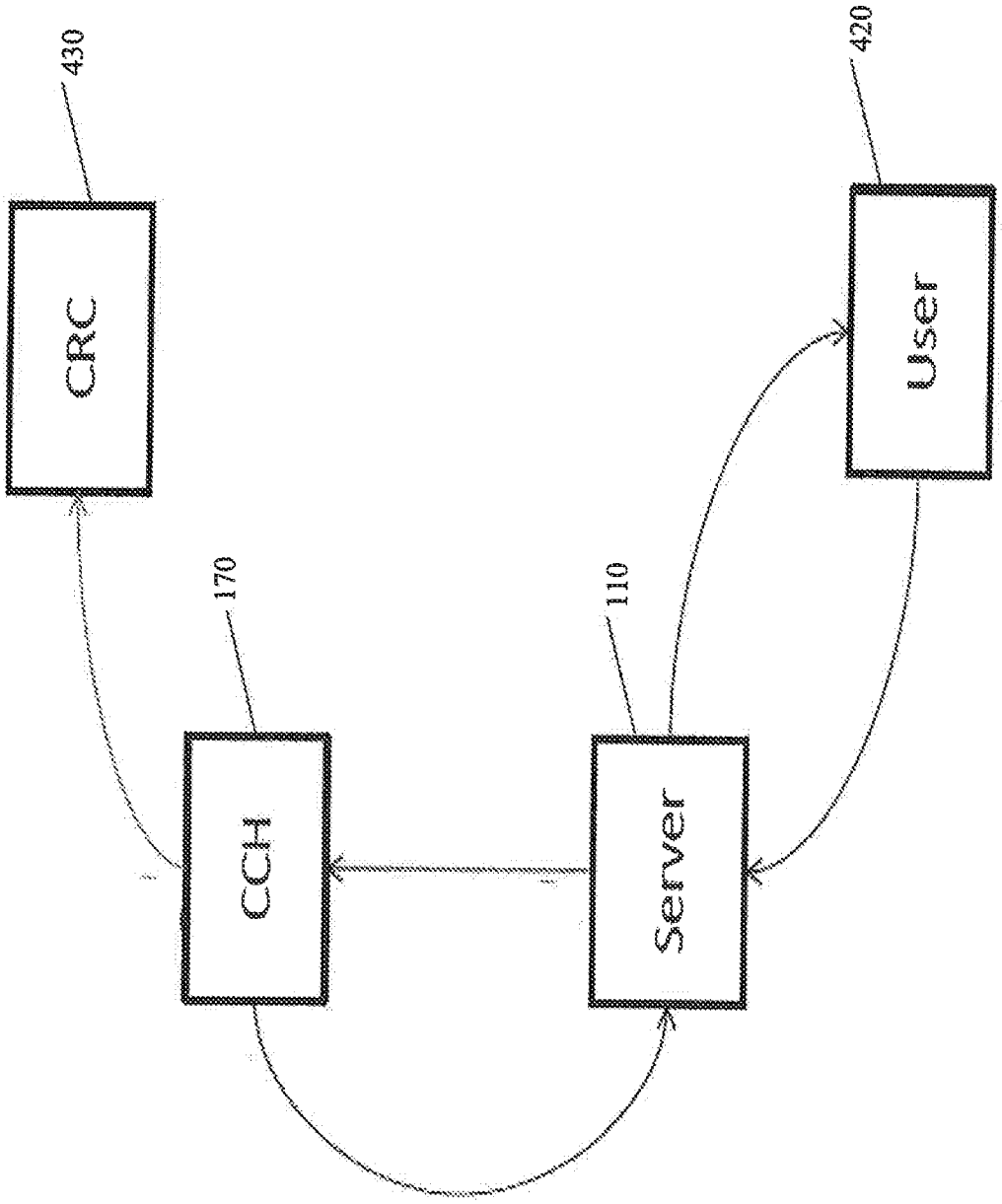


FIG. 5

Petitioner Exhibit 1002-1197

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2016/050297

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/32 (2012.01) ***G06Q 40/02 (2012.01)***

According to International Patent Classification (IPC)

