SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR INITIATING PULL PAYMENTS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 63/570,321, filed March 27, 2024, the disclosure of which is hereby incorporated by reference in its entirety.

BACKGROUND

1. Technical Field

[0002] This disclosure relates generally to electronic payment processing networks and, in non-limiting embodiments or aspects, to systems, methods, and computer program products for initiating pull payments.

2. Technical Considerations

[0003] A merchant may provide a merchant identifier for a user to input to a mobile device and initiate a transaction. The mobile device may then, based on the merchant identifier, trigger a push payment transaction from the account of the user to the account of the merchant. However, push payments may be slower than pull payments in instances where the payer (*e.g.*, the user) requires information of the payee (*e.g.*, the merchant) and relies on an issuer system of the user's payment device to cause funds to be transferred to the account of the merchant. Furthermore, push payments may experience higher failure rates than pull payments, partly owing to a user inputting the wrong information about the value of the transaction or the merchant identity. Pull payments, in contrast, allow a payee to control the timing of the transaction and lock in a transaction value that is approved by the payer.

[0004] There is a need in the art for a technical framework that permits a user to initiate a pull payment transaction based on information of a merchant, while minimizing risks of user input error and fraud.

SUMMARY

[0005] Accordingly, provided are improved systems, methods, and computer program products for initiating pull payments.

[0006] According to non-limiting embodiments or aspects, provided is a system for initiating pull payments. The system includes at least one processor configured to

receive a transaction request from a mobile device of a user, the transaction request including a merchant identifier, an account identifier, and a transaction value. The at least one processor is also configured to communicate an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity. The at least one processor is further configured to receive the proof of identity from the mobile device. The at least one processor is further configured to, in response to receiving the proof of identity, identify at least one payment enabler system based on the transaction request. The at least one processor is further configured to initiate a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an account associated with the account identifier to a merchant account associated with the merchant identifier.

[0007] In some non-limiting embodiments or aspects, the transaction request may be initiated by the mobile device via an application programming interface of a payment application on the mobile device.

[0008] In some non-limiting embodiments or aspects, the transaction request may be initiated by the mobile device in response to the mobile device scanning encoded indicia, and the encoded indicia scanned by the mobile device may include the merchant identifier.

[0009] In some non-limiting embodiments or aspects, the transaction request initiated by the mobile device may be associated with a push payment transaction type. The transaction request may be configured at least partly based on the merchant identifier.

[0010] In some non-limiting embodiments or aspects, the transaction request initiated by the mobile device may be associated with a pull payment transaction type, the transaction request configured at least partly based on the encoded indicia.

[0011] In some non-limiting embodiments or aspects, the encoded indicia may include a two-dimensional barcode, and the merchant identifier may be encoded in the two-dimensional barcode.

[0012] In some non-limiting embodiments or aspects, the merchant identifier may include a first portion and a second portion, the first portion including an identifier associated with the at least one payment enabler system, and the second portion including an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

[0013] In some non-limiting embodiments or aspects, the at least one processor may be further configured to, before communicating the authentication request to the authentication system, determine the at least one payment enabler system based on the first portion of the merchant identifier, transmit a verification request to the at least one payment enabler system based on the second portion of the merchant identifier, and receive a verification response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.

[0014] According to non-limiting embodiments or aspects, provided is a method for initiating pull payments. The method includes receiving, with at least one processor, a transaction request from a mobile device of a user, the transaction request including a merchant identifier, an account identifier, and a transaction value. The method also includes communicating, with at least one processor, an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity. The method further includes receiving, with at least one processor, the proof of identity from the mobile device. The method further includes, in response to receiving the proof of identity, identifying, with at least one processor, at least one payment enabler system based on the transaction request. The method further includes initiating, with at least one processor, a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an account associated with the account identifier to a merchant account associated with the merchant identifier.

[0015] In some non-limiting embodiments or aspects, the transaction request may be initiated by the mobile device in response to the mobile device scanning encoded indicia, and the encoded indicia scanned by the mobile device may include the merchant identifier.

[0016] In some non-limiting embodiments or aspects, the transaction request initiated by the mobile device may be associated with a pull payment transaction type. The transaction request may be configured at least partly based on the encoded indicia.

[0017] In some non-limiting embodiments or aspects, the encoded indicia may include a two-dimensional barcode, and the merchant identifier may be encoded in the two-dimensional barcode.

[0018] In some non-limiting embodiments or aspects, the merchant identifier may include a first portion and a second portion, the first portion including an identifier associated with the at least one payment enabler system, and the second portion including an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

[0019] In some non-limiting embodiments or aspects, the method may further include, before communicating the authentication request to the authentication system, determining, with at least one processor, the at least one payment enabler system based on the first portion of the merchant identifier, transmitting, with at least one processor, a verification request to the at least one payment enabler system based on the second portion of the merchant identifier, and receiving, with at least one processor, a verification response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.

[0020] According to non-limiting embodiments or aspects, provided is a computer program product for initiating pull payments. The computer program product includes at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to receive a transaction request from a mobile device of a user, the transaction request including a merchant identifier, an account identifier, and a transaction value. The program instructions also cause the at least one processor to communicate an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity. The program instructions further cause the at least one processor to receive the proof of identity from the mobile device. The program instructions further cause the at least one processor to, in response to receiving the proof of identity, identify at least one payment enabler system based on the transaction request. The program instructions further cause the at least one processor to initiate a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an account associated with the account identifier to a merchant account associated with the merchant identifier.

[0021] In some non-limiting embodiments or aspects, the transaction request may be initiated by the mobile device in response to the mobile device scanning encoded

indicia, and the encoded indicia scanned by the mobile device may include the merchant identifier.

[0022] In some non-limiting embodiments or aspects, the transaction request initiated by the mobile device may be associated with a pull payment transaction type. The transaction request may be configured at least partly based on the encoded indicia.

[0023] In some non-limiting embodiments or aspects, the encoded indicia may include a two-dimensional barcode, and the merchant identifier may be encoded in the two-dimensional barcode.

[0024] In some non-limiting embodiments or aspects, the merchant identifier may include a first portion and a second portion, the first portion including an identifier associated with the at least one payment enabler system, and the second portion including an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

[0025] In some non-limiting embodiments or aspects, the program instructions may further cause the at least one processor to, before communicating the authentication request to the authentication system, determine the at least one payment enabler system based on the first portion of the merchant identifier, transmit a verification request to the at least one payment enabler system based on the second portion of the merchant identifier, and receive a verification response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.

[0026] Further non-limiting embodiments or aspects are set forth in the following numbered clauses:

[0027] Clause 1: A system comprising: at least one processor configured to: receive a transaction request from a mobile device of a user, the transaction request comprising a merchant identifier, an account identifier, and a transaction value; communicate an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity; receive the proof of identity from the mobile device; in response to receiving the proof of identity, identify at least one payment enabler system based on the transaction request; and initiate a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an

account associated with the account identifier to a merchant account associated with the merchant identifier.

[0028] Clause 2: The system of clause 1, wherein the transaction request is initiated by the mobile device via an application programming interface of a payment application on the mobile device.

[0029] Clause 3: The system of clause 1 or 2, wherein the transaction request is initiated by the mobile device in response to the mobile device scanning encoded indicia, and wherein the encoded indicia scanned by the mobile device comprises the merchant identifier.

[0030] Clause 4: The system of any of clauses 1-3, wherein the transaction request initiated by the mobile device is associated with a push payment transaction type, the transaction request configured at least partly based on the merchant identifier.

[0031] Clause 5: The system of any of clauses 1-4, wherein the transaction request initiated by the mobile device is associated with a pull payment transaction type, the transaction request configured at least partly based on the encoded indicia.

