

## TITLE

## SYSTEM AND METHOD FOR MULTIFACTOR PAYMENT

## TECHNICAL FIELD

**[0001]** This disclosure is related to Near Field Communication for contactless payments.

## SUMMARY

**[0002]** In one aspect, the present disclosure provides a method comprising receiving, by a card, transaction information from a point-of-service device, wherein the transaction information comprises a transaction amount; receiving, by an application associated with the card, the application running on a mobile device, the transaction information from the card; and selectively pursuing, by the card, based on the transaction amount, a multifactor authentication that comprises transmitting, by the card, to the application running on the mobile device, a first partial cryptogram; generating, by the application running on the mobile device, a second partial cryptogram; combining, by the application running on the mobile device, the first partial cryptogram and the second partial cryptogram to form a full cryptogram; and transmitting, by the application running on the mobile device, the full cryptogram to the point-of-service device.

**[0003]** In one aspect, the method further comprises an initial pairing of the card and the application, the initial pairing comprising: receiving, by the application running on the mobile device, card information; splitting, by the application running on the mobile device, the card information into a first portion and a second portion, wherein the first portion and the second portion comprise less than all of the card information; transmitting, by the application running on the mobile device, the first portion to the card; and storing, by the application running on the mobile device, the second portion.

**[0004]** In one aspect, the first partial cryptogram is based on the first portion of the card information.

**[0005]** In one aspect, the second partial cryptogram is based on the second portion of the card information.

**[0006]** In one aspect, the mobile device and the card are enabled for near field communication, and wherein the method further comprises receiving, by application running on the mobile device, the first partial cryptogram through the near field communication.

**[0007]** In one aspect, the method further comprises storing, by the card, a predetermined threshold based on a transaction amount limit.

**[0008]** In one aspect, the selectively pursuing the multifactor authentication is based on the transaction amount equaling to or exceeding the predetermined threshold.

**[0009]** In another aspect, the present disclosure provides a method comprising receiving, by a mobile device, card information associated with a card; splitting, by the mobile device, the card information into a first portion and a second portion, wherein the first portion and the second portion comprise less than all of the card information; transmitting, by the mobile device, the first portion to the card; storing, by the mobile device, the second portion; receiving, by the mobile device, from a point-of-service device, transaction information associated with a transaction by the card; receiving, by the mobile device, a first partial cryptogram from the card; generating, by the mobile device, a second partial cryptogram; combining, by the mobile device, the first partial cryptogram and the second partial cryptogram to form a full cryptogram; and transmitting, by the mobile device, the full cryptogram to the point-of-service device.

**[0010]** In one aspect, the first partial cryptogram is based on the first portion of the card information.

**[0011]** In one aspect, the second partial cryptogram is based on the second portion of the card information.

**[0012]** In one aspect, the mobile device and the card are enabled for near field communication, and further comprising receiving, by the mobile device, the first partial cryptogram through the near field communication from the card.

**[0013]** In one aspect, the method further comprises storing, by the card, a predetermined threshold based on a transaction amount limit.

**[0014]** In one aspect, the method further comprises initiating a payment for the transaction, wherein the transaction information comprises a transaction amount; and determining, by the card, that the transaction amount exceeds the predetermined threshold; and wherein the combining is based on the transaction amount exceeding the predetermined threshold.

**[0015]** In one aspect, the method further comprises initiating a payment for the transaction, wherein the transaction information comprises a transaction amount; determining, by the card, that the transaction amount is above the predetermined threshold; and generating, by the card, the first partial cryptogram, based on the transaction amount exceeding the predetermined threshold.

**[0016]** In another aspect, the present disclosure provides a payment card associated with a cardholder account, the payment card, comprising a card processor circuit configured to store account information associated with the cardholder account; store a predetermined threshold based on a transaction amount limit; receive a first transaction information associated with a first transaction, wherein the first transaction information comprises a first transaction amount; receive a second transaction information associated with a second transaction, wherein the second transaction information comprises a second transaction amount; based on a comparison of the first transaction amount and the predetermined threshold, generate a full cryptogram from the account information and the first transaction amount to authenticate the first transaction; and based on a comparison of the second transaction amount and the predetermined threshold, generate a partial cryptogram from the account information and the second transaction amount to authenticate the second transaction.

**[0017]** In one aspect, the card processor circuit is configured to generate the partial cryptogram based on the second transaction amount equaling or exceeding the predetermined threshold.

**[0018]** In one aspect, the card processor circuit is configured to generate the full cryptogram based on the first transaction amount being less than the predetermined threshold.

**[0019]** In one aspect, the card processor circuit is configured to store the account information separate from a portion of the account information.

**[0020]** In one aspect, the payment card further comprises a communication circuit configured to wirelessly connect the card processor circuit to a mobile device, wherein the card processor circuit is configured to transmit, through the communication circuit, the partial cryptogram to the mobile device.

**[0021]** In one aspect, the card processor circuit is configured to transmit the full cryptogram to a point of service device.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0022]** In the description, for purposes of explanation and not limitation, specific details are set forth, such as particular aspects, procedures, techniques, etc. to provide a thorough understanding of the present technology. However, it will be apparent to one skilled in the art that the present technology may be practiced in other aspects that depart from these specific details.

**[0023]** The accompanying drawings, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate aspects of concepts that include the claimed disclosure and explain various principles and advantages of those aspects.

**[0024]** The apparatuses, systems, and methods disclosed herein have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the various aspects of the present disclosure so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

**[0025]** FIG. 1 illustrates a system for payment using a mobile device and a card, according to at least one aspect of the present disclosure.

**[0026]** FIG. 2 illustrates a method of payment using a mobile device and a card, according to at least one aspect of the present disclosure.

**[0027]** FIG. 3 illustrates a method of paring the mobile device and the card, according to at least one aspect of the present disclosure.

**[0028]** FIG. 4 illustrates a method of payment using a modified POS device, according to at least one aspect of the present disclosure.

**[0029]** FIG. 5 is a block diagram of a computer apparatus with data processing subsystems or components, according to at least one aspect of the present disclosure.

**[0030]** FIG. 6 is a diagrammatic representation of an example system that includes a host machine within which a set of instructions to perform any one or more of the methodologies discussed herein may be executed, according to at least one aspect of the present disclosure.

**[0031]** FIG. 7 illustrates a block diagram of a communication device that may be used in various embodiments, according to at least one aspect of the present disclosure.

**[0032]** FIG. 8 illustrates the internal components of a card that may be used in accordance with at least one aspect of the present disclosure.

**[0033]** FIG. 9 depicts a payment network that may be used in various in accordance with at least one aspect of the present disclosure.

## DESCRIPTION

**[0034]** The following disclosure may provide exemplary systems, devices, and methods for conducting a financial transaction and related activities. Although reference may be made to such financial transactions in the examples provided below, aspects are not so limited. That is, the systems, methods, and apparatuses may be utilized for any suitable purpose.

**[0035]** Before discussing specific embodiments, aspects, or examples, some descriptions of terms used herein are provided below.

**[0036]** As used herein, the term “acceptance device” may be any suitable device that can accept or initiate a transaction. Non-limiting examples of an acceptance device may include a point-of-sale system, cash register, transaction processing computer, an authentication computer, a computing device, or a merchant server, such as a web server or e-commerce payment gateway configured to receive payment or transaction information. An acceptance device may further contain at least one processor, memory, secure element, speaker, display, wireless radio, card reader, or any other suitable component, or any combination thereof.

**[0037]** An “access device” may be any suitable device that provides access to a remote system. An access device also may be used for communicating with a merchant computer, a transaction processing computer, an authentication computer, or any other suitable system. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS or point-of-sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a user mobile device. In some embodiments or aspects, where an access device may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a payment device and/or mobile device. In a further example, communication may occur between a contactless element of a portable communication device and an access device, such as a merchant device reader or point-of-sale terminal, by using a wireless communications mechanism, such as near field communications (NFC), RF, infra-red, optical communications, etc. In some embodiments or aspects, a cellular

phone, tablet, or other dedicated wireless device used as a POS terminal may be referred to as a mobile point-of-sale or an “mPOS” terminal.

**[0038]** “Account credentials” may include any information that identifies an account and allows a payment processor to verify that a device, person, or entity has permission to access the account. For example, account credentials may include an account identifier (e.g., a PAN), a token (e.g., account identifier substitute), an expiration date, a cryptogram, a verification value (e.g., card verification value (CVV)), personal information associated with an account (e.g., address, etc.), an account alias, or any combination thereof. Account credentials may be static or dynamic such that they change over time. Further, in some embodiments or aspects, the account credentials may include information that is both static and dynamic. For example, an account identifier and expiration date may be static but a cryptogram may be dynamic and change for each transaction. Further, in some embodiments or aspects, some or all of the account credentials may be stored in a secure memory of a user device. The secure memory of the user device may be configured such that the data stored in the secure memory may not be directly accessible by outside applications and a payment application associated with the secure memory may be accessed to obtain the credentials stored on the secure memory. Accordingly, a mobile application may interface with a payment application in order to gain access to payment credentials stored on the secure memory.

**[0039]** Further, the term “account credential,” “account number,” or “payment credential” may refer to any suitable information associated with an account (e.g., a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (primary account number or “account number”), user name, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. Payment credentials may be any information that identifies or is associated with a payment account. Payment credentials may be provided in order to make a payment from a payment account. Payment credentials can also include a user name, an expiration date, a gift card number or code, and any other suitable information.

**[0040]** The term “account data,” as used herein, refers to any data concerning one or more accounts for one or more users. Account data may include, for example, one or more account identifiers, user identifiers, transaction histories, balances, credit limits, issuer institution identifiers, and/or the like.

**[0041]** As used herein, the term “account identifier” may refer to one or more types of identifiers associated with an account (e.g., a unique identifier of an account, an account number, a PAN, a card number, a payment card number, a token, and/or the like) of a user. In some non-limiting embodiments or aspects, an issuer may provide an account identifier (e.g., a PAN, a token, a globally unique identifier (GUID), a universally unique identifier (UUID), and/or the like) to a user that uniquely identifies one or more accounts associated with that user. In some non-limiting embodiments or aspects, an account identifier may be embodied on a payment device (e.g., a portable financial instrument, a payment card, a card, a debit card, and/or the like) and/or may be electronic information communicated to the user that the user may use for electronic payment transactions. In some non-limiting embodiments or aspects, an account identifier may be an original account identifier, where the original account identifier was provided to a user at the creation of the account associated with the account identifier. In some non-limiting embodiments or aspects, the account identifier may be an account identifier (e.g., a supplemental account identifier) that is provided to a user after the original account identifier was provided to the user. For example, if the original account identifier is forgotten by the user, stolen from the user, and/or the like, a supplemental account identifier may be provided to the user. In some non-limiting embodiments or aspects, an account identifier may be directly or indirectly associated with an issuer such that an account identifier may be a token that maps to a PAN or other type of identifier. Account identifiers may be alphanumeric, any combination of characters and/or symbols, and/or the like.

**[0042]** An “application” may include any software module configured to perform a specific function or functions when executed by a processor of a computer. For example, a “mobile application” may include a software module that is configured to be operated by a mobile device. Applications may be configured to perform many different functions. For instance, a “payment application” may include a software module that is configured to store and provide account credentials for a transaction. A “wallet application” may include a software module with similar functionality to a payment application that has multiple accounts provisioned or enrolled such that they are usable through the wallet application. Further, an “application” or “application program interface” (API) refers to computer code or other data stored on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An “interface” refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, touchscreen, etc.).

**[0043]** “Authentication” is a process by which the credential of an endpoint (including but not limited to applications, people, devices, process, and systems) can be verified to ensure that the endpoint is who they are declared to be.