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

FAMPAT: mobile device, smartphone, tax, VAT, GST, refund, rebate, reimbursement, electronic ticket, voucher, QR code and other related terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2014-0032089 A (KTIS CORPORATION) 14 March 2014 paragraphs [0001], [0025], [0068]-[0071], [0076], [0077], [0086]-[0088], [0113], [0114], [0124], [0125] of the machine translation	1-49
A	WO 2011/147912 A1 (GLOBAL BLUE HOLDINGS AB) 1 December 2011 paragraphs [0069], [00143], [00153]	-
A	US 2015/0127534 A1 (BHAMBHANI, M. M.) 7 May 2015 paragraph [0035]	-
A L	How VAT refund claim on purchases works. 6 July 2015 [Retrieved on 2016-09-28 from https://web.archive.org/web/20150706170705/http://www.optimal-tax-free.com/en/vat-refund/; for the purpose of establishing publication date of this citation] the whole document	-

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

*Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28/09/2016 *(day/month/year)*	30/09/2016 *(day/month/year)*

Name and mailing address of the ISA/SG

IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE

Intellectual Property Office of Singapore
51 Bras Basah Road
#01-01 Manulife Centre
Singapore 189554

Email: pct@ipos.gov.sg

Authorized officer

Lee Yi Chau

IPOS Customer Service Tel. No.: (+65) 6339 8616

Petitioner Exhibit 1002-1198

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG2016/050297

Note: This Annex lists known patent family members relating to the patent documents cited in this International Search Report. This Authority is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2014-0032089 A	14/03/2014	WO 2014/038775 A1	13/03/2014
WO 2011/147912 A1	01/12/2011	AU 2011257210 A1	06/12/2012
		AU 2011257210 B2	21/05/2015
		AU 2011257210 B8	11/06/2015
		EP 2577592 A1	10/04/2013
		EP 2577593 A1	10/04/2013
		EP 2577595 A1	10/04/2013
		EP 2577596 A1	20/04/2013
		GB 2480662 A	30/11/2011
		GB 2480664 A	30/11/2011
		JP 2013-527535 A	27/06/2013
		JP 5754751 B2	29/07/2015
		JP 2013-534653 A	05/09/2013
		JP 5791128 B2	07/10/2015
		KR 2013-0052577 A	22/05/2013
		KR 101560868 B1	15/10/2015
		KR 2013-0050943 A	16/05/2013
		KR 2015-0038708 A	08/04/2015
		SG 176401 A1	29/12/2011
		SG 176403 A1	29/12/2011
		SG 176405 A1	29/12/2011
		WO 2011/147913 A1	01/12/2011
		WO 2011/147914 A1	01/12/2011
		WO 2011/147918 A1	01/12/2011
US 2015/0127534 A1	07/05/2015	NONE	

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 August 2017 (24.08.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/143079 A1

(51) International Patent Classification:
G06Q 30/06 (2012.01) *G06Q 20/18* (2012.01)
G07F 7/00 (2006.01) *G06Q 20/20* (2012.01)
G06Q 20/16 (2012.01) *G06Q 20/32* (2012.01)

(21) International Application Number:
PCT/US2017/018194

(22) International Filing Date:
16 February 2017 (16.02.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/296,543 17 February 2016 (17.02.2016) US

(71) Applicant: **PAYRANGE, INC.** [US/US]; 919 SW Taylor, Suite 500, Portland, OR 97205 (US).

(72) Inventor: **PATEL, Paresh, K.**; 700 Ne Multnomah Street, Suite 1400, Portland, OR 97232 (US).

(74) Agents: **CRISMAN, Douglas, J.** et al.; Morgan Lewis & Bockius LLP, 1400 Page Mill Road, Palo Alto, CA 94304 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: SYSTEMS AND METHODS FOR DETERMINING ELECTRIC PULSES TO PROVIDE TO AN UNATTENDED MACHINE BASED ON REMOTELY-CONFIGURED OPTIONS