[0032] Clause 6: The system of any of clauses 1-5, wherein the encoded indicia comprises a two-dimensional barcode, and wherein the merchant identifier is encoded in the two-dimensional barcode.

[0033] Clause 7: The system of any of clauses 1-6, wherein the merchant identifier comprises a first portion and a second portion, the first portion comprising an identifier associated with the at least one payment enabler system, and the second portion comprising an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

[0034] Clause 8: The system of any of clauses 1-7, wherein the at least one processor is further configured to, before communicating the authentication request to the authentication system: determine the at least one payment enabler system based on the first portion of the merchant identifier; transmit a verification request to the at least one payment enabler system based on the second portion of the merchant identifier; and receive a verification response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.

[0035] Clause 9: A method comprising: receiving, with at least one processor, a transaction request from a mobile device of a user, the transaction request comprising

a merchant identifier, an account identifier, and a transaction value; communicating, with at least one processor, an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity; receiving, with at least one processor, the proof of identity from the mobile device; in response to receiving the proof of identity, identifying, with at least one processor, at least one payment enabler system based on the transaction request; and initiating, with at least one processor, a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an account associated with the account identifier to a merchant account associated with the merchant identifier.

[0036] Clause 10: The method of clause 9, wherein the transaction request is initiated by the mobile device in response to the mobile device scanning encoded indicia, and wherein the encoded indicia scanned by the mobile device comprises the merchant identifier.

[0037] Clause 11: The method of clause 9 or 10, wherein the transaction request initiated by the mobile device is associated with a pull payment transaction type, the transaction request configured at least partly based on the encoded indicia.

[0038] Clause 12: The method of any of clauses 9-11, wherein the encoded indicia comprises a two-dimensional barcode, and wherein the merchant identifier is encoded in the two-dimensional barcode.

[0039] Clause 13: The method of any of clauses 9-12, wherein the merchant identifier comprises a first portion and a second portion, the first portion comprising an identifier associated with the at least one payment enabler system, and the second portion comprising an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

[0040] Clause 14: The method of any of clauses 9-13, further comprising, before communicating the authentication request to the authentication system: determining, with at least one processor, the at least one payment enabler system based on the first portion of the merchant identifier; transmitting, with at least one processor, a verification request to the at least one payment enabler system based on the second portion of the merchant identifier; and receiving, with at least one processor, a verification response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.

[0041] Clause 15: A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to: receive a transaction request from a mobile device of a user, the transaction request comprising a merchant identifier, an account identifier, and a transaction value; communicate an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity; receive the proof of identity from the mobile device; in response to receiving the proof of identity, identify at least one payment enabler system based on the transaction request; and initiate a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an account associated with the account identifier to a merchant account associated with the merchant identifier.

[0042] Clause 16: The computer program product of clause 15, wherein the transaction request is initiated by the mobile device in response to the mobile device scanning encoded indicia, and wherein the encoded indicia scanned by the mobile device comprises the merchant identifier.

[0043] Clause 17: The computer program product of clause 15 or 16, wherein the transaction request initiated by the mobile device is associated with a pull payment transaction type, the transaction request configured at least partly based on the encoded indicia.

[0044] Clause 18: The computer program product of any of clauses 15-17, wherein the encoded indicia comprises a two-dimensional barcode, and wherein the merchant identifier is encoded in the two-dimensional barcode.

[0045] Clause 19: The computer program product of any of clauses 15-18, wherein the merchant identifier comprises a first portion and a second portion, the first portion comprising an identifier associated with the at least one payment enabler system, and the second portion comprising an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

[0046] Clause 20: The computer program product of any of clauses 15-19, wherein the program instructions further cause the at least one processor to, before communicating the authentication request to the authentication system: determine the at least one payment enabler system based on the first portion of the merchant identifier; transmit a verification request to the at least one payment enabler system based on the second portion of the merchant identifier; and receive a verification

response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.

[0047] These and other features and characteristics of the present disclosure, as well as the methods of operation and functions of the related elements of structures and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the disclosed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0048] Additional advantages and details are explained in greater detail below with reference to the non-limiting, exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0049] FIG. 1 is a schematic diagram of a system for initiating pull payments, according to some non-limiting embodiments or aspects;

[0050] FIG. 2 is a schematic diagram of example components of one or more devices of FIG. 1, according to some non-limiting embodiments or aspects;

[0051] FIG. 3 is a flow diagram of a method for initiating pull payments, according to some non-limiting embodiments or aspects;

[0052] FIG. 4 is a flow diagram of a method for initiating pull payments, according to some non-limiting embodiments or aspects; and

[0053] FIG. 5 is a schematic diagram of a system for initiating pull payments, according to some non-limiting embodiments or aspects.

DETAILED DESCRIPTION

[0054] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the embodiments as they are oriented in the drawing figures. However, it is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified

to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings, and described in the following specification, are simply exemplary and non-limiting embodiments or aspects of the disclosed subject matter. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0055] Some non-limiting embodiments or aspects may be described herein in connection with thresholds. As used herein, satisfying a threshold may refer to a value being greater than the threshold, more than the threshold, higher than the threshold, greater than or equal to the threshold, less than the threshold, fewer than the threshold, lower than the threshold, less than or equal to the threshold, equal to the threshold, etc.

[0056] No aspect, component, element, structure, act, step, function, instruction, and/or the like used herein should be construed as critical or essential unless explicitly described as such. Also, as used herein, the articles "a" and "an" are intended to include one or more items and may be used interchangeably with "one or more" and "at least one." Furthermore, as used herein, the term "set" is intended to include one or more items (*e.g.*, related items, unrelated items, a combination of related and unrelated items, and/or the like) and may be used interchangeably with "one or more" or "at least one." Where only one item is intended, the term "one" or similar language is used. Also, as used herein, the terms "has," "have," "having," or the like are intended to be open-ended terms. Further, the phrase "based on" is intended to mean "based at least partially on" unless explicitly stated otherwise. In addition, reference to an action being "based on" a condition may refer to the action being "in response to" the condition. For example, the phrases "based on" and "in response to" may, in some non-limiting embodiments or aspects, refer to a condition for automatically triggering an action (*e.g.*, a specific operation of an electronic device, such as a computing device, a processor, and/or the like).

[0057] As used herein, the term "communication" may refer to the reception, receipt, transmission, transfer, provision, and/or the like of data (*e.g.*, information, signals, messages, instructions, commands, and/or the like). For one unit (*e.g.*, a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication 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. This may refer to a direct or indirect connection (*e.g.*, a direct communication

connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments or aspects, a message may refer to a network packet (*e.g.*, a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0058] As used herein, the term "computing device" may refer to one or more electronic devices configured to process data. A computing device may, in some examples, include the necessary components to receive, process, and output data, such as a processor, a display, a memory, an input device, a network interface, and/or the like. A computing device may be a mobile device. 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. A computing device may also be a desktop computer or other form of non-mobile computer.

[0059] As used herein, the term "server" may refer to or include one or more computing devices 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 computing devices (*e.g.*, servers, point-of-sale (POS) devices, mobile devices, etc.) directly or indirectly communicating in the network environment may constitute a "system."

[0060] 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). 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 device, server, or processor, and/or a combination of devices, servers, and/or processors. For example, as used in the specification and the claims, a first device, 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 device, server, or processor recited as performing a second step or a second function.

[0061] As used herein, the term "acquirer institution" may refer to an entity licensed and/or approved by a transaction service provider to originate transactions (*e.g.*, payment transactions) using a payment device associated with the transaction service provider. The transactions the acquirer institution may originate may include payment transactions (*e.g.*, purchases, original credit transactions (OCTs), account funding transactions (AFTs), and/or the like). In some non-limiting embodiments or aspects, an acquirer institution may be a financial institution, such as a bank. As used herein, the term "acquirer system" may refer to one or more computing devices operated by or on behalf of an acquirer institution, such as a server computer executing one or more software applications.