**[0044]** An “authorization platform” (e.g., an “issuer”) may be a system that can authorize a transaction.

**[0045]** An “authorization request message” may be an electronic message that is sent to a payment processing network and/or an issuer of a payment account to request authorization for a payment transaction. An authorization request message according to some embodiments or aspects may comply with International Organization for Standardization (ISO) 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or a payment account. An ISO 8583 message includes a message type indicator, one or more bitmaps indicating which data elements are present in the message, and data elements of the message. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may be generated by an acceptance device or a server and may be sent to an issuing financial institution directly or through a payment network. In some embodiments or aspects of the present disclosure, an authorization request message may include a payment token, an expiration date, a token presentment mode, a token requestor identifier, a token cryptogram, a token assurance level, and data used to generate the token assurance level. The payment token may include a payment token issuer identifier that may be a substitute for a real issuer identifier for an issuer. For example, the real issuer identifier may be part of a BIN range associated with the issuer. An authorization request message may also comprise additional data elements corresponding to “identification information” including, for example, a service code, a CVV or CVC (card verification value or code), a dCVV or dCVC (dynamic card verification value or code), token cryptogram, an expiration date, etc. An authorization request message may also comprise “transaction information,” such as any information associated with a current transaction (e.g., the transaction amount, merchant identifier, merchant location, etc.) as well as any other information that may be utilized in determining whether to identify and/or authorize a payment transaction.

**[0046]** An “authorization response message” may be an electronic message reply to an authorization request message generated by an issuing financial institution (e.g., issuer) or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval—transaction was approved; Decline—transaction was not approved; or Call Center—response pending more

information, merchant must call the toll-free authorization phone number. The authorization response message may include an authorization code, which may be a code that an account issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (e.g., POS terminal) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments or aspects, a payment processing network may generate and/or forward the authorization response message to the merchant.

**[0047]** As used herein, an “authorization system” may refer to a system, a device, or components of a device that may utilize information to determine the probability or likelihood that a transaction is fraudulent. Although the term “merchant processor” may be referred to separately from an “authorization system” in portions of this disclosure, in some embodiments or aspects they may comprise one and the same system or systems that may perform substantially the same functionality, but in relation to different components of the system (e.g., providing information to a merchant or an issuer). In some embodiments or aspects, authorization systems may quantify the probabilities or likelihood of a fraudulent transaction by generating a “risk score.” In some embodiments or aspects, the authorization system may approve or reject a transaction. An exemplary embodiment or aspect of an authorization system is provided in U.S. Pat. No. 7,809,650 to Bruesewitz et al. entitled “Method and System for Providing Risk Information in Connection with Transaction Processing,” which is hereby incorporated by reference in its entirety. It should be understood that embodiments or aspects are not so limited.

**[0048]** An “authorizing entity” may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An “issuer” may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer.

**[0049]** As used herein, the terms “client” and “client device” may refer to one or more client-side devices or systems (e.g., remote from a transaction service provider) used to initiate or facilitate a transaction (e.g., a payment transaction). Moreover, a “client” may also refer to an entity (e.g., a merchant, an acquirer, and/or the like) that owns, utilizes, and/or operates a client device for initiating transactions (e.g., for initiating transactions with a transaction service provider).

**[0050]** The terms “client device” and “user device” refer to any electronic device that is

configured to communicate with one or more servers or remote devices and/or systems. A client device or a user device may include a mobile device, a network-enabled appliance (e.g., a network-enabled television, refrigerator, thermostat, and/or the like), a computer, a POS system, and/or any other device or system capable of communicating with a network. A client device may further include a desktop computer, laptop computer, mobile computer (e.g., smartphone), a wearable computer (e.g., a watch, pair of glasses, lens, clothing, and/or the like), a cellular phone, a network-enabled appliance (e.g., a network-enabled television, refrigerator, thermostat, and/or the like), a point-of-sale (POS) system, and/or any other device, system, and/or software application configured to communicate with a remote device or system.

**[0051]** As used herein, the term “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, calls, commands, and/or the like). A communication may use a direct or indirect connection and may be wired and/or wireless in nature. As an example, for one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to communicate with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. The one unit may communicate with the other unit even though the information may be modified, processed, relayed, and/or routed between the one unit and the other unit. In one example, a first unit may communicate with a second unit even though the first unit receives information and does not communicate information to the second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives data and does not actively transmit data to the second unit. As another example, a first unit may communicate with a second unit if an intermediary unit (e.g., a third unit located between the first unit and the second unit) receives information from the first unit, processes the information received from the first unit to produce processed information, and communicates the processed information to the second unit. In some non-limiting embodiments or aspects, a message may refer to a packet (e.g., a data packet, a network packet, and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

**[0052]** A “communication channel” may refer to any suitable path for communication between two or more entities. Suitable communications channels may be present directly between two entities such as a payment processing network and a merchant or issuer computer, or may include a number of different entities. Any suitable communications protocols may be used for generating a communications channel. A communication channel

may in some instances comprise a “secure communication channel” or a “tunnel,” either of which may be established in any known manner, including the use of mutual authentication and a session key and establishment of a secure communications session. However, any method of creating a secure communication channel may be used, and communication channels may be wired or wireless, as well as long-range, short-range, or medium-range. By establishing a secure channel, sensitive information related to a payment device (such as account number, CVV values, expiration dates, etc.) may be securely transmitted between the two entities to facilitate a transaction

**[0053]** Throughout the specification, the term “complete payment credentials” should be broadly interpreted and may include any payment or financial account details that can be used to process a transaction. The first payment credential portion may be any part of the complete payment credentials while the second payment credential portion is the remaining part such that the first and second portions together form the complete payment credentials. In some embodiments or aspects, the first payment credential portion is transmitted “in the clear” during a transaction, while a shared key is used to transmit the second payment credential portion in an encrypted format.

**[0054]** As used herein, the term “comprising” is not intended to be limiting, but may be a transitional term synonymous with “including,” “containing,” or “characterized by.” The term “comprising” may thereby be inclusive or open-ended and does not exclude additional, unrecited elements or method steps when used in a claim. For instance, in describing a method, “comprising” indicates that the claim is open-ended and allows for additional steps. In describing a device, “comprising” may mean that a named element(s) may be essential for an embodiment or aspect, but other elements may be added and still form a construct within the scope of a claim. In contrast, the transitional phrase “consisting of” excludes any element, step, or ingredient not specified in a claim. This is consistent with the use of the term throughout the specification.

**[0055]** As used herein, the term “computing device” or “computer device” may refer to one or more electronic devices that are configured to directly or indirectly communicate with or over one or more networks. A computing device may be a mobile device, a desktop computer, and/or the like. As an example, a mobile device may include a cellular phone (e.g., a smartphone or standard cellular phone), a portable computer, a wearable device (e.g., watches, glasses, lenses, clothing, and/or the like), a personal digital assistant (PDA), and/or other like devices. The computing device may not be a mobile device, such as a desktop computer. Furthermore, the term “computer” may refer to any computing device that includes the necessary components to send, receive, process, and/or output data, and

normally includes a display device, a processor, a memory, an input device, a network interface, and/or the like.

**[0056]** A “condition” may be a value such as transaction amount, transaction type, the time of day at which settlement for a payment processing network occurs, merchant category code (MCC), merchant verification value (MVV), whether a payment processing network is subject to regulation, etc.

**[0057]** A “consumer” may include an individual or a user that may be associated with one or more personal accounts and/or consumer devices. The consumer also may be referred to as a cardholder, account holder, or user.

**[0058]** A “cryptographic algorithm” can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), etc. Encryption techniques may include symmetric and asymmetric encryption techniques.

**[0059]** Reference to “a device,” “a server,” “a processor,” and/or the like, as used herein, may refer to a previously-recited device, server, or processor that is recited as performing a previous step or function, a different server or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server or a first processor that is recited as performing a first step or a first function may refer to the same or different server or the same or different processor recited as performing a second step or a second function.

**[0060]** A “digital wallet” can include an electronic device that allows an individual to conduct electronic commerce transactions. A digital wallet may be designed to streamline the purchase and payment process. A digital wallet may allow the user to load one or more payment cards onto the digital wallet so as to make a payment without having to enter an account number or present a physical card.

**[0061]** A “digital wallet provider” may include an entity, such as an issuing bank or third party service provider, that issues a digital wallet to a user that enables the user to conduct financial transactions. A digital wallet provider may provide standalone user-facing software applications that store account numbers, or representations of the account numbers (e.g., payment tokens), on behalf of a cardholder (or other user) to facilitate payments at more than one unrelated merchant, perform person-to-person payments, or load financial value

into the digital wallet. A digital wallet provider may enable a user to access its account via a personal computer, mobile device or access device. Additionally, a digital wallet provider may also provide one or more of the following functions: storing multiple payment cards and other payment products on behalf of a user, storing other information including billing address, shipping addresses, and transaction history, initiating a transaction by one or more methods, such as providing a user name and password, NFC or a physical token, and may facilitate pass-through or two-step transactions.

**[0062]** As used herein, an “electronic wallet,” “digital wallet” or “mobile wallet” can store user profile information, payment information (including tokens), bank account information, and/or the like and can be used in a variety of transactions, such as but not limited to eCommerce, social networks, money transfer/personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital goods purchases, utility payments, purchasing games or gaming credits from gaming websites, transferring funds between users, and/or the like.

**[0063]** As used herein, the terms “electronic wallet,” “electronic wallet mobile application,” and “digital wallet” may refer to one or more electronic devices and/or one or more software applications configured to initiate and/or conduct transactions (e.g., payment transactions, electronic payment transactions, and/or the like). For example, an electronic wallet may include a user device (e.g., a mobile device) executing an application program and server-side software and/or databases for maintaining and providing transaction data to the user device.

**[0064]** As used herein, the term “electronic wallet provider” may include an entity that provides and/or maintains an electronic wallet and/or an electronic wallet mobile application for a user (e.g., a customer). Examples of an electronic wallet provider include, but are not limited to, Google Wallet™, Android Pay®, Apple Pay®, and Samsung Pay®, and/or other like electronic payment systems. In some non-limiting examples, a financial institution (e.g., an issuer institution) may be an electronic wallet provider. As used herein, the term “electronic wallet provider system” may refer to one or more computer systems, computer devices, servers, groups of servers, and/or the like operated by or on behalf of an electronic wallet provider.

**[0065]** As used herein, the term “electronic wallet transaction processing system” may refer to one or more electronic devices and/or software applications configured to process and/or a request to authenticate a user for a transaction initiated and/or conducted by an electronic wallet application. For example, an electronic wallet transaction processing

system may include server-side software and/or databases for maintaining and providing transaction data and/or account data to a merchant system and/or a payment gateway system for processing and/or authenticating a user for an electronic wallet transaction. An “electronic wallet transaction processing system provider” may include an entity that provides and/or maintains an electronic wallet transaction processing system, such as Visa Checkout, Mastercard MasterPass™, PayPal Checkout, and/or other like electronic wallet transaction processing system providers. In some non-limiting examples, a transaction service provider system may be an electronic wallet transaction processing system.

**[0066]** An “identification and verification (ID&V) method” may be used to ensure that the payment token is replacing a PAN that was legitimately being used by the token requestor. Examples of ID&V methods may include, but are not limited to, an account verification message, a risk score based on assessment of the primary account number (PAN) and use of one time password by the issuer or its agent to verify the account holder. Exemplary ID&V methods may be performed using information such as a user signature, a password, an offline or online personal identification number (PIN), an offline or online enciphered PIN, a combination of offline PIN and signature, a combination of offline enciphered PIN and signature, user biometrics (e.g., voice recognition, fingerprint matching, etc.), a pattern, a glyph, knowledge-based challenge responses, hardware tokens (multiple solution options), one time passwords (OTPs) with limited use, software tokens, two-channel authentication processes (e.g., via phone), etc. Using the ID&V, a confidence level may be established with respect to the token to PAN binding.