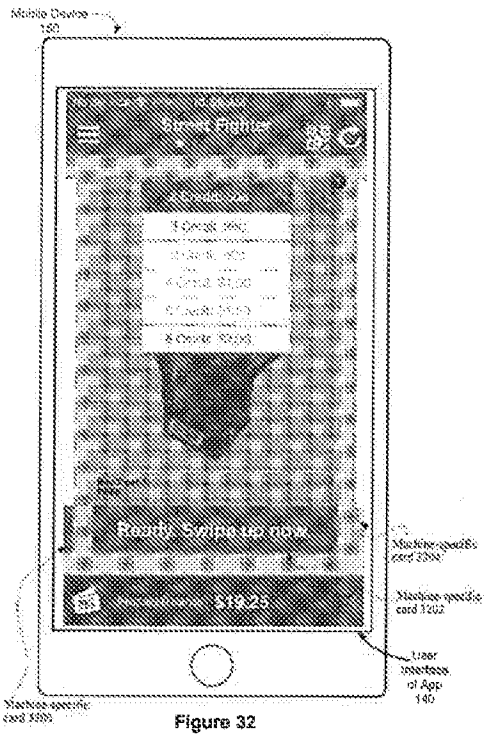


Figure 32

(57) Abstract: Disclosed herein are systems and methods for determining electric pulses to provide to an unattended machine based on remotely-configured options. An example method includes: detecting presence of the unattended machine in proximity to the mobile device. After detecting the presence, the method includes: receiving, from a server, information about a first set of remotely-configured options. In response to receiving the information about the first set of remotely-configured options, the method includes: displaying user interface objects that allow for selection of respective options in the first set of remotely-configured options. After detecting a selection of a first user interface object, receiving, from the server, specifications regarding electric pulses to be provided to the unattended machine by a pulse- providing device. After sending an authorization grant and the specifications to the pulse- providing device, the method includes: receiving an indication that the electric pulses were provided to the unattended machine according to the specifications.

WO 2017/143079 A1

Petitioner Exhibit 1002-1200

SYSTEMS AND METHODS FOR DETERMINING ELECTRIC PULSES TO PROVIDE TO AN UNATTENDED MACHINE BASED ON REMOTELY-CONFIGURED OPTIONS

FIELD OF THE INVENTION

[0001] The present application relates to the field of providing electric pulses at unattended machines, and in particular, to determining electric pulses to provide to an unattended machine based on remotely-configured options.

BACKGROUND OF THE INVENTION

[0002] Electric pulse-based credit machines are one type of "payment accepting unit" or "unattended machine" (unattended machines or payment accepting units are also referred to herein generically as "machines"). An unattended machine is equipment that requires payment for the dispensing of products (e.g., items stocked by a vending machine) and/or services (e.g., video game plays).

[0003] A consumer using an electric pulse-based credit machine such as a video game, kiddie ride, or coin-op laundry is restricted to a predefined default amount per payment increment as established by the machine (i.e., a direct mapping of coins that are inserted to credits validated by the machine). For example, if one credit allowed the user to play one game, the user would need to send 3 credits (i.e., insert 3 coins into the machine) if they wished to play three games.

[0004] Because the pricing options are predefined and physically programmed into the machine, machine operators are unable to offer up-front discounts, time-based discounts, or other options that allow the machine operators to flexibly control available pricing options. In addition, users are unable to take advantage of promotions and have to keep inserting coins into the unattended machines according to existing options.

SUMMARY

[0005] Disclosed herein are systems and methods that address the above deficiencies. In particular, disclosed herein are systems and methods for determining electric pulses to provide to an unattended machine based on remotely configured options. For example, a machine operator is able to access a web-based interface in order to add or modify pricing options for a particular unattended machine. When a user later receives an authorization grant for the particular unattended machine, that user is able to take advantage of the new or modified pricing options. In this way, machine operators can establish pricing schedules and

Petitioner Exhibit 1002-1201

users can take advantage of unique promotions offered by the machine operators. Additionally, users need not constantly add individual coins in order to access services provided by an unattended machine, instead the users can simply and easily take advantage of the unique promotions via an application that is executing on their own mobile phone (thus avoiding inefficiencies, such as lost coins, jammed coins, broken coin-accepting interfaces, and other like difficulties often encountered at unattended machines).

[0006] In addition to vending machines, other unattended machines include: parking meters, toll booths, laundromat washers and dryers, a video gaming console (i.e., a coin-operated arcade game), a coin-operated pool table, a coin-operated dart machine, a coin-operation vacuum or air pump (such as those commonly found at gas stations), or other offline-payment operated machines that dispense goods (e.g., products stocked by a vending machine) and/or provide services (e.g., allow a user to use the services, such as playing a video game, using the washer or dryer, etc.)