[0062] As used herein, the term "account identifier" may include one or more primary account numbers (PANs), tokens, or other identifiers associated with a customer account. The term "token" may refer to an identifier that is used as a substitute or replacement identifier for an original account identifier, such as a PAN. Account identifiers may be alphanumeric or any combination of characters and/or symbols. Tokens may be associated with a PAN or other original account identifier in one or more data structures (*e.g.*, one or more databases, and/or the like) such that they may be used to conduct a transaction without directly using the original account identifier. In some examples, an original account identifier, such as a PAN, may be associated with a plurality of tokens for different individuals or purposes.

[0063] 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). As an example, a "client device" may refer to one or more POS devices used by a merchant, one or more acquirer host computers used by an acquirer, one or more mobile devices used by a user, one or more computing devices used by a payment device provider system, and/or the like. In some non-limiting embodiments or aspects, a client device may be an electronic device configured to communicate with one or more networks and initiate or facilitate transactions. For example, a client device may include one or more

computers, portable computers, laptop computers, tablet computers, mobile devices, cellular phones, wearable devices (*e.g.*, watches, glasses, lenses, clothing, and/or the like), PDAs, and/or the like. 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).

[0064] As used herein, the terms "electronic wallet" and "electronic wallet application" refer to one or more electronic devices and/or software applications configured to initiate and/or conduct payment transactions. For example, an electronic wallet may include a mobile device executing an electronic wallet application, and may further include server-side software and/or databases for maintaining and providing transaction data to the mobile device. An "electronic wallet provider" may include an entity that provides and/or maintains an electronic wallet for a customer, such as Google Pay®, Android Pay®, Apple Pay®, Samsung Pay®, and/or other like electronic payment systems. In some non-limiting examples, an issuer bank may be an electronic wallet provider.

[0065] As used herein, the term "issuer institution" may refer to one or more entities, such as a bank, that provide accounts to customers for conducting transactions (*e.g.*, payment transactions), such as initiating credit and/or debit payments. For example, an issuer institution may provide an account identifier, such as a PAN, to a customer that uniquely identifies one or more accounts associated with that customer. The account identifier may be embodied on a portable financial device, such as a physical financial instrument, *e.g.*, a payment card, and/or may be electronic and used for electronic payments. The term "issuer system" refers to one or more computer devices operated by or on behalf of an issuer institution, such as a server computer executing one or more software applications. For example, an issuer system may include one or more authorization servers for authorizing a transaction.

[0066] As used herein, the term "merchant" may refer to an individual or entity that provides goods and/or services, or access to goods and/or services, to customers based on a transaction, such as a payment transaction. The term "merchant" or "merchant system" may also 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.

[0067] As used herein, a "point-of-sale (POS) device" may refer to one or more devices, which may be used by a merchant to conduct a transaction (*e.g.*, a payment transaction) and/or process a transaction. For example, a POS device may include one or more client devices. Additionally, or alternatively, a POS device may include peripheral devices, card readers, scanning devices (*e.g.*, code scanners), Bluetooth® communication receivers, near-field communication (NFC) receivers, radio frequency identification (RFID) receivers, and/or other contactless transceivers or receivers, contact-based receivers, payment terminals, and/or the like. As used herein, a "point-of-sale (POS) system" may refer to one or more client devices and/or peripheral devices used by a merchant to conduct a transaction. For example, a POS system may include one or more POS devices and/or other like devices that may be used to conduct a payment transaction. In some non-limiting embodiments or aspects, a POS system (*e.g.*, a merchant POS system) may include one or more server computers programmed or configured to process online payment transactions through webpages, mobile applications, and/or the like.

[0068] As used herein, the term "payment device" may refer to an electronic payment device, a portable financial device, a payment card (*e.g.*, a credit or debit card), a gift card, a smartcard, smart media, a payroll card, a healthcare card, a wristband, 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 PDA, a pager, a security card, a computing device, an access card, a wireless terminal, a transponder, and/or the like. In some non-limiting embodiments or aspects, the payment 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).

[0069] 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 institution. For example, a transaction service provider may include a payment network such as Visa® or any other entity that processes transactions. The term "transaction processing system" may refer to one or more computer systems operated by or on behalf of a transaction service provider, such as a transaction processing server executing one or more software applications. A transaction processing server may include one or more processors

and, in some non-limiting embodiments or aspects, may be operated by or on behalf of a transaction service provider.

[0070] The systems, methods, and computer program products described herein provide a number of technical improvements to electronic payment processing ecosystems. For example, by using encoded indicia (*e.g.*, a one-dimensional barcode, a two-dimensional barcode (*e.g.*, a quick response (QR) code), a character-based code, etc.) to encode data that may be used to initiate a transaction request by a mobile device, the user need not have prior knowledge of identifying information for the merchant. This reduces information asymmetry in the system and removes additional data flows for a user searching for or a merchant transmitting, for example, a merchant identifier. By way of further example, transaction security is greatly improved by involving a proof of identity authentication process (*e.g.*, generating a passcode, receiving the passcode from the user's mobile device, etc.), reducing the number of injection or man-in-the-middle attack points for the system. Furthermore, by initiating a pull payment transaction (*e.g.*, where a recipient merchant causes funds to be transferred, or "pulled", from a user transaction account) in response to the transaction request and satisfied authentication proof—instead of a push payment transaction (*e.g.*, where an issuer of a payment device causes funds to be transferred, or "pushed", from a user transaction account)—the user and merchant can begin the process of transferring funds instead of relying on an issuer system to first generate a push payment transaction. Pull payments also have the advantage of reduced system error, such as resulting from incorrect user input related to transaction amount, merchant account information, and/or the like. Additionally, the described systems and methods may be technically compatible with pre-existing encoded indicia that are configured, at least initially, for push payment transactions. As such, encoded indicia can be ultimately used to trigger a pull payment transaction by modifying an intended push payment transaction flow into a pull payment transaction flow. This flexibility of implementation represents a technical improvement over fixed-rail payment processing solutions.

[0071] FIG. 1 is a schematic diagram of an example system 100 in which devices, systems, and/or methods, described herein, may be implemented. As shown in FIG. 1, system 100 may include transaction processing system 102, authentication system 103, mobile device 104, payment enabler system 105, and communication network 108. Transaction processing system 102, authentication system 103, mobile device

104, and/or payment enabler system 105 may interconnect (*e.g.*, establish a connection to communicate) via wired connections, wireless connections, or a combination of wired and wireless connections.

[0072] Transaction processing system 102 may include one or more computing devices configured to communicate with authentication system 103, mobile device 104, and/or payment enabler system 105 at least partly over communication network 108. Transaction processing system 102 may be configured to receive a transaction request from mobile device 104, communicate an authentication request to authentication system 103, receive a proof of identity from mobile device 104, identify a payment enabler system 105, and initiate a pull payment transaction via the payment enabler system 105. Transaction processing system 102 may include or be in communication with authentication system 103.

[0073] Authentication system 103 may include one or more computing devices configured to communicate with transaction processing system 102, mobile device 104, and/or payment enabler system 105 at least partly over communication network 108. Authentication system 103 may be configured to receive an authentication request from transaction processing system 102, generate a prompt (*e.g.*, message) for proof of identity from the user of mobile device 104, and transmit the prompt for proof of identity to mobile device 104. Authentication system 103 may include or be in communication with transaction processing system 102.