**[0067]** As used herein, “identification information” may include any suitable information associated with an account (e.g., a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (primary account number or “account number”), user name, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. CVV2 is generally understood to be a static verification value associated with a payment device. CVV2 values are generally visible to a user (e.g., a consumer), whereas CVV and dCVV values are typically embedded in memory or authorization request messages and are not readily known to the user (although they are known to the issuer and payment processors).

**[0068]** An “interface” may include any software module configured to process communications. For example, an interface may be configured to receive, process, and respond to a particular entity in a particular communication format. Further, a computer,

device, and/or system may include any number of interfaces depending on the functionality and capabilities of the computer, device, and/or system. In some embodiments or aspects, an interface may include an application programming interface (API) or other communication format or protocol that may be provided to third parties or to a particular entity to allow for communication with a device. Additionally, an interface may be designed based on functionality, a designated entity configured to communicate with, or any other variable. For example, an interface may be configured to allow for a system to field a particular request or may be configured to allow a particular entity to communicate with the system.

**[0069]** A “key” may refer to a piece of information that is used in a cryptographic algorithm to transform input data into another representation. An exemplary encryption key may include a master derivation key (MDK) which may be used to generate a limited use key (LUK) that is provided to a computer device of a user. An LUK can be an encryption key that is intended for limited use (e.g., a limited number of transactions or a limited time period) and is not intended to be used for the lifetime of an account. Further details regarding LUKs can be found in U.S. Published Patent Application No. 2015/0180836, which is herein incorporated by reference in its entirety and is assigned to the same assignee as the present application. The MDK may be used to generate and provision the token, as well as, authenticate the token when used in authorization processing by validating static and variable transaction data.

**[0070]** A “key check value (KCV)” may refer to value obtained by passing a data value through a non-reversible algorithm. The key check value may be calculated using a cryptographic algorithm which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key is not feasible.

**[0071]** As used herein, the term “merchant” may refer to one or more individuals or entities (e.g., operators of retail businesses that provide goods and/or services, and/or access to goods and/or services, to a user (e.g., a customer, a consumer, a customer of the merchant, and/or the like) based on a transaction (e.g., a payment transaction)). As used herein “merchant system” may refer to one or more computer systems operated by or on behalf of a merchant, such as a server computer executing one or more software applications.

**[0072]** A “merchant application” may include any application associated with a relying party to a transaction. For example, a merchant mobile application may be associated with a particular merchant or may be associated with a number of different merchants. In some

embodiments or aspects, the merchant mobile application may store information identifying a particular merchant server computer that is configured to provide a sales environment in which the merchant server computer is capable of processing remote transactions initiated by the merchant application. Further, the merchant mobile application may also include a general purpose browser or other software designed to interact with one or more merchant server computers. In some cases, the merchant mobile application may be installed in the general purpose memory of a user device and thus, may be susceptible to malicious attacks.

**[0073]** As used herein, a “mobile device” may comprise any electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (e.g., cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, etc. Further examples of mobile devices include wearable devices, such as smart watches, fitness bands, ankle bracelets, rings, earrings, etc., as well as automobiles with remote communication capabilities. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g., when a device has remote access to a network by tethering to another device—e.g., using the other device as a modem—both devices taken together may be considered a single mobile device). A mobile device may also comprise a verification token in the form of, for instance, a secured hardware or software component within the mobile device and/or one or more external components that may be coupled to the mobile device. A detailed description of an exemplary mobile device is provided below.

**[0074]** As used herein, an “online purchase” can be the purchase of a digital or physical item or service via a network, such as the Internet.

**[0075]** An “original” transaction may include any transaction including an authorization provided by an issuer or an authorization provided on-behalf-of an issuer.

**[0076]** As used herein, a “payment account” (which may be associated with one or more payment devices) may refer to any suitable payment account including a card account, a checking account, or a prepaid account.

**[0077]** A “payment application” or “wallet application” may store credentials (e.g.,

account identifier, expiration date, card verification value (CVV), etc.) for accounts provisioned onto the user device. The account credentials may be stored in general memory on the mobile device or on a secure trusted execution environment (e.g., a secure element) of the user device. Further, in some embodiments or aspects, the account credentials may be stored by a remote computer and the payment/wallet application may retrieve the credentials (or a portion thereof) from the remote computer before/during a transaction. Any number of different commands or communication protocols may be used to interface with the payment application and/or wallet application in order to obtain and use stored credentials associated with each application.

**[0078]** The payment application or wallet application may be configured to provide credentials to an authorized software application or module on a user device. For example, a payment application may be configured to interface with a master applet in order to provide credentials to a mobile application for a transaction. For instance, the payment application may provide a software development kit (SDK) or application programming interface (API) that the master wallet applet may use to interface with the payment application and/or wallet application. The payment application and/or wallet application may be configured to provide the sensitive information in encrypted form using stored encryption keys. Thus, each payment application and/or wallet application may have different commands and/or instructions for accessing the associated credentials stored by the payment/wallet application. For instance, each payment application and/or wallet application may have a different application program interface (API) with different commands, data requirements, authentication processes, etc., for interacting with other applications operating on the user device. Accordingly, a master wallet applet may include a number of different APIs, one for each of the different payment applications and/or wallet applications that the master wallet applet is configured to interface with.

**[0079]** A “payment device” may refer to any device that may be used to conduct a financial transaction, such as to provide payment information to a merchant. A payment device may be in any suitable form. The payment device may be a software object, a hardware object, or a physical object. As examples of physical objects, the payment device may comprise a substrate such as a paper or plastic card, and information that is printed, embossed, encoded, or otherwise included at or near a surface of an object. A hardware object can relate to circuitry (e.g., permanent voltage values), and a software object can relate to non-permanent data stored on a device. For example, suitable payment devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, debit devices (e.g., a debit card), credit

devices (e.g., a card), stored value devices (e.g., a stored value card or “prepaid” card), magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of payment devices include cellular or wireless telephones (e.g., a smartphone), personal digital assistants (PDAs), portable computer (e.g., tablet or laptop computer), pagers, payment cards, security cards, access cards, smart media, transponders, 2-D barcodes, an electronic or digital wallet, and the like. If the payment device is in the form of a debit, credit, or smartcard, the payment device may also optionally have features such as magnetic stripes. Such devices can operate in either a contact or contactless mode. In some non-limiting embodiments or aspects, a payment device may include an electronic payment device, such as a smartcard, a chip card, integrated circuit card, and/or the like. An electronic payment device may include an embedded integrated circuit and the embedded integrated circuit may include a data storage medium (e.g., volatile and/or non-volatile memory) to store information associated with the payment device, such as an account identifier, a name of the account holder, and/or the like. The payment device may interface with an access device such as a point-of-sale device to initiate the transaction. In some embodiments or aspects, a mobile device can function as a payment device (e.g., a mobile device can store and be able to transmit payment credentials for a transaction). Further, a payment device may be associated with a value such as a monetary value, a discount, or store credit, and a payment device may be associated with an entity such as a bank, a merchant, a payment processing network, or a person. A payment device may be used to make a payment transaction.

**[0080]** As used herein, the term “payment gateway” may refer to an entity and/or a payment processing system operated by or on behalf of such an entity (e.g., a merchant service provider, a payment service provider, a payment facilitator, a payment facilitator that contracts with an acquirer, a payment aggregator, and/or the like), which provides payment services (e.g., transaction service provider payment services, payment processing services, and/or the like) to one or more merchants. The payment services may be associated with the use of portable financial devices managed by a transaction service provider. As used herein, the term “payment gateway system” may refer to one or more computer systems, computer devices, servers, groups of servers, and/or the like, operated by or on behalf of a payment gateway and/or to a payment gateway itself. The term “payment gateway mobile application” may refer to one or more electronic devices and/or one or more software applications configured to provide payment services for transactions (e.g., payment transactions, electronic payment transactions, and/or the like).

**[0081]** A “payment network” may refer to an electronic payment system used to accept,

transmit, or process transactions made by payment devices for money, goods, or services. The payment network may transfer information and funds among issuers, acquirers, merchants, and payment device users. One illustrative non-limiting example of a payment network is VisaNet, which is operated by Visa, Inc.

**[0082]** A “payment processing network” may refer to a system that receives accumulated transaction information from the gateway processing service, typically at a fixed time each day, and performs a settlement process. Settlement may involve posting the transactions to the accounts associated with the payment devices used for the transactions and calculating the net debit or credit position of each user of the payment devices. An exemplary payment processing network is Interlink®.

**[0083]** The terms “point-of-sale system,” “POS system,” or “POS terminal,” as used herein, may refer to one or more computers and/or peripheral devices used by a merchant to engage in payment transactions with customers, including one or more card readers, near-field communication (NFC) receivers, radio-frequency identification (RFID) receivers, and/or other contactless transceivers or receivers, contact-based receivers, payment terminals, computers, servers, input devices, and/or other like devices that can be used to initiate a payment transaction. A POS terminal may be located proximal to a user, such as at a physical store location, or a POS terminal may be remote from the user, such as a server interacting with a user browsing on their personal computer. POS terminals may include mobile devices.

**[0084]** As used herein, the term “portable financial device” may refer to a payment card (e.g., a credit or debit card), a gift card, a smartcard, smart media, a payroll card, a healthcare card, a wrist band, a machine-readable medium containing account information, a keychain device or fob, an RFID transponder, a retailer discount or loyalty card, a cellular phone, an electronic wallet mobile application, a personal digital assistant (PDA), a pager, a security card, a computer, an access card, a wireless terminal, a transponder, and/or the like. In some non-limiting embodiments or aspects, the portable financial device may include volatile or non-volatile memory to store information (e.g., an account identifier, a name of the account holder, and/or the like).

**[0085]** A “primary account number (PAN)” may be a variable length, (e.g., 13 to 19-digit) industry standard-compliant account number that is generated within account ranges associated with a BIN by an issuer.

**[0086]** A “processing network” may include an electronic system used to accept,

transmit, or process transactions made by devices. The processing network may transfer information among transacting parties (e.g., issuers, acquirers, merchants, device users, etc.).

**[0087]** A payment processing network that is “providing degraded service” satisfies one or more system degradation criteria. System degradation criteria include any condition resulting in delayed processing of an authorization request message by a payment processing network. System degradation criteria may also include failure of a payment processing network to process an authorization request message.

**[0088]** As used herein, the term “product” may refer to one or more goods and/or services offered by a merchant.

**[0089]** A “real account identifier” may include an original account identifier associated with a payment account. For example, a real account identifier may be a primary account number (PAN) issued by an issuer for a card account (e.g., card, debit card, etc.). For instance, in some embodiments or aspects, a real account identifier may include a sixteen digit numerical value such as “4147 0900 0000 1234.” The first six digits of the real account identifier (e.g., “414709”), may represent a real issuer identifier (BIN) that may identify an issuer associated with the real account identifier.

**[0090]** As used herein, a “secure element” may include a secure computer memory in an electronic device capable of storing sensitive data or applications. A secure element may, but need not be, physically isolated from other memory in an electronic device. A secure element may comprise, or may be contained within, a hardware security module, a software security module, or other mechanism providing for secure and controlled access to the data stored within it. A secure element may further comprise a dedicated crypto-processor used for accessing its contents and executing secure operations.