[0007] (A1) In one aspect, a method of determining electric pulses to provide to an unattended machine based on remotely-configured options for the unattended machine is provided. The method is performed at an application executing on a mobile device. The method includes: detecting, based on a broadcast received from a pulse-providing device that is coupled with the unattended machine, presence of the unattended machine in proximity to the mobile device. After detecting the presence of the unattended machine, the method includes: receiving, from a server (in some instances, the server is not capable of communicating directly with the unattended machine, because the unattended machine does not have a network connection), information about a first set of remotely-configured options for interacting with the unattended machine. In response to receiving the information about the first set of remotely-configured options, the method includes: displaying, in the application, user interface objects that allow for selection of respective options in the first set of remotely-configured options. The method further includes: detecting a selection of a first user interface object that corresponds to a first option in the first set of remotely-configured options. After (or in response to) detecting the selection of the first user interface object, the method includes: receiving, from the server, information that includes an authorization grant for the first option at the unattended machine, the information including specifications regarding electric pulses to be provided to the unattended machine by the pulse-providing device in accordance with the first option. In accordance with a determination that a trigger condition has been satisfied, the method includes: sending the information that includes the

Petitioner Exhibit 1002-1202

authorization grant and the specifications to the pulse-providing device. After sending the authorization grant and the pulse information to the pulse-providing device, receiving an indication, from the pulse-providing device, that the electric pulses were provided to the unattended machine according to the specifications.

[0008] (A2) In accordance with some implementations of the method of A1, the remotely-configured options are pricing options.

[0009] (A3) In accordance with some implementations of the method of any one of A1-A2, the remotely-configured options are pricing options that are determined according to a predefined pricing schedule.

[0010] (A4) In accordance with some implementations of the method of A3, the predefined pricing schedule is determined based on a current time of day at the server.

[0011] (A5) In accordance with some implementations of the method of any one of A1-A4, the remotely-configured options are configured by an operator of the unattended machine without requiring any physical interactions with the unattended machine.

[0012] (A6) In accordance with some implementations of the method of any one of A1-A5, the method further includes: receiving a second indication from the server that the remotely-configured options are no longer current; and in response to receiving the second indication from the server, receiving an updated set of remotely-configured pricing options that is distinct from the first set of remotely-configured pricing options.

[0013] (A7) In some implementations, a mobile device is also provided. The mobile device includes one or more processors and memory storing one or more programs to be executed by the one or more processors, the one or more programs including instructions for performing the method of any one of A1-A6.

[0014] (A8) In some implementations, a non-transitory computer readable storage medium is also provided. The non-transitory computer readable storage medium stores one or more programs, the one or more programs including instructions, which, when executed by a mobile device with one or more processors, cause the mobile device to perform the method of any one of A1-A6.

[0015] (A9) In some implementations an additional method is provided. The additional method is for determining electric pulses to provide to an unattended machine based on remotely-configured options for the unattended machine, and the method is performed at a pulse-providing device that is coupled with the unattended machine. The

Petitioner Exhibit 1002-1203

method includes: receiving, from an application executing on a mobile device, an authorization grant that includes specifications regarding electric pulses to be provided to the unattended machine by the pulse-providing device in accordance with a pricing option selected by a user at the application executing on the mobile device, wherein the pricing option is specific to the unattended machine. In response to receiving the authorization grant, the method includes: determining whether the authorization grant is valid. In accordance with a determination that the authorization grant is valid, the method includes: providing electric pulses to the unattended machine according to the specifications. After providing the electric pulses to the unattended machine, the method includes: sending, to the application executing on the mobile device, an indication that the electric pulses were provided to the unattended machine according to the specifications.

[0016] (A10) In some implementations of the method of A9, the pricing option is not available to users that interact with the unattended machine via mechanical insertion of coins.

[0017] (A11) In some implementations, a pulse-providing device is provided. The pulse-providing device includes: one or more processors and memory storing one or more programs to be executed by the one or more processors, the one or more programs including instructions for performing the method of any one of A9-A10.

[0018] (A12) In some implementations, a non-transitory computer readable storage medium is provided. The non-transitory computer readable storage medium stores one or more programs, the one or more programs including instructions, which, when executed by a pulse-providing device with one or more processors, cause the pulse-providing device to perform the method of any one of A9-A10.

[0019] (A13) Some implementations also provide for a system for determining electric pulses to provide to an unattended machine based on remotely-configured options for the unattended machine. The system includes: a pulse-providing device that is coupled with the unattended machine, wherein the pulse-providing device is configured to: perform operations described in the method of any one of A9-A10; an application that is executing on a mobile device, wherein the application is configured to: perform operations described in the method of any one of A1-A6; and a server that is in communication with the application that is executing on the mobile device, wherein the server is configured to: perform operations including retrieving specifications for electric pulses that are associated with selected pricing options and sending those retrieve specifications to the mobile device.