[0074] Mobile device 104 may include one or more computing devices configured to communicate with transaction processing system 102, authentication system 103, and/or payment enabler system 105 at least partly over communication network 108. Mobile device 104 may be configured to scan encoded indicia (*e.g.*, a one-dimensional barcode, a two-dimensional barcode (*e.g.*, a QR code), a character-based code, etc.), generate a transaction request, transmit the transaction request to transaction processing system 102, receive a prompt for proof of identity from authentication system 103, and transmit the proof of identity to transaction processing system 102 and/or authentication system 103. In some non-limiting embodiments or aspects, mobile device 104 may store at least a portion of the program instructions for a mobile application (*e.g.*, a native application stored and operated on mobile device 104).

[0075] Payment enabler system 105 may include one or more computing devices configured to communicate with transaction processing system 102, authentication system 103, and/or mobile device 104 at least partly over communication network 108.

Payment enabler system 105 may be configured to initiate a pull payment transaction based on one or more messages transmitted from transaction processing system 102.

[0076] Communication network 108 may include one or more wired and/or wireless networks over which the systems and devices of system 100 may communicate. For example, communication network 108 may include a cellular network (*e.g.*, a long-term evolution (LTE®) network, a third generation (3G) network, a fourth generation (4G) network, a fifth generation (5G) network, a code division multiple access (CDMA) network, etc.), a public land mobile network (PLMN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a telephone network (*e.g.*, the public switched telephone network (PSTN)), a private network, an ad hoc network, an intranet, the Internet, a fiber optic-based network, a cloud computing network, and/or the like, and/or a combination of these or other types of networks.

[0077] The number and arrangement of systems and devices shown in FIG. 1 are provided as an example. There may be additional systems and/or devices, fewer systems and/or devices, different systems and/or devices, or differently arranged systems and/or devices than those shown in FIG. 1. Furthermore, two or more systems and/or devices shown in FIG. 1 may be implemented within a single system or device, or a single system or device shown in FIG. 1 may be implemented as multiple, distributed devices. Additionally, or alternatively, a set of systems (*e.g.*, one or more systems) or a set of devices (*e.g.*, one or more devices) of system 100 may perform one or more functions described as being performed by another set of systems or another set of devices of system 100.

[0078] In some non-limiting embodiments or aspects, transaction processing system 102 may be configured to perform one or more steps of a method for initiating pull payments. For example, transaction processing system 102 may include at least one processor that is configured to receive a transaction request (*e.g.*, a message configured to initiate a transaction in an electronic payment processing network) from mobile device 104 of a user. The transaction request may include a merchant identifier (*e.g.*, a unique string, number, code, sequence, and/or the like associated with merchant), an account identifier (*e.g.*, a unique string, number, code, sequence, and/or the like, associated with a user transaction account), and a transaction value (*e.g.*, an amount of currency to be exchanged between user and merchant). The at least one processor of transaction processing system 102 may be further configured to communicate an authentication request to authentication system 103. The

authentication request may be triggered by the receipt of the transaction request from mobile device 104. The authentication request may be configured to cause authentication system 103 to prompt (*e.g.*, transmit a message to) the user for a proof of identity.

[0079] In some non-limiting embodiments or aspects, when prompting the user for a proof of identity, authentication system 103 may be caused, via trigger of the authentication request, to generate a passcode (*e.g.*, a one time-password) that may be used by user to authenticate the user's identity (*e.g.*, by proof of possession of a device that is configured to receive the passcode, such as mobile device 104). In response to receiving the authentication request, authentication system 103 may generate the passcode and transmit the passcode to mobile device 104 (*e.g.*, via email, a text-based messaging system, audio call, and/or the like). Mobile device 104 may receive the passcode from authentication system 103. The user of mobile device 104 may input the received passcode into a user interface of mobile device 104 (*e.g.*, a web browser, a native application, and/or the like). The user interface of mobile device 104 may be the same or separate user interface used by mobile device 104 to trigger the transaction request (*e.g.*, in response to scanning the encoded indicia, which may be displayed in connection with a physical or virtual merchant storefront). The user may, by inputting the passcode, cause the passcode to be transmitted to transaction processing system 102 and/or authentication system 103. Transaction processing system 102 and/or authentication system 103, therefore, may receive the passcode from mobile device 104.

[0080] In some non-limiting embodiments or aspects, when prompting the user for a proof of identity, authentication system 103 may be caused, via trigger of the authentication request, to transmit a message to mobile device 104 requesting input by user of credentials (*e.g.*, username, password, key, and/or the like) as a proof of knowledge to prove the user's identity. In response, user may input the credentials into a user interface of mobile device 104, which may or may not be the same interface used by user to initiate the transaction request. Mobile device 104 may transmit the credentials to transaction processing system 102 and/or authentication system 103, and transaction processing system 102 and/or authentication system 103 may verify that the credentials satisfy the requirement for a proof of identity (*e.g.*, the input credentials match a stored set of credentials for the user). It will be appreciated that

additional and/or alternate step-up authentication processes and proofs of identity may be employed to verify the identity of the user.

[0081] In some non-limiting embodiments or aspects, in response to receiving the proof of identity from mobile device 104, transaction processing system 102 may identify payment enabler system 105 based on the transaction request. Payment enabler system 105 may be determined based, at least partly, on the merchant identifier. For example, a first portion of the merchant identifier may include an identifier associated with payment enabler system 105. After payment enabler system 105 is determined, transaction processing system 102 may generate and transmit a message to payment enabler system 105 to cause a pull payment transaction to be initiated. As such, transaction processing system 102 may initiate the pull payment transaction, via payment enabler system 105, to transfer the transaction value from an account associated with the account identifier (*e.g.*, a user transaction account) to a merchant account associated with the merchant identifier (*e.g.*, a merchant transaction account).

[0082] In some non-limiting embodiments or aspects, the transaction request may be initiated by mobile device 104 via an application programming interface (API). As used herein, an API includes a set of defined rules to enable different software programs to communicate with each other, *e.g.*, acting as an intermediary layer that processes data transfers between two or more computing devices. For example, mobile device 104 may initiate the transaction request via an API of a payment application (*e.g.*, a native application, a web-browser-based application, etc.) on mobile device 104 (*e.g.*, executed on, accessed by, etc.), wherein the API is configured to facilitate communication between mobile device 104 and, *e.g.*, transaction processing system 102 and/or authentication system 103. The application programming interface may provide a channel for input on mobile device 104 to be communicated to transaction processing system 102. The user of mobile device 104 may initiate the transaction request using the payment application by inputting one or more of the merchant identifier, the account identifier, and a transaction value. For transaction flows on mobile device 104, merchant identifier and the transaction value may be automatically populated in the payment application by the merchant-side POS device (*e.g.*, a merchant website). User may select a control (*e.g.*, activate a button labeled “submit” or “pay”) to cause the transaction request to be transmitted to transaction processing system 102.

[0083] Additionally, or alternatively, and in some non-limiting embodiments or aspects, transaction request may be initiated by mobile device 104 in response to mobile device 104 scanning (*e.g.*, capturing image data via a camera) encoded indicia. The encoded indicia scanned by mobile device 104 may include the merchant identifier. Certain encoded indicia may be configured with the intent of permitting a push payment transaction—the described systems and methods may still make use of such encoded indicia to ultimately cause a pull payment transaction to be initiated. In such situations, the transaction request initiated by the mobile device may initially be associated with a push payment transaction type, and the configuration of the transaction request may be at least partly based on the merchant identifier. In some non-limiting embodiments or aspects, when mobile device 104 scans encoded indicia, the information encoded in the encoded indicia may be used to initiate a transaction request via an API of a programming application accessed by mobile device 104.