**[0091]** As used herein, the term “server” may include one or more computing devices which can be individual, stand-alone machines located at the same or different locations, may be owned or operated by the same or different entities, and may further be one or more clusters of distributed computers or “virtual” machines housed within a datacenter. It should be understood and appreciated by a person of skill in the art that functions performed by one “server” can be spread across multiple disparate computing devices for various reasons. As used herein, a “server” is intended to refer to all such scenarios and should not be construed or limited to one specific configuration. Further, a server as described herein may, but need not, reside at (or be operated by) a merchant, a payment network, a financial institution, a

healthcare provider, a social media provider, a government agency, or agents of any of the aforementioned entities. The term “server” may also refer to or include one or more processors or computers, storage devices, or similar computer arrangements that are operated by or facilitate communication and processing for multiple parties in a network environment, such as the Internet, although it will be appreciated that communication may be facilitated over one or more public or private network environments and that various other arrangements are possible. Further, multiple computers, e.g., servers, or other computerized devices, e.g., point-of-sale devices, directly or indirectly communicating in the network environment may constitute a “system,” such as a merchant's point-of-sale system. Reference to “a server” or “a processor,” as used herein, may refer to a previously-recited server and/or processor that is recited as performing a previous step or function, a different server and/or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server and/or a first processor that is recited as performing a first step or function may refer to the same or different server and/or a processor recited as performing a second step or function.

**[0092]** A “server computer” may typically be a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. The server computer may be associated with an entity such as a payment processing network, a wallet provider, a merchant, an authentication cloud, an acquirer or an issuer. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers. In some embodiments or aspects, the server computer may provide and/or support payment network cloud service.

**[0093]** As used herein, “short range communication” or “short range wireless communication” may comprise any method of providing short-range contact or contactless communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between a payment device and an access device. In some embodiments or aspects, short range communications may be in conformance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Short range communication typically comprises communications at a range of less than 2 meters. In some embodiments or aspects, it may be preferable to limit the range

of short range communications (e.g., to a range of less than 1 meter, less than 10 centimeters, or less than 2.54 centimeters) for security, technical, and/or practical considerations. For instance, it may not be desirable for a POS terminal to communicate with every payment device that is within a 2 meter radius because each of those payment devices may not be involved in a transaction, or such communication may interfere with a current transaction involving different financial transaction devices. Typically the payment device or the access device also includes a protocol for determining resolution of collisions (e.g., when two payment devices are communicating with the access device simultaneously). The use of short range communications may be used when the merchant and the consumer are in close geographic proximity, such as when the consumer is at the merchant's place of business.

**[0094]** A “substitute” transaction may be any transaction that is associated with an original transaction and that takes place after the original transaction, including repeat, refunds, reversals or exceptions (chargebacks, re-presentments, etc.).

**[0095]** As used herein, the term “system” may refer to one or more computing devices or combinations of computing devices (e.g., processors, servers, client devices, software applications, components of such, and/or the like).

**[0096]** The “time of day” may be a cut-off time for settlement. For example, a user may wish to use a first routing priority list during a first time range and a second routing priority list during a second time range such that a payment processing network to which a transaction is routed has a cut off time that occurs within a particular period of time after the transaction occurs.

**[0097]** A “transaction amount” may be the price assessed to the consumer for the transaction. The transaction amount condition may be a threshold value (e.g., all transactions for an amount exceeding \$100) or a range (e.g., all transactions in the range of \$25-\$50). For example, a user may wish to use a first routing priority list for a transaction for an amount in the range of \$0.01-\$100 and a second routing priority list for a transaction for an amount exceeding \$100.

**[0098]** The term “transaction data” may include any data associated with one or more transactions. In some embodiments or aspects, the transaction data may merely include an account identifier (e.g., a PAN) or payment token. Alternatively, in other embodiments or aspects, the transaction data may include any information generated, stored, or associated with a merchant, consumer, account, or any other related information to a transaction. For

example, transaction data may include data in an authorization request message that is generated in response to a payment transaction being initiated by a consumer with a merchant. Alternatively, transaction data may include information associated with one or more transactions that have been previously processed and the transaction information has been stored on a merchant database or other merchant computer. The transaction data may include an account identifier associated with the payment instrument used to initiate the transaction, consumer personal information, products or services purchased, or any other information that may be relevant or suitable for transaction processing. Additionally, the transaction information may include a payment token or other tokenized or masked account identifier substitute that may be used to complete a transaction and protect the underlying account information of the consumer.

**[0099]** As used herein, the term “transaction service provider” may refer to an entity that receives transaction authorization requests from merchants or other entities and provides guarantees of payment, in some cases through an agreement between the transaction service provider and an issuer. For example, a transaction service provider may include a payment network, such as Visa®, MasterCard®, American Express®, or any other entity that processes transactions. As used herein “transaction service provider system” may refer to one or more systems operated by or operated on behalf of a transaction service provider, such as a transaction service provider system executing one or more software applications associated with the transaction service provider. In some non-limiting embodiments or aspects, a transaction processing system may include one or more server computers with one or more processors and, in some non-limiting embodiments or aspects, may be operated by or on behalf of a transaction service provider.

**[0100]** A “user” may include an individual. In some embodiments or aspects, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer.

**[0101]** A “user device” is an electronic device that may be transported and/or operated by a user. A user device may provide remote communication capabilities to a network. The user device may be configured to transmit and receive data or communications to and from other devices. In some embodiments or aspects, the user device may be portable. Examples of user devices may include mobile phones (e.g., smart phones, cellular phones, etc.), PDAs, portable media players, wearable electronic devices (e.g., smart watches, fitness bands, ankle bracelets, rings, earrings, etc.), electronic reader devices, and portable computing devices (e.g., laptops, netbooks, ultrabooks, etc.). Examples of user devices may also include automobiles with remote communication capabilities.

**[0102]** “User information” may include any information that is associated with a user. For example, the user information may include a device identifier of a device that the user owns or operates and/or account credentials of an account that the user holds. A device identifier may include a unique identifier assigned to a user device that can later be used to verify the user device. In some embodiments or aspects, the device identifier may include a device fingerprint. The device fingerprint may be an aggregation of device attributes. The device fingerprint may be generated by a software development kit (SDK) provided on the user device using, for example, a unique identifier assigned by the operating system, an International Mobile Station Equipment Identity (IMEI) number, operating system (OS) version, plug-in version, and the like.

**[0103]** NFC (Near Field Communication) is useable for contactless payments. There are issues that prevent customers from adopting this new technology. One such reason is that NFC payments have security issues. In addition to that, in certain countries, these security concerns have forced regulators to place an upper limit on the amount of transactions that can be done with NFC.

**[0104]** Most mobile phones have NFC capabilities, and there are many mobile wallets that contain NFC payment capabilities. This disclosure is directed to combining the NFC capabilities of the mobile phone with an NFC enabled card to make the payment process with NFC more secure. In this disclosure, the NFC enabled mobile phone acts as an additional factor on top of the NFC enabled card. This disclosure is directed to splitting the card information randomly between two NFC devices, such that the split card information does not work without the other part of the split information.

**[0105]** In another aspect, both a card and a mobile device are programmed to generate a partial cryptogram with a portion of the card credentials. Each of the card and the mobile device generate their own unique cryptogram which in itself can't be used for a transaction. In one aspect, the point of sale device is configured to combine the two cryptograms and then use the full cryptogram for completing the transaction. The full cryptogram generated after combination by the POS is the same as a complete cryptogram that can be generated by a card in a normal transaction flow. In another aspect, the mobile device is configured to combine the two cryptograms and then use the full cryptogram for completing the transaction.

**[0106]** For example, a cardholder pairs an NFC-enabled mobile device with an NFC card. In this pairing process, card details are scrambled, encrypted and split in two between both the mobile device and the card. When the cardholder taps the card on a POS terminal,

and only half of the card details are transferred from the card to the POS terminal. There are additional metadata bits that indicate that the card details sent are to be followed by a second factor. This tap of card will have to be followed by a second tap of an NFC enabled mobile device (in a short time interval), which transfers the remaining card details to the POS machine. The NFC transfer from the NFC enabled mobile device can only happen after a successful biometric verification of the user. The POS device has additional capability of decrypting the card details received and making sense of the two splits of card details it received in two subsequent taps. Once the POS device receives both halves, it can combine the split card details and get the full card details. A traditional NFC payment process is subsequently followed. The subsequent taps can be in any order. The multifactor identification module in the POS terminal is configured to unscramble and combine the data irrespective of the order of tapping the mobile device and the card.

**[0107]** As can be seen in the above steps, the transaction can occur only when both the mobile device and the card are used. This ensures that one of the mobile device with NFC payments, or the card with NFC payments is lost, there can be no transactions with that single device. This allows an increase in the limit of tap and pay cards, and also the number of tap and pay transactions in a day.

**[0108]** FIG. 1 illustrates a system 100 for payment using a mobile device 106 and a card 104, according to at least one aspect of the present disclosure. The system 100 receives information from a user 102. The user 102 has a card 104 and a mobile device 106. To complete a transaction, the user 102 brings the card 104 within a threshold distance for near field communication (NFC) to a point-of-service (POS) device 108. The POS device 108 receives card information from the card 104. The card 104 and the mobile device 106 are enabled for NFC.

**[0109]** The card 104 stores card information. The card information can include payment credentials or account credentials. The card information comprises at least one of a card number, a CVV, a name, and an expiration date. In one aspect, the card 104 is configured to send additional metadata bits that indicate that the card details sent to the POS device 108 are to be followed by a second factor when multifactor authentication is enabled. In another aspect, the card 104 is configured to send additional metadata bits that indicate that the card details sent to the POS device 108 are to be followed by a second factor when the transaction amount exceeds a threshold.

**[0110]** The mobile device 106 is configured to execute the methods illustrated in FIGS 2-4. The mobile device 106 can execute the methods through an application on the mobile

device 106 or an electronic wallet application on the mobile device 106.

**[0111]** FIG. 2 illustrates a method 200 of payment using a mobile device 106 and a card 104, according to at least one aspect of the present disclosure. FIG. 2 is described in conjunction with FIG. 1. A payment is initiated 202 for a transaction. To begin a payment transaction, the card 104 is located within the predetermined distance of the POS device 108. The predetermined distance is the threshold distance for NFC to be operable. According to method 200, the card 104 receives 203 transaction information from the POS device 108 for the payment transaction. In one aspect, the transaction information comprises at least a transaction amount. In one aspect, the card 104 transfers metadata bits to the POS device 108 that indicate the card information will be sent by a second factor.

**[0112]** In one aspect, the card 104 determines 204 whether a transaction amount is equal to or above a threshold. For example, if the card 104 determines 204 that the transaction amount is equal to or greater than the threshold, the method 200 proceeds along the Yes path and the mobile device 106 receives 208 the partial cryptogram from the card 104. The card 104 generates the first partial cryptogram based on the transaction amount being equal to or exceeding the threshold. The card 104 transmits the first partial cryptogram to the application running on the mobile device 106. In one aspect, selectively pursuing multifactor authentication is based on the transaction amount equaling or exceeding the threshold.

**[0113]** In another aspect, the POS device 108 determines whether the transaction amount is equal to or above the threshold. For example, if the POS device 108 determines 204 that the transaction amount is equal to or exceeds the threshold, the method 200 proceeds along the Yes path and the mobile device 106 receives 208 the partial cryptogram from the card 104. The card 104 generates the first partial cryptogram based on the transaction amount being equal to or exceeding the threshold.

**[0114]** The determination that the transaction amount exceeds the threshold indicates that the two factor authentication process is to begin. The user 102 brings the card 104 within the threshold distance of the mobile device 106 to send the first partial cryptogram from the card 104 to the mobile device 106. The method 200 continues and the mobile device 106 receives 208 the first partial cryptogram based on the transaction amount equaling or exceeding the threshold.