Petitioner Exhibit 1002-1204

[0020] In another aspect, a method of presenting representations of payment accepting unit events is performed at a device (e.g., the mobile device 150, Figures 5 and 21) with one or more processors, memory, one or more output devices, and two or more communication capabilities. After sending a request to a payment module (e.g., the adapter module 100, Figures 5 and 20), via a first communication capability (e.g., a short-range communication technology/protocol such as BLE), to initiate a transaction with a payment accepting unit (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120") associated with the payment module, the method includes obtaining a notification from the payment module via the first communication capability, where the notification indicates an event at the payment accepting unit associated with the payment module. In response to obtaining the notification, the method includes providing a representation of the notification to a user of the mobile device via the one or more output devices of the mobile device (e.g., a message displayed on a display of the mobile device, a vibration produced by a vibration mechanism of the mobile device, an aural alert produced by a speaker of the mobile device, and/or the like).

[0021] In one more aspect, a method of retrofitting an offline-payment operated machine to accept electronic payments is performed at a payment module (e.g., the adapter module 100, Figures 5 and 20) with one or more processors, memory, a short-range communication capability (e.g., a short-range communication technology/protocol such as BLE), and a first interface module configured to couple the payment module with a control unit of an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120"). The method includes receiving a transaction request via the short-range communication capability from a respective mobile device to perform a transaction with the offline-payment operated machine. The method includes validating the transaction request, where validation of the transaction request indicates that the respective mobile device is authorized to initiate payment for the transaction by a remote server (e.g., the server 130, Figures 5 and 22) via the long-range communication capability (e.g., the long-range communication technology/protocol such as GSM, CDMA, or Wi-Fi). In accordance with a determination that the transaction request is valid, the method includes causing the offline-payment operated machine to perform the requested transaction by issuing a signal to perform the transaction to the control unit of the offline-payment operated machine via the first interface module.

Petitioner Exhibit 1002-1205

[0022] In a further aspect, a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) includes one or more processors and memory storing one or more programs for execution by the one or more processors, the one or more programs include instructions for performing, or controlling performance of, the operations of any of the methods described herein. In some implementations, a non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) with one or more processors, cause the computer system to perform, or control performance of, the operations of any of the methods described herein. In some implementations, a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) includes means for performing, or controlling performance of, the operations of any of the methods described herein.

[0023] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] Figure 1 is a schematic diagram that shows three zones: a "communication zone" (e.g., Bluetooth range), an "authorization zone," and a "payment zone" in accordance with some implementations.

[0025] Figure 2 is a schematic diagram that shows the three zones of Figure 1 with multiple users therein in accordance with some implementations.

[0026] Figure 3 is a table that illustrates the hands-free credit or alert user principle in accordance with some implementations.

[0027] Figure 4 is a flow chart showing the logging received signal strength indicator (RSSI) information in accordance with some implementations.

Petitioner Exhibit 1002-1206

[0028] Figure 5 is a block schematic that shows elements of the payment processing system including, but not limited to, the adapter module, the machine, the mobile device, and servers, as well as communications therebetween in accordance with some implementations.

[0029] Figure 6 is a block schematic that shows three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or servers in accordance with some implementations.

[0030] Figure 7 is a block diagram that shows communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server in accordance with some implementations.

[0031] Figure 8A is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "communication zone" (e.g., Bluetooth range) in accordance with some implementations.

[0032] Figure 8B is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "authorization zone" in accordance with some implementations.

[0033] Figure 8C is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "payment zone" and, in particular, detailing a hands-free mode embodiment and a swipe mode embodiment in accordance with some implementations.

[0034] Figure 8D is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in a vending transaction including a loop for multiple transactions in accordance with some implementations.

[0035] Figure 8E is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in the login mode in accordance with some implementations.

[0036] Figure 8F is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending

Petitioner Exhibit 1002-1207

sequence, and purchase flow) during boot-up of the adapter module in accordance with some implementations.

[0037] Figure 8G is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) during an account check/update process in accordance with some implementations.

[0038] Figures 9A-9E are flow charts that show example steps and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in accordance with some implementations.