[0084] In some non-limiting embodiments or aspects, the encoded indicia may include encoded data identifying a push payment transaction type, a pull payment transaction type, and/or the like. In latter scenarios, the encoded indicia may be specially generated and may designate pull payment transactions for streamlined use in the disclosed systems. By way of using encoded indicia that identifies a pull payment transaction type from the start, the disclosed systems may avoid needing to reconfigure an initial push payment transaction into a pull payment transaction. For example, the transaction request initiated by mobile device 104 may be associated with a pull payment transaction type. The transaction request may be configured at least partly based on the encoded indicia.

[0085] In some non-limiting embodiments or aspects, the merchant identifier may be a unique identifier (*e.g.*, unique relative to other merchant identifiers) associated with the merchant and payment enabler system 105. For example, the merchant identifier may include a first portion and a second portion (*e.g.*, combined, interleaved, concatenated, etc.). The first portion may include an identifier associated with payment enabler system 105. The second portion may include an identifier associated with the merchant configured to receive payment via payment enabler system 105. For example, the merchant identifier may be configured in the format of “abc@xyz”, where “abc” represents a multi-character alphanumeric sequence assigned to the merchant for use with payment enabler system 105, and where “xyz” represents a multi-character alphanumeric sequence assigned to payment enabler system 105 for

use in the electronic payment processing network. The "xyz" sequence may be used by transaction processing system 102 to determine (*e.g.*, via a lookup table, a searchable database, etc.) payment enabler system 105 for initiating the pull payment transaction. The identifier associated with payment enabler system 105 may be determined based on alias mappings (*e.g.*, represented by the second portion of the merchant identifier).

[0086] In some non-limiting embodiments or aspects, the at least one processor of transaction processing system 102 may be further configured to, before communicating the authentication request to the authentication system, determine payment enabler system 105 based on the first portion of the merchant identifier (*e.g.*, identifying payment enabler system 105 using an identifier associated with payment enabler system 105 in the first portion), transmit a verification request (*e.g.*, a message configured to cause payment enabler system 105 to verify whether the merchant is configured for pull payment transactions) to payment enabler system 105 based on the second portion merchant identifier (*e.g.*, a verification request comprising the second portion), and receive a verification response (*e.g.*, a message configured to identify whether the merchant is configured for pull payment transactions) from payment enabler system 105. In response to the verification response from payment enabler system 105 indicating that the merchant is configured for pull payment transactions via payment enabler system 105, transaction processing system 102 may communicate the authentication request to authentication system 103. In this manner, the authentication process flow can be avoided or triggered at a different part of the transaction sequence if the merchant is not configured for pull payment transactions. This results in computational savings by avoiding wasted messaging and reducing the identity verification burden on transaction processing system 102 and/or authentication system 103.

[0087] In some non-limiting embodiments or aspects, transaction processing system 102 may include authentication system 103, an interoperability service system, a digital configuration platform, and/or a developer portal system. Authentication system 103 of transaction processing system 102 may be configured to provision tokens, generate and validated one-time-passwords (OTPs), and generate cryptograms for payment processing. The interoperability service system of transaction processing system 102 may be configured to manage incoming application programming interface (API) calls related to payment and merchant/key lookup. The

interoperability service system may be further configured to manage outbound calls to payment enabler system 105 (*e.g.*, for initiating payment), and calls to mobile application provider system 502 (*e.g.*, for sending transaction status notifications). The digital configuration platform of transaction processing system 102 may be configured to host client profile metadata (*e.g.*, QR signing public keys, aliasing, API keys, etc.). The developer portal system of transaction processing system 102 may be configured to provide interoperability as a service, including by facilitating client integration with message-level encryption (MLE), whitelisted ports, API keys, and/or the like.

[0088] In some non-limiting embodiments or aspects, payment enabler system 105 may perform a number of roles. For example, payment enabler system 105 may be configured to onboard and maintain system profiles for a plurality of merchants. Payment enabler system 105 may be further configured to collect consent from existing merchants and accept payments from payment devices using previously implemented universal payments interface (UPI) quick response (QR) codes. Payment enabler system 105 may be further configured to deploy QR codes, and to provide an API for merchant lookups. Furthermore, payment enabler system 105 may be further configured to, upon receiving a payment request via the API, communicate with acquirer system 506 and/or a payment gateway for further payment processing in a pull-based model, and to transmit a notification to the interoperability core service of the transaction processing system 102.

[0089] Referring now to FIG. 2, shown is a diagram of example components of a device 200, according to non-limiting embodiments. Device 200 may correspond to transaction processing system 102, authentication system 103, mobile device 104, or payment enabler system 105, as an example. In some non-limiting embodiments, such systems or devices may include at least one device 200 and/or at least one component of device 200. The number and arrangement of components shown are provided as an example. In some non-limiting embodiments, device 200 may include additional components, fewer components, different components, or differently arranged components than those shown. Additionally, or alternatively, a set of components (*e.g.*, one or more components) of device 200 may perform one or more functions described as being performed by another set of components of device 200.

[0090] As shown in FIG. 2, device 200 may include a bus 202, a processor 204, memory 206, a storage component 208, an input component 210, an output

component 212, and a communication interface 214. Bus 202 may include a component that permits communication among the components of device 200. In some non-limiting embodiments, processor 204 may be implemented in hardware, firmware, or a combination of hardware and software. For example, processor 204 may include a processor (*e.g.*, a central processing unit (CPU), a graphics processing unit (GPU), an accelerated processing unit (APU), etc.), a microprocessor, a digital signal processor (DSP), and/or any processing component (*e.g.*, a field-programmable gate array (FPGA), an application-specific integrated circuit (ASIC), etc.) that can be programmed to perform a function. Memory 206 may include random access memory (RAM), read only memory (ROM), and/or another type of dynamic or static storage device (*e.g.*, flash memory, magnetic memory, optical memory, etc.) that stores information and/or instructions for use by processor 204.

[0091] With continued reference to FIG. 2, storage component 208 may store information and/or software related to the operation and use of device 200. For example, storage component 208 may include a hard disk (*e.g.*, a magnetic disk, an optical disk, a magneto-optic disk, a solid-state disk, etc.) and/or another type of computer-readable medium. Input component 210 may include a component that permits device 200 to receive information, such as via user input (*e.g.*, a touch screen display, a keyboard, a keypad, a mouse, a button, a switch, a microphone, etc.). Additionally, or alternatively, input component 210 may include a sensor for sensing information (*e.g.*, a global positioning system (GPS) component, an accelerometer, a gyroscope, an actuator, etc.). Output component 212 may include a component that provides output information from device 200 (*e.g.*, a display, a speaker, one or more light-emitting diodes (LEDs), etc.). Communication interface 214 may include a transceiver-like component (*e.g.*, a transceiver, a separate receiver and transmitter, etc.) that enables device 200 to communicate with other devices, such as via a wired connection, a wireless connection, or a combination of wired and wireless connections. Communication interface 214 may permit device 200 to receive information from another device and/or provide information to another device. For example, communication interface 214 may include an Ethernet interface, an optical interface, a coaxial interface, an infrared interface, a radio frequency (RF) interface, a universal serial bus (USB) interface, a Wi-Fi® interface, a cellular network interface, and/or the like.