**[0115]** If the POS device 108 or the card 104 determines 204 that the transaction amount is less than the threshold, the method 200 proceeds along the No path and the card

104 generates a full cryptogram based on the transaction amount being less than the threshold and sends 206 the full cryptogram to the POS device 108. The full cryptogram is based on at least the card information.

**[0116]** In one aspect, the threshold is a predetermined threshold based on a transaction amount limit. In another aspect, the threshold is a number of NFC payment transactions within a given period. In one aspect, the threshold is a value set by at least one of regulations in a given location, a user, or a card issuer. In one aspect, the card 104 stores the threshold for a transaction. In another aspect, the POS device 108 stores the threshold and provides the threshold to the card 104 in the transaction information. In another aspect, the mobile device 106 stores the threshold amount and provides the threshold to the card 104 during the pairing process (described in FIG. 3).

**[0117]** In accordance with the method 200, proceeding along the Yes path, the mobile device 106 receives 208 a first partial cryptogram from the card 104. In one aspect, the first partial cryptogram is based on a first portion of the card information. The card 104 transfers the first partial cryptogram to the mobile device 106 via NFC. The card 104 and the mobile device 106 are within the threshold distance for NFC to be operable during the transfer of the first partial cryptogram. In one aspect, the first partial cryptogram is generated after the card 104 receives transaction information from the POS device 108 and the first partial cryptogram is further based on the transaction information.

**[0118]** In accordance with the method 200, the mobile device 106 receives 207 the transaction information. In one aspect, the mobile device 106 receives 207 the transaction information from the card 104. The card 104 is brought within the threshold distance of the mobile device 106 for NFC to be operable. The card 104 transfers the transaction information via NFC. In another aspect, the mobile device 106 receives 207 the transaction information from the POS device 108. The POS device 108 transfers the transaction information via NFC to the mobile device 106, such that the mobile device 106 and POS device 108 are within the threshold distance for NFC to be operable.

**[0119]** Still in accordance with the method 200, proceeding along the Yes path, the mobile device 106 generates 210 a second partial cryptogram. The mobile device 106 stores a second portion of the card information and generates 210 the second partial cryptogram. In one aspect, the second partial cryptogram is based on the second portion of the card information. The mobile device 106 utilizes a cryptographic algorithm to generate the second partial cryptogram. In one aspect, the second partial cryptogram is generated after the mobile device 106 receives the transaction information and the second partial cryptogram is

further based on the transaction information.

**[0120]** Still in accordance with the method 200, proceeding along the Yes path, the mobile device 106 combines 212 the first partial cryptogram and the second partial cryptogram to form a full cryptogram. The full cryptogram is based on the card information. The mobile device 106 utilizes a cryptographic algorithm to generate the full cryptogram based on the first and second partial cryptogram. In one aspect, the mobile device 106 does not combine the first and second cryptograms unless a successful biometric verification of the user 102 occurs. The full cryptogram comprises all the card information required by the POS device 108 to complete a payment transaction.

**[0121]** Still in accordance with the method 200, proceeding along the Yes path, the mobile device 106 transmits 214 the full cryptogram to the POS device 108 device via NFC. The mobile device 106 transfers the full cryptogram to the POS device 108 when the mobile device 106 is within a threshold distance of the POS device 108 such that NFC is operable. In one aspect, the mobile device 106 does not transmit the full cryptogram unless a successful biometric verification of the user 102 occurs on the mobile device 106.

**[0122]** In one aspect, if the card 104 determines that multifactor authentication is enabled, the card 104 generates the first partial cryptogram based. In another aspect, if the POS device 108 determines that multifactor authentication is enabled, the POS device 108 includes the information in the transaction information sent from the POS device 108 to the card 104.

**[0123]** For example, the card selectively pursues based on the transaction amount multifactor authentication. The multifactor authentication comprises transmitting, by the card, a first partial cryptogram to the mobile device. During the multifactor authentication, the application running on the mobile device generates a second partial cryptogram, combines the first partial cryptogram and the second partial cryptogram to form a full cryptogram, and transmits the full cryptogram to the point-of-service device.

**[0124]** In one aspect, the card 104 determines if multifactor authentication is enabled and compares a transaction amount to a threshold. The card 104 receives the transaction information from the POS device 108. Based on the transaction amount being less than the threshold, the transaction proceeds with an NFC payment from the card, where the card transfers the full cryptogram of card information. Based on the multifactor authentication not being enabled and the transaction amount is equal to or greater than the threshold, the transaction does not proceed with an NFC payment. Based on the determination that

multifactor authentication is enabled and the transaction amount is equal to or greater than the threshold, the card 104 generates the first partial cryptogram and sends the first partial cryptogram to the mobile device 106. The mobile device 106 generates and retrieves the second partial cryptogram, combines the first cryptogram and the second cryptogram to generate the full cryptogram, and transmits the full cryptogram to the POS device 108.

**[0125]** FIG. 3 illustrates a method 300 of pairing the mobile device 106 and the card 104, according to at least one aspect of the present disclosure. FIG. 3 is discussed in conjunction with FIG. 1 and FIG. 2. In one aspect, the card 104 and the mobile device 106 are paired to enable multifactor authentication. In one aspect, the card 104 and mobile device 106 are paired before the method of FIG. 2 begins.

**[0126]** In one aspect, the method 300 includes an initial pairing the mobile device 106 with the card 104. To pair the mobile device 106 and the card 104, the mobile device 106 and the card 104 are located 302 within a threshold distance for NFC to be operable. The mobile device 106 receives 304 the card information from the card 104 via NFC. The mobile device 106 splits 306 the card information into the first portion and the second portion. The full card information is not contained in either the first or second portion. The card information is split in an arbitrary manner, such that the first portion can comprise a different amount of information than the second portion. The mobile device 106 is configured to transmit 308 the first portion to the card 104 via NFC. The mobile device 106 stores 310 the second portion of the card information. The card 104 stores the first portion and is configured to generate a first cryptogram based on the first portion. The mobile device 106 is configured to generate a second cryptogram based on the second portion.

**[0127]** In one aspect, the mobile device 106 scrambles the card information and encrypts the card information. In one aspect, card information is scrambled and encrypted before splitting the card information. In one aspect, the card information is scrambled after it is split but before the first and second partial cryptograms are generated.

**[0128]** In one aspect, the card 104 may be programmed with a first portion of card information and the full card information. Pairing may require registering the card 104 on a mobile application on the mobile device 106 such that the mobile device 106 receives the second portion of the card information from a server. The mobile device 106 stores the second portion of the card information.

**[0129]** FIG. 4 illustrates a method 400 of payment using a modified POS device, according to at least one aspect of the present disclosure. FIG. 4 is described in conjunction

with FIG. 1. In one aspect, the mobile device 106 and the card 104 are paired according to the method 300 of FIG. 3 prior to the payment being initiated. The user 102 initiates 402 a payment at a modified POS device. If no payment is being initiated, the mobile device 106 closes 404 the payment application. The modified POS device is similar to the POS device 108 but the modified POS device includes a multifactor authentication module. The user 102 locates the card 104 within the threshold distance of the modified POS device for NFC to be enabled. For example, the user 102 taps 406 the card 104 on the modified POS device to initiate the NFC payment. The card 104 sends the first cryptogram to the modified POS device. In one aspect, the first cryptogram comprises encrypted and scrambled data according to the method of FIG. 3. In one aspect, the card 104 and mobile device 106 have been paired according to FIG. 3 before the user 102 initiates the payment. In one aspect, the card 104 sends additional metadata bits that indicate that the card information is to be followed by a second factor.

**[0130]** The modified POS determines 408 whether multifactor authentication is enabled. If the multifactor authentication is not enabled, the method 400 proceeds along the No path and executes 410 a regular NFC payment process where the card 104 sends the full set of card information via NFC to the modified POS device. If multifactor authentication is enabled, the method 400 proceeds along the Yes path and the mobile device 106 is located within the threshold distance of the modified POS device for NFC to be operable. For example, the mobile device 106 is located near the modified POS device or tapped to the POS device to send 412 the remaining encrypted and scrambled data to the POS device. In one aspect, the NFC transfer from the mobile device 106 can only happen after a successful biometric verification of the user 102. The mobile device 106 transfers the second cryptogram to the modified POS device. In one aspect, the second cryptogram comprises encrypted and scrambled data according the method of FIG. 3.

**[0131]** The multifactor authentication module of the modified POS device is configured to unscramble and decrypt the first cryptogram and the second cryptogram. The multifactor authentication module of the modified POS device is configured to combine 414 the first cryptogram and the second cryptogram to generate the full cryptogram of the card information. The payment is processed 416 at the modified POS device with the full cryptogram.

**[0132]** FIGS. 5-9 below describe various hardware environments suitable for implementing the system 100 for payment using a mobile device 106 and a card 104 as shown in FIG. 1. The hardware environments described in FIGS. 5-9 may facilitate the implementation of the methods 200, 300, 400 described herein with reference to FIGS. 2-4

using the computer apparatus 3000, computer system 4000, mobile device 5000, card 1000, or payment network 2000 described herein below with reference to FIGS. 5-9. It will be understood by those skilled in the art that the hardware environments shown in FIGS. 5-9 are merely examples and those skilled in the art will appreciate that the system 100 and methods 200, 300, 400 may be implemented in various hardware environments without limiting the scope of the present disclosure and appended claims.

**[0133]** FIG. 5 is a block diagram of a computer apparatus 3000 with data processing subsystems or components, according to at least one aspect of the present disclosure. The subsystems shown in FIG. 5 are interconnected via a system bus 3010. Additional subsystems such as a printer 3018, keyboard 3026, fixed disk 3028 (or other memory comprising computer-readable media), monitor 3022 (which is coupled to a display adapter 3020), and others are shown. Peripherals and input/output (I/O) devices, which couple to an I/O controller 3012 (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as a serial port 3024. For example, the serial port 3024 or external interface 3030 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor 3016 to communicate with each subsystem and to control the execution of instructions from system memory 3014 or the fixed disk 3028, as well as the exchange of information between subsystems. The system memory 3014 and/or the fixed disk 3028 may embody a computer-readable medium.

**[0134]** FIG. 6 is a diagrammatic representation of an example computer system 4000 that includes a host machine 4002 within which a set of instructions to perform any one or more of the methodologies discussed herein may be executed, according to at least one aspect of the present disclosure. In various aspects, the host machine 4002 operates as a stand-alone device or may be connected (e.g., networked) to other machines. In a networked deployment, the host machine 4002 may operate in the capacity of a server or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The host machine 4002 may be a computer or computing device, a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a cellular telephone, a portable music player (e.g., a portable hard drive audio device such as an Moving Picture Experts Group Audio Layer 3 (MP3) player), a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to

include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

**[0135]** The example computer system 4000 includes the host machine 4002, running a host operating system 4004 (OS) on a processor or multiple processor(s)/processor core(s) 4006 (e.g., a central processing unit (CPU), a graphics processing unit (GPU), or both), and various memory nodes 4008. The host OS 4004 may include a hypervisor 4010 that is able to control the functions and/or communicate with a virtual machine ("VM") 4012 running on machine readable media. The VM 4012 also may include a virtual CPU or vCPU 4014. The memory nodes 4008 may be linked or pinned to virtual memory nodes or vNodes 4016. When the memory node 4008 is linked or pinned to a corresponding vNode 4016, then data may be mapped directly from the memory nodes 4008 to their corresponding vNodes 4016.