[0039] Figures 10A-10D show a mobile device with a graphical representation of a mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment processing system in accordance with some implementations.

[0040] Figure 11 is a perspective view of the in-line dongle adapter module in accordance with some implementations.

[0041] Figure 12 is a front plan view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0042] Figure 13 is a back plan view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0043] Figure 14 is a side view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0044] Figure 15 is a first end view of a connector receptacle of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0045] Figure 16 is a second end view of a connector receptacle of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0046] Figure 17 is a perspective view taken from the first end of the in-line dongle adapter module of Figure 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for illustrative purposes in accordance with some implementations.

[0047] Figure 18 is a perspective view taken from the second end of the in-line dongle adapter module of Figure 11, the connectors and cables between which the in-line

Petitioner Exhibit 1002-1208

dongle adapter module is inserted being shown in broken lines for illustrative purposes in accordance with some implementations.

[0048] Figure 19 is a perspective view of the in-line dongle adapter module of Figure 11 within a vending machine in accordance with some implementations.

[0049] Figure 20 is a block diagram of an adapter module in accordance with some implementations.

[0050] Figure 21 is a block diagram of a mobile device in accordance with some implementations.

[0051] Figure 22 is a block diagram of a server in accordance with some implementations.

[0052] Figure 23 is a schematic flow diagram of a process for authenticating a user to perform a transaction in the payment processing system in accordance with some implementations.

[0053] Figure 24A is a block diagram of a packet of information broadcast by the payment module (sometimes also herein called the "adapter module") in accordance with some implementations.

[0054] Figure 24B is a block diagram of an authorization request in accordance with some implementations.

[0055] Figure 24C is a block diagram of an authorization grant token in accordance with some implementations.

[0056] Figure 24D is a block diagram of transaction information generated by the payment module in accordance with some implementations.

[0057] Figure 25A illustrates a schematic flow diagram of a process for providing a representation of a machine event at a mobile device in accordance with some implementations

[0058] Figure 25B is a schematic flow diagram of a process for processing acknowledgment information in the payment processing system in accordance with some implementations.

[0059] Figures 26A-26D illustrate example user interfaces for providing a representation of a machine event at a mobile device in accordance with some implementations.

[0060] Figures 27A-27B illustrate a flowchart diagram of a method of presenting representations of payment accepting unit events in accordance with some implementations.

[0061] Figure 28A illustrates a block diagram of an offline-payment operated machine in accordance with some implementations.

[0062] Figure 28B illustrates signals sampled by the payment module in accordance with some implementations.

[0063] Figures 29A-29B illustrate a flowchart diagram of a method 1600 of retrofitting an offline-payment operated machine to accept electronic payments in accordance with some implementations.

[0064] Figure 30 illustrates a flowchart diagram of a method of enabling a payment operated machine to accept electronic payments in accordance with some implementations.

[0065] Figure 31 is a schematic flow diagram of a process for determining electric pulses to provide to an unattended machine based on remotely configured options for the unattended machine, in accordance with some implementations.

[0066] Figure 32 illustrates an example of a user interface on a mobile device that is used for selecting one of the remotely configured options for the unattended machine, in accordance with some implementations.

[0067] Figure 33 is a flow diagram of a method of determining electric pulses to provide to an unattended machine based on remotely configured options for the unattended machine, in accordance with some implementations.

[0068] Like reference numerals refer to corresponding parts throughout the several views of the drawings.

DETAILED DESCRIPTION OF THE INVENTION

[0069] Disclosed herein is a payment processing system or, more specifically, a mobile-device-to-machine payment processing system for processing transactions over a non-persistent network connection. The mobile-device-to-machine payment processing system disclosed herein focuses on the unattended retail space (e.g., a payment accepting unit 120, sometimes also herein called a "machine 120"). More specifically, the mobile-device-to-

Petitioner Exhibit 1002-1210

machine payment processing system disclosed herein allows a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0070] The mobile-device-to-machine payment processing system described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0071] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter module 100 (sometimes also herein called "payment module 100") such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit 120 (e.g., a vending machine) (sometimes also herein called 'the machine 120"). Installation is as simple as "powering down" (turning off) the machine 120, identifying the "wire" that connects with a payment receiving mechanism (e.g., the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial ("in-line") with the wire (e.g., connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter module 100 back into position, and "powering up" (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g., cash).