[0092] Device 200 may perform one or more processes described herein. Device 200 may perform these processes based on processor 204 executing software instructions stored by a computer-readable medium, such as memory 206 and/or storage component 208. A computer-readable medium may include any non-transitory memory device. A memory device includes memory space located inside of a single physical storage device or memory space spread across multiple physical storage devices. Software instructions may be read into memory 206 and/or storage component 208 from another computer-readable medium or from another device via communication interface 214. When executed, software instructions stored in memory 206 and/or storage component 208 may cause processor 204 to perform one or more processes described herein. Additionally, or alternatively, hardwired circuitry may be used in place of or in combination with software instructions to perform one or more processes described herein. Thus, embodiments described herein are not limited to any specific combination of hardware circuitry and software. The term "configured to," as used herein, may refer to an arrangement of software, device(s), and/or hardware for performing and/or enabling one or more functions (*e.g.*, actions, processes, steps of a process, and/or the like). For example, "a processor configured to" may refer to a processor that executes software instructions (*e.g.*, program code) that cause the processor to perform one or more functions.

[0093] Referring now to FIG. 3, FIG. 3 is a flow diagram of a non-limiting embodiment or aspect of a method 300 for initiating pull payments, according to some non-limiting embodiments or aspects. The steps shown in FIG. 3 are for example purposes only. It will be appreciated that additional, fewer, different, and/or a different order of steps may be used in non-limiting embodiments or aspects. In some non-limiting embodiments or aspects, a step may be automatically performed in response to performance and/or completion of a prior step. In some non-limiting embodiments or aspects, one or more of the steps of method 300 may be performed (*e.g.*, completely, partially, and/or the like) by transaction processing system 102. In some non-limiting embodiments or aspects, one or more of the steps of method 300 may be performed (*e.g.*, completely, partially, and/or the like) by another system, another device, another group of systems, or another group of devices, separate from or including transaction processing system 102.

[0094] As shown in FIG. 3, at step 302, method 300 may include initiating a transaction request. For example, mobile device 104 may initiate a transaction

request (*e.g.*, by generating and transmitting a message to transaction processing system 102). The transaction request may include a merchant identifier, an account identifier, and a transaction value. The account identifier may be automatically inserted to transaction request by mobile device 104 based on information of a payment device stored locally on mobile device 104. The merchant identifier may be automatically inserted based on decoded data generated from scanning encoded indicia, based on data provided by a merchant-side POS system, and/or the like. Additionally, or alternatively, the merchant identifier may include first portion and a second portion. The first portion may include an identifier associated with the at least one payment enabler system 105. The second portion may include an identifier associated with the merchant configured to receive payment via the at least one payment enabler system 105.

[0095] In some non-limiting embodiments or aspects, the transaction request may be initiated by mobile device 104 in response to mobile device 104 scanning encoded indicia. The encoded indicia scanned by mobile device 104 may include the merchant identifier (*e.g.*, encoded into a two-dimensional barcode). The encoded indicia scanned by mobile device 104 may further include an identifier of a pull-payment or push-payment transaction type (*e.g.*, encoded into the two-dimensional barcode). In some non-limiting embodiments or aspects, the transaction request initiated by mobile device 104 may be associated with a push payment transaction type. Additionally, or alternatively, the transaction request initiated by mobile device 104 may be associated with a pull payment transaction type. The transaction request may be configured at least partly based on the merchant identifier, the encoded indicia, and/or the like. In some non-limiting embodiments or aspects, the encoded indicia may include a two-dimensional barcode.

[0096] Additionally, or alternatively, the transaction request may be initiated by mobile device 104 via an API that is configured as an intermediary layer between an application accessed on mobile device 104 and at least one processor of transaction processing system 102,

[0097] As shown in FIG. 3, at step 304, method 300 may include receiving the transaction request. For example, transaction processing system 102 may receive the transaction request from mobile device 104. The transaction request may be initially associated with a push payment transaction type or a pull payment transaction type. For transaction requests initially associated with a push payment transaction type,

transaction processing system 102 may reconfigure the transaction to a pull payment transaction over method 300.

[0098] As shown in FIG. 3, at step 306, method 300 may include communicating an authentication request. For example, transaction processing system 102 may communicate an authentication request to authentication system 103. The authentication request may be configured to, when received by authentication system 103, cause authentication system 103 to prompt the user for a proof of identity. The authentication request may be further configured to, when received by authentication system 103, cause authentication system 103 to transmit the prompt (*e.g.*, message) for a proof of identity to mobile device 104.

[0099] In some non-limiting embodiments or aspects, before communicating the authentication request in step 306, transaction processing system 102 may be configured to perform a verification process to ensure that the merchant is configured for pull payment transactions with the at least one payment enabler system 105. For example, transaction processing system 102 may determine the at least one payment enabler system 105 based on the first portion of the merchant identifier (*e.g.*, an identifier associated with payment enabler system 105). Transaction processing system 102 may further transmit a verification request to the at least one payment enabler system 105 based on the second portion of the merchant identifier (*e.g.*, associated with merchant configured to receive payment via the payment enabler system 105). Transaction processing system 102 may further receive a verification response from the at least one payment enabler system 105. The verification response may indicate whether the merchant is configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system 105.

[0100] As shown in FIG. 3, at step 308, method 300 may include receiving the proof of identity. For example, transaction processing system 102 may receive the proof of identity (*e.g.*, credentials, one-time passcode, etc.) from mobile device 104. In this manner, the user may authenticate their identity via a proof of possession of mobile device 104, and/or a proof of knowledge of secret information.

[0101] As shown in FIG. 3, at step 310, method 300 may include identifying at least one payment enabler system 105. For example, transaction processing system 102 may, in response to receiving the proof of identity from mobile device 104, identify at

least one payment enabler system 105 based on the transaction request. Payment enabler system 105 may be identified based at least partly on the merchant identifier.

[0102] As shown in FIG. 3, at step 312, method 300 may include initiating a pull payment transaction. For example, transaction processing system 102 may initiate a pull payment transaction via payment enabler system 105 that was identified in step 310. The initiated pull payment transaction may be configured to transfer the transaction value from an account associated with the account identifier (*e.g.*, a user transaction account) to a merchant account associated with the merchant identifier (*e.g.*, a merchant transaction account).

[0103] Referring now to FIG. 4, FIG. 4 is a flow diagram of a non-limiting embodiment or aspect of a method 400 for initiating pull payments, according to some non-limiting embodiments or aspects. The steps shown in FIG. 4 are for example purposes only. It will be appreciated that additional, fewer, different, and/or a different order of steps may be used in non-limiting embodiments or aspects. In some non-limiting embodiments or aspects, a step may be automatically performed in response to performance and/or completion of a prior step.

[0104] As shown in FIG. 4, at step 402, method 400 may include accessing a mobile application. For example, user 401 (*e.g.*, a payment device holder) may access a mobile application operated on mobile device 104. The mobile application may be an application provided by a mobile application provider, such as a merchant marketplace application, an issuer banking application, a third party funds transfer application, and/or the like. As such, for the purpose of illustrating method 400, steps involving mobile device 104 (*e.g.*, steps 404, 406, 414, 418, 424, and 434) may also be described as occurring, at least partly, in the mobile application.

[0105] As shown in FIG. 4, at step 404, method 400 may include scanning encoded indicia. For example, user 401 may use the mobile application of mobile device 104 to scan encoded indicia (*e.g.*, a QR code). In some non-limiting embodiments or aspects, the mobile application may make use of a camera of mobile device 104 to scan the encoded indicia, and thereafter mobile device 104 may decode the encoded indicia to acquire, at least partly, a merchant identifier, an identifier of a transaction type, and/or the like. In some non-limiting embodiments or aspects, step 404 may further include receiving, via input by user 401, a selection of a source of funds to be applied to the transaction. This selection may be associated with a payment device

associated with a specific network, a universal payment interface (UPI), and/or the like.