**[0136]** All the various components shown in host machine 4002 may be connected with and to each other, or communicate to each other via a bus (not shown) or via other coupling or communication channels or mechanisms. The host machine 4002 may further include a video display, audio device or other peripherals 4018 (e.g., a liquid crystal display (LCD), alpha-numeric input device(s) (e.g., a keyboard), a cursor control device (e.g., a mouse), a voice recognition or biometric verification unit, an external drive, or a signal generation device (e.g., a speaker)); a persistent storage device 4020 (also referred to as disk drive unit); and a network interface device 4022. The host machine 4002 may further include a data encryption module (not shown) to encrypt data. The components provided in the host machine 4002 are those typically found in computer systems that may be suitable for use with aspects of the present disclosure and are intended to represent a broad category of such computer components that are known in the art. Thus, the example computer system 4000 can be a server, minicomputer, mainframe computer, or any other computer system. The computer may also include different bus configurations, networked platforms, multi-processor platforms, and the like. Various operating systems may be used including UNIX, LINUX, WINDOWS, QNX ANDROID, IOS, CHROME, TIZEN, and other suitable operating systems.

**[0137]** The disk drive unit 4024 also may be a Solid-state Drive (SSD), a hard disk drive (HDD) or other includes a computer or machine-readable medium on which is stored one or more sets of instructions and data structures (e.g., data/instructions 4026) embodying or utilizing any one or more of the methodologies or functions described herein. The data/instructions 4026 also may reside, completely or at least partially, within the main memory node 4008 and/or within the processor(s) 4006 during execution thereof by the host machine 4002. The data/instructions 4026 may further be transmitted or received over a network 4028 via the network interface device 4022 utilizing any one of several well-known

transfer protocols (e.g., Hyper Text Transfer Protocol (HTTP)).

**[0138]** The processor(s) 4006 and memory nodes 4008 also may comprise machine-readable media. The term "computer-readable medium" or "machine-readable medium" should be taken to include a single medium or multiple medium (e.g., a centralized or distributed database and/or associated caches and servers) that store the one or more sets of instructions. The term "computer-readable medium" shall also be taken to include any medium that is capable of storing, encoding, or carrying a set of instructions for execution by the host machine 4002 and that causes the host machine 4002 to perform any one or more of the methodologies of the present application, or that is capable of storing, encoding, or carrying data structures utilized by or associated with such a set of instructions. The term "computer-readable medium" shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media, and carrier wave signals. Such media may also include, without limitation, hard disks, floppy disks, flash memory cards, digital video discs, random access memory (RAM), read only memory (ROM), and the like. The example aspects described herein may be implemented in an operating environment comprising software installed on a computer, in hardware, or in a combination of software and hardware.

**[0139]** One skilled in the art will recognize that Internet service may be configured to provide Internet access to one or more computing devices that are coupled to the Internet service, and that the computing devices may include one or more processors, buses, memory devices, display devices, input/output devices, and the like. Furthermore, those skilled in the art may appreciate that the Internet service may be coupled to one or more databases, repositories, servers, and the like, which may be utilized to implement any of the various aspects of the disclosure as described herein.

**[0140]** The computer program instructions also may be loaded onto a computer, a server, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

**[0141]** Suitable networks may include or interface with any one or more of, for instance, a local intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network), a MAN (Metropolitan Area Network), a virtual private network (VPN), a storage area network (SAN), a frame relay connection, an Advanced Intelligent Network

(AIN) connection, a synchronous optical network (SONET) connection, a digital T1, T3, E1 or E3 line, Digital Data Service (DDS) connection, DSL (Digital Subscriber Line) connection, an Ethernet connection, an ISDN (Integrated Services Digital Network) line, a dial-up port such as a V.90, V.34 or V.34bis analog modem connection, a cable modem, an ATM (Asynchronous Transfer Mode) connection, or an FDDI (Fiber Distributed Data Interface) or CDDI (Copper Distributed Data Interface) connection. Furthermore, communications may also include links to any of a variety of wireless networks, including WAP (Wireless Application Protocol), GPRS (General Packet Radio Service), GSM (Global System for Mobile Communication), CDMA (Code Division Multiple Access) or TDMA (Time Division Multiple Access), cellular phone networks, GPS (Global Positioning System), CDPD (cellular digital packet data), RIM (Research in Motion, Limited) duplex paging network, Bluetooth radio, or an IEEE 802.11-based radio frequency network. The network 4028 can further include or interface with any one or more of an RS-232 serial connection, an IEEE-1394 (Firewire) connection, a Fiber Channel connection, an IrDA (infrared) port, a SCSI (Small Computer Systems Interface) connection, a USB (Universal Serial Bus) connection or other wired or wireless, digital or analog interface or connection, mesh or Digi® networking.

**[0142]** In general, a cloud-based computing environment is a resource that typically combines the computational power of a large grouping of processors (such as within web servers) and/or that combines the storage capacity of a large grouping of computer memories or storage devices. Systems that provide cloud-based resources may be utilized exclusively by their owners or such systems may be accessible to outside users who deploy applications within the computing infrastructure to obtain the benefit of large computational or storage resources.

**[0143]** The cloud is formed, for example, by a network of web servers that comprise a plurality of computing devices, such as the host machine 4002, with each server 4030 (or at least a plurality thereof) providing processor and/or storage resources. These servers manage workloads provided by multiple users (e.g., cloud resource customers or other users). Typically, each user places workload demands upon the cloud that vary in real-time, sometimes dramatically. The nature and extent of these variations typically depends on the type of business associated with the user.

**[0144]** It is noteworthy that any hardware platform suitable for performing the processing described herein is suitable for use with the technology. The terms “computer-readable storage medium” and “computer-readable storage media” as used herein refer to any medium or media that participate in providing instructions to a CPU for execution. Such media can take many forms, including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical or magnetic disks,

such as a fixed disk. Volatile media include dynamic memory, such as system RAM. Transmission media include coaxial cables, copper wire and fiber optics, among others, including the wires that comprise one aspect of a bus. Transmission media can also take the form of acoustic or light waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Common forms of computer-readable media include, for example, a flexible disk, a hard disk, magnetic tape, any other magnetic medium, a CD-ROM disk, digital video disk (DVD), any other optical medium, any other physical medium with patterns of marks or holes, a RAM, a PROM, an EPROM, an EEPROM, a FLASH EPROM, any other memory chip or data exchange adapter, a carrier wave, or any other medium from which a computer can read.

**[0145]** Various forms of computer-readable media may be involved in carrying one or more sequences of one or more instructions to a CPU for execution. A bus carries the data to system RAM, from which a CPU retrieves and executes the instructions. The instructions received by system RAM can optionally be stored on a fixed disk either before or after execution by a CPU.

**[0146]** Computer program code for carrying out operations for aspects of the present technology may be written in any combination of one or more programming languages, including an object-oriented programming language such as Java, Smalltalk, C++, or the like and conventional procedural programming languages, such as the "C" programming language, Go, Python, or other programming languages, including assembly languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

**[0147]** FIG. 7 illustrates a block diagram of a communication device 5000 that may be used in various embodiments of the present disclosure. The communication device 5000 is representative of the mobile device 106 described in connection with FIG. 1, and may be a cell phone, a feature phone, a smart phone, a satellite phone, or a computing device having a phone capability.

**[0148]** The communication device 5000 may include a processor 5305 (e.g., a microprocessor or microcontroller) for processing the functions of the communication device 5000 and a display 5320 to allow a user to see the phone numbers and other information and messages. The communication device 5000 further may include an input element 5325

to allow a user to input information into the device (e.g., input buttons, touch screen, etc.), a speaker 5330 to allow the user to hear voice communication, music, etc., and a microphone 5335 to allow the user to transmit his or her voice through the communication device 5000. The processor 5310 of the communication device 5000 may connect to a memory 5315. The memory 5315 may be in the form of a computer-readable medium that stores data and, optionally, computer-executable instructions.

**[0149]** The communication device 5000 also may include a communication element 5340 for connection to communication channels (e.g., a cellular telephone network, data transmission network, Wi-Fi network, satellite-phone network, Internet network, Satellite Internet Network, etc.), and in particular to communicate with the card 104 and/or the POS device 108, for example, as shown in FIG. 1. The communication element 5340 may include an associated wireless transfer element, such as an antenna. The communication element 5340 may include a subscriber identity module (SIM) in the form of an integrated circuit that stores an international mobile subscriber identity and the related key used to identify and authenticate a subscriber using the communication device 5000. One or more subscriber identity modules may be removable from the communication device 5000 or embedded in the communication device 5000.

**[0150]** The communication device 5000 further may include a contactless element 5350, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer element, such as an antenna. The contactless element 5350 may be associated with (e.g., embedded within) the communication device 5000 and data or control instructions transmitted via a cellular network, such as for example, a mobile communication network of the mobile service provider, and may be applied to the contactless element 5350 by means of a contactless element interface (not shown). The contactless element interface may function to permit the exchange of data and/or control instructions between mobile device circuitry (and hence the cellular network) and the contactless element 5350.

**[0151]** The contactless element 5350 may be capable of transferring and receiving data using a near field communications (NFC) capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as radio-frequency identification (RFID), Bluetooth, infra-red, or other data transfer capability that can be used to exchange data between the communication device 5000 and an interrogation device. Thus, the communication device 5000 may be capable of communicating and transferring data and/or control instructions via both a cellular network

and near field communications capability.

**[0152]** The data stored in the memory 5315 may include: operation data relating to the operation of the communication device 5000, personal data (e.g., name, date of birth, identification number, etc.), financial data (e.g., bank account information, a bank identification number (BIN), credit or debit card number information, account balance information, expiration date, loyalty provider account numbers, tokens, etc.), transit information (e.g., as in a subway or train pass), access information (e.g., as in access badges), etc. A user may transmit this data from the communication device 5000 to selected receivers.

**[0153]** The communication device 5000 also may comprise a secure element 5302. The secure element 5302 may include a microprocessor integrated circuit, which can store sensitive data and run secure applications such as payment. The secure element can be embedded in any mobile device. The secure element may act as a vault, protecting what is inside the secure element (applications and data) from malware attacks that are typical in the host, such as, for example, the mobile device operating system.

**[0154]** The communication device 5000 may be, amongst other things, a notification device that can receive alert messages and access reports, a portable merchant device that can be used to transmit control data identifying a discount to be applied, or a portable consumer device that can be used to make payments.

**[0155]** FIG. 8 illustrates the internal components of a card 1000 that may be used in accordance with at least one aspect of the present disclosure. The card is representative of the card 104 described in connection with FIG. 1. Embedded within the plastic support 1002, a processor or central processing unit (processor) 1008 is electrically coupled to a display 1004, button 1006, read-only-memory 1010 (ROM), Random Access Memory 1012 (RAM), a non-volatile programmable memory 1014, input/output circuitry 1016, and power supply 1020. It is understood by those familiar with the art that some or all of these elements may be embedded together in some combination as an integrated circuit (IC). Embodiments may also contain a conductive contact-making element 1018.

**[0156]** A processor 1008 may be any central processing unit, microprocessor, micro-controller, computational device or circuit known in the art.

**[0157]** A ROM 1010 is embedded with an operating system.

**[0158]** A non-volatile programmable memory 1014 is configured to be an application

memory device, and may store information such as the card information and the first portion of the card information as described in FIGS 2-4. Examples of non-volatile programmable memory 1014 include, but not limited to: a magnetic stripe, flash memory, Electrically Erasable Programmable Read-Only Memory (EEPROM), or any other non-volatile computer memory or storage known in the art.

**[0159]** The RAM 1012 is any temporary memory storage medium element known in the art. Random access memory is usually (but does not have to be) volatile memory.