[0072] Non-persistent Network Connection: Although payment accepting units (or "machines") that accept only cash (e.g., paper currency and coins) may not require a connection (persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g., credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment

Petitioner Exhibit 1002-1211

accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no network connection is available, cashless payments is not possible. In addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, the mobile-device-to-machine payment processing system described herein minimizes (i.e., the manual mode) or eliminates (i.e., the hands-free mode) user interaction with the mobile device 150. Further, in some implementations, the mobile-device-to-machine payment processing system described herein facilitates the acceptance of cashless payments without requiring any network connection near the payment accepting unit 120. In some implementations, when the mobile-device-to-machine payment processing system described herein is located in a remote location where network connection is unavailable, the mobile-device-to-machine payment processing system, therefore, can still accept cashless payments.

[0073] Manual (Swipe-to-Pay) Mode: Using a "swipe-to-pay" feature (or just "swipe") refers to a user's action implemented on his/her mobile device 150 where he/she quickly brushes his/her finger (or other pre-determined interaction) on the mobile device's touch screen 152 (Figures 10A-10D) or other input devices associated with the mobile device 150. From the user's perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g., a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user "swipes" to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 (Figure 19) of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0074] Hands-Free Mode: A "hands-free pay" feature (or just "hands-free") would most likely be used with "favorite" payment accepting units 120 (e.g., a frequently used vending machine at a user's work or school). From the user's perspective, he/she would approach the favorite payment accepting unit 120 and notice that the display 122, 124 (Figure

Petitioner Exhibit 1002-1212

19) of the payment accepting unit 120 shows funds available, he/she would select the product or service using the payment accepting unit's input mechanisms (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and he/she would retrieve dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g., a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately "arm's-length" distance (e.g., 3 to 5 feet) of the payment accepting unit 120, the user could observe the transferred funds on the display 122, 124 (Figure 19) of the payment accepting unit 120. The transaction is completed just as if cash was inserted into the payment accepting unit 120 with the user inputting his/her selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150. Figure 3 details when the hands-free mode would be available.

[0075] Multiple Vending Transactions (Multi-Vend): Both the manual and hands-free modes could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his/her first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124 (Figure 19) on the payment accepting unit 120. He/she could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 (Figure 19) may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the user walks away, the system clears (e.g., returns unused funds to the application 140 on the mobile device 150).

[0076] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment processing system described herein, operators of machines 120 can increase frequency of visits by purchasers and items sold with each visit.

[0077] The mobile-device-to-machine payment processing system described herein may be implemented as an apparatus, system, and/or method for enabling payments to a

Petitioner Exhibit 1002-1213

machine 120 via a mobile device 150. The mobile-device-to-machine payment processing system may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment processing system is not intended to be of a limiting nature.

DEFINITIONS

[0078] Before describing the mobile-device-to-machine payment processing system and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

[0079] Adapter Module 100: As shown in Figures 1 and 2, the adapter module 100 (sometimes also herein called the "payment module 100") is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component, it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g., components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. Figure 20 shows components associated with the adapter module 100. As shown in Figure 20, the communications unit 770 of the adapter module 100 includes short-range communication capability 776 (e.g., Bluetooth mechanisms).The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., a computer or a payment accepting unit) as long as the components are associated with each other.

[0080] Mobile Device 150 and Application 140 (also referred to as a "mobile application," "mobile app," or "app"): In general, a mobile device 150 may be a user's personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and the application 140, however, are not "trusted" in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or

Petitioner Exhibit 1002-1214

unuseable) by the mobile device 150. This keeps the communications passed between the adapter module 100 and the server 130 secured and safe from hacking. Mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g., a hardware-software combination) known or yet to be discovered that has structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application (e.g., the application 140) running on it. The term "app" is used broadly to include any software program(s) capable of implementing the features described herein. Figures 10A-10D show user interfaces for the application 140 displayed by the mobile device 150. It should be noted that the phrase "mobile device" can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an "app" can be assumed to be running on an associated mobile device unless specifically stated otherwise. Figure 21 shows components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., the cell phone itself) as long as the components are associated with each other.

[0081] Payment accepting unit 120 (or Machine 120): A payment accepting unit 120 (or the machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash (paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.