[0106] As shown in FIG. 4, at step 406, method 400 may include fetching merchant details (*e.g.*, identifying information) from transaction processing system 102. For example, mobile device 104 may communicate with transaction processing system 102 to request details of the merchant associated with the scanned encoded indicia. The request may include the data of the scanned encoded indicia (*e.g.*, a merchant identifier). The request may also include the selection by the user 401 of a source of funds. Mobile device 104 may communicate with an interoperability system of transaction processing system 102 to fetch the merchant details.

[0107] As shown in FIG. 4, at step 408, method 400 may include fetching merchant details (*e.g.*, identifying information) from payment enabler system 105. For example, transaction processing system 102 (*e.g.*, an interoperability system thereof) may request merchant details from payment enabler system 105.

[0108] As shown in FIG. 4, at step 410, method 400 may include transmitting merchant details to transaction processing system 102. For example, in response to the request transmitted by transaction processing system 102 in step 408, payment enabler system 105 may transmit the requested merchant details to transaction processing system 102 in step 410. Payment enabler system 105 may include and/or be associated with a database including merchant details for a plurality of merchants that have been configured for pull payment transactions via payment enabler system 105.

[0109] As shown in FIG. 4, at step 412, method 400 may include transmitting merchant details to mobile device 104. For example, in response to receiving the merchant details from payment enabler system 105 in step 410, transaction processing system 102 (*e.g.*, an interoperability system thereof) may forward some or all of the merchant details to mobile device 104 in step 412.

[0110] As shown in FIG. 4, at step 414, method 400 may include displaying at least a portion of the merchant details. For example, mobile device 104 may, in response to receiving merchant details from transaction processing system 102 in step 412, display at least a portion of the merchant details on a display of mobile device 104. Accordingly, user 401 may review the displayed data and verify that user 401 is about to transact with the correct merchant. If user 401 wishes to continue, they may proceed to step 416.

[0111] As shown in FIG. 4, at step 416, method 400 may include initiating a request to pay the merchant. For example, user 401 may, in response to reviewing the displayed merchant details on mobile device 104, proceed with initiating a request to pay the merchant a transaction value to be debited from a transaction account of user 401 and credited to a transaction account of the merchant. The intent of user 401 may be input to mobile device 104 via one or more input components 210.

[0112] As shown in FIG. 4, at step 418, method 400 may include transmitting an authentication request. For example, mobile device 104 may, in response to the input of user 401 indicating a desire to proceed, generate and transmit an authentication request to authentication system 103. In some non-limiting embodiments or aspects, authentication system 103 may include a token provisioning system, and further may be associated with or included in transaction processing system 102. Additionally, or alternatively, mobile device 104 may transmit the authentication request at least partly through transaction processing system 102.

[0113] As shown in FIG. 4, at step 420, method 400 may include generating and transmitting a passcode. For example, in response to receiving the authentication request, authentication system 103 may generate a passcode (*e.g.*, a one-time password (OTP)) and transmit the passcode to user 401 (*e.g.*, via mobile device 104 or another computing device associated with user 401). In some non-limiting embodiments or aspects, authentication system 103 may forward the passcode to an issuer system (*e.g.*, associated with a source of funds designated by user 401), which may transmit the passcode to user 401.

[0114] As shown in FIG. 4, at step 422, method 400 may include entering the passcode. For example, in response to receiving the passcode from authentication system 103, user 401 may input the passcode to a user interface of mobile device 104. User 401 may use, for example, an input component 210 of mobile device 104 to input the passcode received from authentication system 103. Mobile device 104 may communicate, via a backend (*e.g.*, an application programming interface (API), a unique uniform resource locator (URL), etc.) with authentication system 103 and/or transaction processing system 102 to provide the passcode for authentication.

[0115] As shown in FIG. 4, at step 424, method 400 may include transmitting a request to transaction processing system 102. The request may include the passcode. For example, mobile device 104 may transmit a request to transaction processing system 102 to cause transaction processing system 102 to authenticate user 401. By

way of another example, the request may include a packet of data indicating that authentication system 103 has received and verified that the passcode user 401 input was correct. In either case, transaction processing system 102, after determining that user 401 input the correct passcode, may proceed to identify payment enabler system 105 to proceed with the pull payment transaction.

[0116] As shown in FIG. 4, at step 426, method 400 may include identifying payment enabler system 105 and transmitting a transaction request. For example, transaction processing system 102 (*e.g.*, an interoperability system thereof) may, in response to receiving the request from mobile device 104 in step 424, identify payment enabler system 105 and transmit a transaction request to payment enabler system 105.

[0117] As shown in FIG. 4, at step 428, method 400 may include processing the pull payment transaction. For example, the transaction request transmitted from transaction processing system 102 in step 426 may cause payment enabler system 105 to process the pull payment transaction, such as through a payment gateway associated with payment enabler system 105. The pull payment transaction may cause the transaction value to be debited from an account of user 401 and credited to an account of the merchant.

[0118] As shown in FIG. 4, at step 430, method 400 may include transmitting a transaction notification to transaction processing system 102. For example, after processing the pull payment transaction, payment enabler system 105 may generate and transmit a transaction notification (*e.g.*, confirming initiating of the pull payment transaction) to transaction processing system 102 (*e.g.*, an interoperability system thereof). The transaction notification may include transaction data (*e.g.*, transaction date, transaction time, transaction value, transaction description, transaction status, and/or the like).

[0119] As shown in FIG. 4, at step 432, method 400 may include transmitting a transaction notification to mobile device 104. For example, in response to receiving the transaction notification from payment enabler system 105 in step 430, transaction processing system 102 may transmit a transaction notification to mobile device 104, indicating that the pull payment transaction was successfully initiated. In some non-limiting embodiments or aspects, the transaction notification received from payment enabler system 105 in step 430 may be forwarded, modified or unmodified, as the transaction notification in step 432. In some non-limiting embodiments or aspects,

transaction processing system 102 may generate and transmit a separate transaction notification to mobile device 104. The transaction notification of step 432 may include transaction data (*e.g.*, transaction date, transaction time, transaction value, transaction description, transaction status, and/or the like).

[0120] As shown in FIG. 4, at step 434, method 400 may include displaying transaction data. For example, based on the transaction notification transmitted in step 432, mobile device 104 may display some or all of the transaction data to user 401 on a display of mobile device 104. In this manner, user 401 can review the transaction data of the initiated pull payment transaction to verify that the pull payment transaction was successfully processed.

[0121] Referring now to FIG. 5, FIG. 5 is a schematic diagram of a non-limiting embodiment or aspect of a system 500 for initiating pull payments, according to some non-limiting embodiments or aspects. The systems, devices, and configurations shown in FIG. 5 are for example purposes only. One or more systems, devices, or configurations shown in FIG. 5 may be combined with one or more other systems, devices, or configurations, as described herein.

[0122] As shown in FIG. 5, user 401 may be associated with mobile device 104. In some non-limiting embodiments or aspects, user 401 may input data to mobile device 104 and use mobile device 104 to scan encoded indicia. Mobile device 104 may have at least one display configured to display data to user 401 for review by user 401. Mobile device 104 may be further configured as a communication device to communicate with issuer system 507. Additionally, or alternatively, user 401 may possess a separate communication device to communicate with issuer system 507.

[0123] As shown in FIG. 5, mobile device 104 may be communicatively connected to mobile application provider system 502. In some non-limiting embodiments or aspects, mobile device 104 may display a user-facing user interface in a mobile application, and the mobile application may be connected on a backend to mobile application provider system 502, such as through an API. Data transmitted to transaction processing system 102 and/or authentication system 103 from mobile device 104 may be communicated entirely or partly through mobile application provider system 502. Mobile application provider system 502 may be associated with a provider of the mobile application operated on mobile device 104, such as a merchant, an issuer, a third party, and/or the like. For example, a transaction request may be initiated by mobile device 104 scanning encoded indicia, and the transaction

request may be routed to transaction processing system 102 via mobile application provider system 502. Mobile application provider system 502 may connect to transaction processing system 102 via one or more APIs, such as a checkout API, a notification API, and/or the like.