**[0160]** The processor 1008, the ROM 1010, the RAM 1012 and the non-volatile programmable memory 1014 may be coupled to one another through an internal bus system. Data can be interchanged between the input/output circuitry 1016, the processor 1008 and the non-volatile programmable memory 1014. Furthermore, data can be interchanged between the processor 1008 and the non-volatile programmable memory 1014.

**[0161]** The processor is configured to execute the instructions stored in the ROM 1010, RAM 1012, or a non-volatile programmable memory 1014. For example, the method steps the card 104 performs in FIGS. 2-4 can be stored in one of the memories and executed by the processor 1008.

**[0162]** Additionally, in some embodiments, the input/output circuitry 1016 is further coupled to a conductive contact-making element 1018 being formed in a surface area of the plastic support 1002. In some embodiments, the conductive contact-making element 1018 may be replaced by a radio frequency (RF) transceiver. Radio frequency embodiments may typically use any RF transceiver known in the art for use in a radio frequency identifier (RFID) application or commonly used in a "pay wave" or "contactless" card. Additionally, the input/output circuitry 1016 may be coupled to a communication circuit 1030. In one aspect, the communication circuit 1030 may be an NFC circuit to enable NFC communication for the card 1000 to execute the necessary functions illustrated in FIGS. 2-4.

**[0163]** The NFC circuit may be capable of transferring and receiving data using a near field communications (NFC) capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as radio-frequency identification (RFID), Bluetooth, infra-red, or other data transfer capability that can be used to exchange data between the card 1000 and an interrogation device. Thus, the card 1000 may be capable of communicating and transferring data and/or control

instructions via NFC.

**[0164]** Power supply 1020 may be any electrical power supply, including a battery, fuel cell, long-term capacitor or any other power storage known in the art. Power supply 1020 may be recharged by applying a direct current voltage. A voltage is applied to the card 1000 as the supply voltage VCC. Example supply voltages include 5 volts, 3.3 volts, or 1.7 volts.

**[0165]** The processor 1008 (card processor circuit) is configured to store account information associated with the cardholder account and store a predetermined threshold based on a transaction amount limit. The account information and pre-determined threshold can be stored in the memory of the card.

**[0166]** The processor 1008 is configured to receive a first transaction information associated with a first transaction and receive a second transaction information associated with a second transaction. The first transaction information comprises a first transaction amount. The second transaction information comprises a second transaction amount;

**[0167]** The processor 1008 is configured to compare the first transaction amount and the predetermined threshold. Based on the comparison of the first transaction amount and the predetermined threshold, the card 1000 generates a full cryptogram from the account information and the first transaction amount to authenticate the first transaction.

**[0168]** The processor 1008 is configured to compare the second transaction amount and the predetermined threshold. Based on a comparison of the second transaction amount and the predetermined transaction threshold, the card 1000 generates a partial cryptogram from the account information and the second transaction amount to authenticate the second transaction.

**[0169]** In one aspect, the processor 1008 is configured to generate the partial cryptogram based on the second transaction amount equaling or exceeding the predetermined threshold. In one aspect, the processor 1008 is configured to generate the full cryptogram based on the first transaction amount being less than the predetermined threshold.

**[0170]** In one aspect, the processor 1008 is configured to store the account information separate from the portion of the account information.

**[0171]** The card 1000 may also comprises a communication circuit 1030 configured to wirelessly connect the processor 1008 to a mobile device (such as mobile device 106). The processor 1008 is configured to transmit, through the communication circuit 1030, the partial

cryptogram to the mobile device (such as mobile device 106).

**[0172]** In one aspect, the processor 1008 is configured to transmit the full cryptogram to a point-of-service device (such as the POS device 108).

**[0173]** FIG. 9 depicts a payment network 2000 that may be used in various in accordance with at least one aspect of the present disclosure. The payment network 2000 is a more detailed representative of the system 100 described in connection with FIG. 1. The card 1000 is representative of the card 104 described in connection with FIG. 1. The card point-of-sale reader/writer 3210 is representative of the POS device 108 described in connection with FIG. 1. The merchant 3200 includes a system to support the display of a real-time card balance, available credit, cash limit, or available cash balance constructed and operative in accordance with an embodiment of the present invention. As shown, in FIG. 9, the merchant 3200 comprises a card point-of-sale reader/writer 3210 that communicates with a merchant central computer 3230 via the merchant's private network 3220. In some embodiments, merchant central computer 3230 may be coupled to the hot list storage 3240.

**[0174]** The card point-of-sale reader/writer 3210 is any device capable of reading a personal account number off the card 1000, and writing the card balance information to the card 1000.

**[0175]** A merchant central computer 3230 is a networked device capable of communicating transaction data with card point-of-sale reader/writer 3210 and transmitting the transaction data over the network 4100 to the acquirer 3300. In some instances, the payment processor 3400 determines whether the transaction should be allowed; in other instances, the payment processor 3400 queries the issuer 3500 to determine whether the card has enough available credit to allow the transaction.

**[0176]** A hot list storage 3240 may be any list, database, or memory structure containing either invalid or valid primary account numbers

**[0177]** Examples of the devices, systems, and methods according to various aspects of the present disclosure are provided below in the following numbered clauses. An aspect of any of the device(s), method(s) and/or system(s) may include any one or more than one, and any combination of, the numbered clauses described below.

**[0178]** Clause 1. A method comprising: receiving, by a card, transaction information from a point-of-service device, wherein the transaction information comprises a transaction amount; receiving, by an application associated with the card, the application running on a

mobile device, the transaction information from the card; and selectively pursuing, by the card, based on the transaction amount, a multifactor authentication that comprises: transmitting, by the card, to the application running on the mobile device, a first partial cryptogram; generating, by the application running on the mobile device, a second partial cryptogram; combining, by the application running on the mobile device, the first partial cryptogram and the second partial cryptogram to form a full cryptogram; and transmitting, by the application running on the mobile device, the full cryptogram to the point-of-service device.

**[0179]** Clause 2. The method of Clause 1, further comprising an initial pairing of the card and the application, the initial pairing comprising: receiving, by the application running on the mobile device, card information; splitting, by the application running on the mobile device, the card information into a first portion and a second portion, wherein the first portion and the second portion comprise less than all of the card information; transmitting, by the application running on the mobile device, the first portion to the card; and storing, by the application running on the mobile device, the second portion.

**[0180]** Clause 3. The method of Clause 2, wherein the first partial cryptogram is based on the first portion of the card information.

**[0181]** Clause 4. The method of Clause 3, wherein the second partial cryptogram is based on the second portion of the card information.

**[0182]** Clause 5. The method of any one of Clauses 1-4, wherein the mobile device and the card are enabled for near field communication, and wherein the method further comprises: receiving, by application running on the mobile device, the first partial cryptogram through the near field communication.

**[0183]** Clause 6. The method of any one of Clauses 1-5, further comprising: storing, by the card, a predetermined threshold based on a transaction amount limit.

**[0184]** Clause 7. The method of Clause 6, wherein the selectively pursuing the multifactor authentication is based on the transaction amount equaling to or exceeding the predetermined threshold.

**[0185]** Clause 8. A method comprising: receiving, by a mobile device, card information associated with a card; splitting, by the mobile device, the card information into a first portion and a second portion, wherein the first portion and the second portion comprise less than all of the card information; transmitting, by the mobile device, the first portion to the card; storing, by the mobile device, the second portion; receiving, by the mobile device, from a point-of-service device, transaction information associated with a transaction by the card; receiving, by the mobile device, a first partial cryptogram from the card; generating, by the mobile device, a second partial cryptogram; combining, by the mobile device, the first partial cryptogram and the second partial cryptogram to form a full cryptogram; and transmitting, by

the mobile device, the full cryptogram to the point-of-service device.

**[0186]** Clause 9. The method of Clause 8, wherein the first partial cryptogram is based on the first portion of the card information.

**[0187]** Clause 10. The method of Clause 9, wherein the second partial cryptogram is based on the second portion of the card information.

**[0188]** Clause 11. The method of any one of Clauses 8-10, wherein the mobile device and the card are enabled for near field communication, and further comprising receiving, by the mobile device, the first partial cryptogram through the near field communication from the card.

**[0189]** Clause 12. The method of any one of Clauses 8-11, further comprising storing, by the card, a predetermined threshold based on a transaction amount limit.

**[0190]** Clause 13. The method of Clause 12, further comprising: initiating a payment for the transaction, wherein the transaction information comprises a transaction amount; and determining, by the card, that the transaction amount exceeds the predetermined threshold; and wherein the combining is based on the transaction amount exceeding the predetermined threshold.

**[0191]** Clause 14. The method of any one of Clauses 12-13, further comprising: initiating a payment for the transaction, wherein the transaction information comprises a transaction amount; determining, by the card, that the transaction amount is above the predetermined threshold; and generating, by the card, the first partial cryptogram, based on the transaction amount exceeding the predetermined threshold.

**[0192]** Clause 15. A payment card associated with a cardholder account, the payment card, comprising: a card processor circuit configured to: store account information associated with the cardholder account; store a predetermined threshold based on a transaction amount limit; receive a first transaction information associated with a first transaction, wherein the first transaction information comprises a first transaction amount; receive a second transaction information associated with a second transaction, wherein the second transaction information comprises a second transaction amount; based on a comparison of the first transaction amount and the predetermined threshold, generate a full cryptogram from the account information and the first transaction amount to authenticate the first transaction; and based on a comparison of the second transaction amount and the predetermined threshold, generate a partial cryptogram from the account information and the second transaction amount to authenticate the second transaction.

**[0193]** Clause 16. The payment card of Clause 15, wherein the card processor circuit is configured to generate the partial cryptogram based on the second transaction amount equaling or exceeding the predetermined threshold.

**[0194]** Clause 17. The payment card of Clause 16, wherein the card processor circuit is

configured to generate the full cryptogram based on the first transaction amount being less than the predetermined threshold.

**[0195]** Clause 18. The payment card of any one of Clauses 15-17, wherein the card processor circuit is configured to store the account information separate from a portion of the account information.

**[0196]** Clause 19. The payment card of any one of Clauses 15-18, further comprising a communication circuit configured to wirelessly connect the card processor circuit to a mobile device, wherein the card processor circuit is configured to transmit, through the communication circuit, the partial cryptogram to the mobile device.

**[0197]** Clause 20. The payment card of any one of Clauses 15-19, wherein the card processor circuit is configured to transmit the full cryptogram to a point of service device.

**[0198]** The foregoing detailed description has set forth various forms of the systems and/or processes via the use of block diagrams, flowcharts, and/or examples. Insofar as such block diagrams, flowcharts, and/or examples contain one or more functions and/or operations, it will be understood by those within the art that each function and/or operation within such block diagrams, flowcharts, and/or examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or virtually any combination thereof. Those skilled in the art will recognize that some aspects of the forms disclosed herein, in whole or in part, can be equivalently implemented in integrated circuits, as one or more computer programs running on one or more computers (e.g., as one or more programs running on one or more computer systems), as one or more programs running on one or more processors (e.g., as one or more programs running on one or more microprocessors), as firmware, or as virtually any combination thereof, and that designing the circuitry and/or writing the code for the software and or firmware would be well within the skill of one of skill in the art in light of this disclosure. In addition, those skilled in the art will appreciate that the mechanisms of the subject matter described herein are capable of being distributed as one or more program products in a variety of forms, and that an illustrative form of the subject matter described herein applies regardless of the particular type of signal bearing medium used to actually carry out the distribution.