[0082] Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g., a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g., the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over "long-range communication technology" or "long-range communication protocol" (e.g., hardwired, telephone network technology, cellular technology (e.g., GSM, CDMA, or the like), Wi-Fi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication

Petitioner Exhibit 1002-1215

technology over the Internet that is known or yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user's mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g., a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using "short-range communication technology" or "short-range communication protocol" (e.g., Bluetooth (such as Bluetooth 4.0, Bluetooth Smart, Bluetooth Low Energy (BLE)), near-field communication (NFC), Ultra Wideband (UWB), radio frequency identification (RFID), infrared wireless, induction wireless, or any wired or wireless technology that could be used to communicate a small distance (approximately a hundred feet or closer) that is known or yet to be discovered). Therefore, neither the adapter module 100 nor the payment accepting unit 120 requires a traditional persistent long-range wireless network connection. The communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example, Wi-Fi technology could be replaced with another long-range communication technology.

[0083] Server: A server is the host processing server that may be operated by the company running the payment processing system. For each user, the server 130 preferably maintains at least one "virtual wallet" having at least one "balance" (which can be $0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, "cash" or it may be a "promotional value" that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g., via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g., the funding source server 160) may be automatically transferred to restore a predetermined balance. The balance may also be increased based on a promotion (e.g., points earned or coupons). As shown in Figure 22, the server includes appropriate processors 950, memory 960 (which would keep an accounting of the user's balance in a manner similar to a gift card), and communication systems 970. As shown in Figure 22, the communications unit 970 of the server 130 includes long-range communication capability 972 (e.g., cellular technology

Petitioner Exhibit 1002-1216

and/or Wi-Fi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an authorization request (sometimes also herein called an "AuthRequest") from the adapter module 100 (via a mobile device 150) and, if funds are available, returns an authorization grant (sometimes also herein called an "AuthGrant" or an "authorization grant token") for funds. Figure 22 shows components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., a computer or a main frame) as long as the components are associated with each other.

[0084] Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 106. Each adapter module 100 can listen to other adapter modules' advertisements.

[0085] Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g., a payment zone threshold and an authentication zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arm's-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a purchase) from the payment accepting unit 120. A mathematical computation (i.e., In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.

[0086] In-Range Heuristics: A mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or the payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which the mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g., they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g., is the user moving or stationary), and/or other information may also be logged while the

Petitioner Exhibit 1002-1217

user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the payment processing system continues to improve itself based on additional data points.

[0087] Authorization Request ("AuthRequest:): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends a secured authorization request (e.g., the encrypted authorization request) as a "message" (also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (Figure 20) with security technology (e.g., encryption and decryption means) that may be associated with the processing unit 750 and/or the memory 760. Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 130.

[0088] Authorization Grant Token ("AuthGrant"): This is a "message" (also referred to as a communication or transmissions) encrypted by the security unit 955 (Figure 22) with security technology (e.g., encryption and decryption means) of the server 130 with the unique private key corresponding to the adapter module 100. The secured authorization grant (e.g., the encrypted authorization grant) is passed from the server 130 to the adapter module 100 via the mobile device 150 in the form of a message. The mobile device 150, however, is not able to decrypt and/or read the message. The authorization grant is in response to the authorization request. The amount of the funds granted by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g., set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by time (e.g., only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g., the user has a long history with the payment processing system or some known provider (e.g., credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet

Petitioner Exhibit 1002-1218

balance), a pre-authorized time period (e.g., set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g., predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g., if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant remains valid until it expires or some other event occurs to end its validity (e.g., the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the "wallet balance" that is held in a virtual "wallet."

[0089] Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.

[0090] The mobile-device-to-machine payment processing system and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or hybrid of hardware and/or software). The term "hardware" includes at least one "processing unit," "processor," "computer," "programmable apparatus," and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as the processing unit 750 in Figure 20, the processing unit 850 in Figure 21, and the processing unit 950 in Figure 22). The term "software" includes at least one "program," "subprogram," "series of instructions," or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a "machine," such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment processing system (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. "Hardware" such as the adapter module 100, the mobile device 150, and the payment accepting unit 120 may have software (e.g., programs and apps) loaded thereon. The phrase "loaded onto the hardware" also includes being loaded into memory (shown as the memory 760 in Figure 20, the memory 860 in Figure 21, and the memory 960 in Figure 22) associated with or accessible by the hardware. The term "memory" is defined to include any type of hardware (or other

Petitioner Exhibit 1002-1219