**[0199]** Instructions used to program logic to perform various disclosed aspects can be stored within a memory in the system, such as dynamic random access memory (DRAM), cache, flash memory, or other storage. Furthermore, the instructions can be distributed via a network or by way of other computer-readable media. Thus a machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer), but is not limited to, floppy diskettes, optical disks, compact disc,

read-only memory (CD-ROMs), and magneto-optical disks, read-only memory (ROMs), random access memory (RAM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), magnetic or optical cards, flash memory, or a tangible, machine-readable storage used in the transmission of information over the Internet via electrical, optical, acoustical or other forms of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.). Accordingly, the non-transitory computer-readable medium includes any type of tangible machine-readable medium suitable for storing or transmitting electronic instructions or information in a form readable by a machine (e.g., a computer).

**[0200]** Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Python, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer-readable medium, such as RAM, ROM, a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer-readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

**[0201]** As used in any aspect herein, the term “logic” may refer to an app, software, firmware and/or circuitry configured to perform any of the aforementioned operations. Software may be embodied as a software package, code, instructions, instruction sets and/or data recorded on non-transitory computer-readable storage medium. Firmware may be embodied as code, instructions or instruction sets and/or data that are hard-coded (e.g., nonvolatile) in memory devices.

**[0202]** As used in any aspect herein, the terms “component,” “system,” “module” and the like can refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution.

**[0203]** As used in any aspect herein, an “algorithm” refers to a self-consistent sequence of steps leading to a desired result, where a “step” refers to a manipulation of physical quantities and/or logic states which may, though need not necessarily, take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It is common usage to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. These and similar terms may be associated with the appropriate physical quantities and are merely convenient labels applied

to these quantities and/or states.

**[0204]** A network may include a packet switched network. The communication devices may be capable of communicating with each other using a selected packet switched network communications protocol. One example communications protocol may include an Ethernet communications protocol which may be capable of permitting communication using a Transmission Control Protocol/Internet Protocol (TCP/IP). The Ethernet protocol may comply or be compatible with the Ethernet standard published by the Institute of Electrical and Electronics Engineers (IEEE) titled "IEEE 802.3 Standard", published in December, 2008 and/or later versions of this standard. Alternatively or additionally, the communication devices may be capable of communicating with each other using an X.25 communications protocol. The X.25 communications protocol may comply or be compatible with a standard promulgated by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T). Alternatively or additionally, the communication devices may be capable of communicating with each other using a frame relay communications protocol. The frame relay communications protocol may comply or be compatible with a standard promulgated by Consultative Committee for International Telegraph and Telephone (CCITT) and/or the American National Standards Institute (ANSI). Alternatively or additionally, the transceivers may be capable of communicating with each other using an Asynchronous Transfer Mode (ATM) communications protocol. The ATM communications protocol may comply or be compatible with an ATM standard published by the ATM Forum titled "ATM-MPLS Network Interworking 2.0" published August 2001, and/or later versions of this standard. Of course, different and/or after-developed connection-oriented network communication protocols are equally contemplated herein.

**[0205]** Unless specifically stated otherwise as apparent from the foregoing disclosure, it is appreciated that, throughout the present disclosure, discussions using terms such as "processing," "computing," "calculating," "determining," "displaying," or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

**[0206]** One or more components may be referred to herein as "configured to," "configurable to," "operable/operative to," "adapted/adaptable," "able to," "conformable/conformed to," etc. Those skilled in the art will recognize that "configured to" can generally encompass active-state components and/or inactive-state components and/or

standby-state components, unless context requires otherwise.

**[0207]** Those skilled in the art will recognize that, in general, terms used herein, and especially in the appended claims (e.g., bodies of the appended claims) are generally intended as “open” terms (e.g., the term “including” should be interpreted as “including but not limited to,” the term “having” should be interpreted as “having at least,” the term “includes” should be interpreted as “includes but is not limited to,” etc.). It will be further understood by those within the art that if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases “at least one” and “one or more” to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles “a” or “an” limits any particular claim containing such introduced claim recitation to claims containing only one such recitation, even when the same claim includes the introductory phrases “one or more” or “at least one” and indefinite articles such as “a” or “an” (e.g., “a” and/or “an” should typically be interpreted to mean “at least one” or “one or more”); the same holds true for the use of definite articles used to introduce claim recitations.

**[0208]** In addition, even if a specific number of an introduced claim recitation is explicitly recited, those skilled in the art will recognize that such recitation should typically be interpreted to mean at least the recited number (e.g., the bare recitation of “two recitations,” without other modifiers, typically means at least two recitations, or two or more recitations). Furthermore, in those instances where a convention analogous to “at least one of A, B, and C, etc.” is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., “a system having at least one of A, B, and C” would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). In those instances where a convention analogous to “at least one of A, B, or C, etc.” is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., “a system having at least one of A, B, or C” would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). It will be further understood by those within the art that typically a disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms unless context dictates otherwise. For example, the phrase “A or B” will be typically

understood to include the possibilities of “A” or “B” or “A and B.”

**[0209]** With respect to the appended claims, those skilled in the art will appreciate that recited operations therein may generally be performed in any order. Also, although various operational flow diagrams are presented in a sequence(s), it should be understood that the various operations may be performed in other orders than those which are illustrated, or may be performed concurrently. Examples of such alternate orderings may include overlapping, interleaved, interrupted, reordered, incremental, preparatory, supplemental, simultaneous, reverse, or other variant orderings, unless context dictates otherwise. Furthermore, terms like “responsive to,” “related to,” or other past-tense adjectives are generally not intended to exclude such variants, unless context dictates otherwise.

**[0210]** It is worthy to note that any reference to “one aspect,” “an aspect,” “an exemplification,” “one exemplification,” and the like means that a particular feature, structure, or characteristic described in connection with the aspect is included in at least one aspect. Thus, appearances of the phrases “in one aspect,” “in an aspect,” “in an exemplification,” and “in one exemplification” in various places throughout the specification are not necessarily all referring to the same aspect. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner in one or more aspects.

**[0211]** As used herein, the singular form of “a,” “an,” and “the” include the plural references unless the context clearly dictates otherwise.

**[0212]** Any patent application, patent, non-patent publication, or other disclosure material referred to in this specification and/or listed in any Application Data Sheet is incorporated by reference herein, to the extent that the incorporated materials is not inconsistent herewith. As such, and to the extent necessary, the disclosure as explicitly set forth herein supersedes any conflicting material incorporated herein by reference. Any material, or portion thereof, that is said to be incorporated by reference herein, but which conflicts with existing definitions, statements, or other disclosure material set forth herein will only be incorporated to the extent that no conflict arises between that incorporated material and the existing disclosure material. None is admitted to be prior art.

**[0213]** In summary, numerous benefits have been described which result from employing the concepts described herein. The foregoing description of the one or more forms has been presented for purposes of illustration and description. It is not intended to be exhaustive or limiting to the precise form disclosed. Modifications or variations are possible in light of the above teachings. The one or more forms were chosen and described in order

to illustrate principles and practical application to thereby enable one of ordinary skill in the art to utilize the various forms and with various modifications as are suited to the particular use contemplated. It is intended that the claims submitted herewith define the overall scope.

## CLAIMS

What is claimed is:

1. A method comprising:
  - receiving, by a card, transaction information from a point-of-service device, wherein the transaction information comprises a transaction amount;
  - receiving, by an application associated with the card, the application running on a mobile device, the transaction information from the card; and
  - selectively pursuing, by the card, based on the transaction amount, a multifactor authentication that comprises:
    - transmitting, by the card, to the application running on the mobile device, a first partial cryptogram;
    - generating, by the application running on the mobile device, a second partial cryptogram;
    - combining, by the application running on the mobile device, the first partial cryptogram and the second partial cryptogram to form a full cryptogram; and
    - transmitting, by the application running on the mobile device, the full cryptogram to the point-of-service device.
2. The method of claim 1, further comprising an initial pairing of the card and the application, the initial pairing comprising:
  - receiving, by the application running on the mobile device, card information;
  - splitting, by the application running on the mobile device, the card information into a first portion and a second portion, wherein the first portion and the second portion comprise less than all of the card information;
  - transmitting, by the application running on the mobile device, the first portion to the card; and
  - storing, by the application running on the mobile device, the second portion.
3. The method of claim 2, wherein the first partial cryptogram is based on the first portion of the card information.
4. The method of claim 3, wherein the second partial cryptogram is based on the second portion of the card information.

5. The method of claim 1, wherein the mobile device and the card are enabled for near field communication, and wherein the method further comprises:
  - receiving, by application running on the mobile device, the first partial cryptogram through the near field communication.
6. The method of claim 1, further comprising:
  - storing, by the card, a predetermined threshold based on a transaction amount limit.
7. The method of claim 6, wherein the selectively pursuing the multifactor authentication is based on the transaction amount equaling to or exceeding the predetermined threshold.
8. A method comprising:
  - receiving, by a mobile device, card information associated with a card;
  - splitting, by the mobile device, the card information into a first portion and a second portion, wherein the first portion and the second portion comprise less than all of the card information;
  - transmitting, by the mobile device, the first portion to the card;
  - storing, by the mobile device, the second portion;
  - receiving, by the mobile device, from a point-of-service device, transaction information associated with a transaction by the card;
  - receiving, by the mobile device, a first partial cryptogram from the card;
  - generating, by the mobile device, a second partial cryptogram;
  - combining, by the mobile device, the first partial cryptogram and the second partial cryptogram to form a full cryptogram; and
  - transmitting, by the mobile device, the full cryptogram to the point-of-service device.
9. The method of claim 8, wherein the first partial cryptogram is based on the first portion of the card information.
10. The method of claim 9, wherein the second partial cryptogram is based on the second portion of the card information.
11. The method of claim 8, wherein the mobile device and the card are enabled for near field communication, and further comprising receiving, by the mobile device, the first partial cryptogram through the near field communication from the card.

12. The method of claim 8, further comprising storing, by the card, a predetermined threshold based on a transaction amount limit.
13. The method of claim 12, further comprising:  
initiating a payment for the transaction, wherein the transaction information comprises a transaction amount; and  
determining, by the card, that the transaction amount exceeds the predetermined threshold; and  
wherein the combining is based on the transaction amount exceeding the predetermined threshold.
14. The method of claim 12, further comprising:  
initiating a payment for the transaction, wherein the transaction information comprises a transaction amount;  
determining, by the card, that the transaction amount is above the predetermined threshold; and  
generating, by the card, the first partial cryptogram, based on the transaction amount exceeding the predetermined threshold.
15. A payment card associated with a cardholder account, the payment card, comprising:  
a card processor circuit configured to:  
store account information associated with the cardholder account;  
store a predetermined threshold based on a transaction amount limit;  
receive a first transaction information associated with a first transaction,  
wherein the first transaction information comprises a first transaction amount;  
receive a second transaction information associated with a second transaction, wherein the second transaction information comprises a second transaction amount;  
based on a comparison of the first transaction amount and the predetermined threshold, generate a full cryptogram from the account information and the first transaction amount to authenticate the first transaction; and  
based on a comparison of the second transaction amount and the predetermined threshold, generate a partial cryptogram from the account information and the second transaction amount to authenticate the second transaction.

16. The payment card of Claim 15, wherein the card processor circuit is configured to generate the partial cryptogram based on the second transaction amount equaling or exceeding the predetermined threshold.
17. The payment card of Claim 16, wherein the card processor circuit is configured to generate the full cryptogram based on the first transaction amount being less than the predetermined threshold.
18. The payment card of Claim 15, wherein the card processor circuit is configured to store the account information separate from a portion of the account information.
19. The payment card of Claim 15, further comprising a communication circuit configured to wirelessly connect the card processor circuit to a mobile device, wherein the card processor circuit is configured to transmit, through the communication circuit, the partial cryptogram to the mobile device.
20. The payment card of Claim 15, wherein the card processor circuit is configured to transmit the full cryptogram to a point of service device.