[0124] As shown in FIG. 5, the step-up authentication process may be routed from mobile application provider system 502, through authentication system 103, to issuer system 507. In such a process flow, in response to user 401 requesting to transact with merchant, the intent of user 401 may be transmitted, via a series of messages, from mobile application provider system 502, to authentication system 103, to issuer system 507. Authentication system 103 may cause issuer system 507 to prompt user 401 for a proof of identity. In some non-limiting embodiments or aspects, authentication system 103 may prompt user 401 for a proof of identity by transmitting a request for user input of user credentials (*e.g.*, username, password, key, biometric data, etc.). Additionally, or alternatively, when prompting user 401 for a proof of identity, authentication system 103 may generate and transmit a passcode (*e.g.*, a one-time password) to user 401 for authentication of user 401. User 401 may use mobile device 104 or another communication device to input the passcode and prove the identity of user 401.

[0125] As shown in FIG. 5, transaction processing system 102 may be communicatively connected with onboarding system 508. Onboarding system 508 may be associated with or included in payment enabler system 105, transaction processing system 102, and/or the like. Onboarding system 508 may be configured to communicate with merchant systems to onboard merchants into the described systems. Onboarding may include, at least in part, the preconfiguration of hardware and/or software to allow merchant systems to connect and engage in pull payment transactions via payment enabler system 105. Onboarding system 508 may be overseen and operated by operations personnel 501. Furthermore, onboarding system 508 may include and/or be associated with onboarding (OB) database (DB) 504. OB DB 504 may include information of merchants for use in preconfiguring merchant systems for interoperability with the disclosed system. As part of merchant onboarding, a merchant identifier may be assigned to the merchant, relative to a payment enabler system 105. In some non-limiting embodiments or aspects, onboarding system 508 may further onboard mobile application provider systems 502. Therefore, OB DB 504 may further include information of mobile application provider

systems 502. In some non-limiting embodiments or aspects, onboarding system 508 may further onboard payment enabler systems 105. Therefore, OB DB 504 may further include information of payment enabler systems 105. Onboarding system 508 may further facilitate and store, in OB DB 504, public keys of merchants and/or payment enablers that are used for signing encoded indicia (*e.g.*, two-dimensional barcodes).

[0126] As shown in FIG. 5, transaction processing system 102 may further include and/or be associated with transaction (TXN) database (DB) 505. TXN DB 505 may include information of transactions that were processed by transaction processing system 102. Transaction data stored in TXN DB 505 may include, but is not limited to, transaction data, transaction time, transaction amount, user 401 identifier, merchant identifier, payment device identifier, transaction description, transaction type, and/or the like. Transaction processing system 102 may be communicatively connected with and between acquirer system 506 (*e.g.*, associated with transaction accounts of merchants) and issuer system 507 (*e.g.*, associated with transaction accounts of users 401).

[0127] As shown in FIG. 5, payment enabler system 105 may be communicatively connected to transaction processing system 102 and acquirer system 506. Payment enabler system 105 may receive requests for pull payment transactions from transaction processing system 102 and may communicate with acquirer system 506 to cause the pull payment transaction to be performed. Information about the pull payment transaction may be communicated back to transaction processing system 102 from payment enabler system 105 directly, or indirectly via acquirer system 506. In some non-limiting embodiments or aspects, payment enabler system 105 may be connected to transaction processing system 102 via one or more APIs, such as a confirmation API, a payment API, and/or the like.

[0128] With further reference to FIG. 5, when transaction processing system 102 receives the transaction request from mobile application provider system 502, one or more interoperability system of transaction processing system 102 may determine (*e.g.*, sequentially or in parallel) whether the merchant has been configured with one or more payment enabler system 105. If transaction processing system 102 cannot determine that the merchant is preconfigured for a payment enabler system 105, transaction processing system 102 may revert to a default payment process. Otherwise, transaction processing system 102 may present to user 401 one or more

payment enabler systems 105 to complete the transaction, and user 401 may input a selection of a payment enabler system 105 to complete the transaction. Accordingly, transaction processing system 102 may proceed based on the selection of the user. Additionally, or alternatively, a plurality of interoperability systems of transaction processing system 102 may communicate with one another and publish payment enabler system 105 details on a common directory services and, by communicating with one another, determine which interoperability system and/or payment enabler system 105 is best suited for the involved merchant.

[0129] Although embodiments have been described in detail for the purpose of illustration, it is to be understood that such detail is solely for that purpose and that the disclosure is not limited to the disclosed embodiments or aspects, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present disclosure contemplates that, to the extent possible, one or more features of any embodiment or aspect can be combined with one or more features of any other embodiment or aspect.

WHAT IS CLAIMED IS:

1. A system comprising:

at least one processor configured to:

receive a transaction request from a mobile device of a user, the transaction request comprising a merchant identifier, an account identifier, and a transaction value;

communicate an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity;

receive the proof of identity from the mobile device;

in response to receiving the proof of identity, identify at least one payment enabler system based on the transaction request; and

initiate a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an account associated with the account identifier to a merchant account associated with the merchant identifier.

2. The system of claim 1, wherein the transaction request is initiated by the mobile device via an application programming interface of a payment application on the mobile device.

3. The system of claim 1, wherein the transaction request is initiated by the mobile device in response to the mobile device scanning encoded indicia, and wherein the encoded indicia scanned by the mobile device comprises the merchant identifier.

4. The system of claim 3, wherein the transaction request initiated by the mobile device is associated with a push payment transaction type, the transaction request configured at least partly based on the merchant identifier.

5. The system of claim 3, wherein the transaction request initiated by the mobile device is associated with a pull payment transaction type, the transaction request configured at least partly based on the encoded indicia.

6. The system of claim 3, wherein the encoded indicia comprises a two-dimensional barcode, and wherein the merchant identifier is encoded in the two-dimensional barcode.

7. The system of claim 1, wherein the merchant identifier comprises a first portion and a second portion, the first portion comprising an identifier associated with the at least one payment enabler system, and the second portion comprising an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

8. The system of claim 7, wherein the at least one processor is further configured to, before communicating the authentication request to the authentication system:

determine the at least one payment enabler system based on the first portion of the merchant identifier;

transmit a verification request to the at least one payment enabler system based on the second portion of the merchant identifier; and

receive a verification response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.

9. A method comprising:

receiving, with at least one processor, a transaction request from a mobile device of a user, the transaction request comprising a merchant identifier, an account identifier, and a transaction value;

communicating, with at least one processor, an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity;

receiving, with at least one processor, the proof of identity from the mobile device;

in response to receiving the proof of identity, identifying, with at least one processor, at least one payment enabler system based on the transaction request; and

initiating, with at least one processor, a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an account associated with the account identifier to a merchant account associated with the merchant identifier.

10. The method of claim 9, wherein the transaction request is initiated by the mobile device in response to the mobile device scanning encoded indicia, and wherein the encoded indicia scanned by the mobile device comprises the merchant identifier.

11. The method of claim 10, wherein the transaction request initiated by the mobile device is associated with a pull payment transaction type, the transaction request configured at least partly based on the encoded indicia.

12. The method of claim 10, wherein the encoded indicia comprises a two-dimensional barcode, and wherein the merchant identifier is encoded in the two-dimensional barcode.

13. The method of claim 9, wherein the merchant identifier comprises of a first portion and a second portion, the first portion comprising an identifier associated with the at least one payment enabler system, and the second portion comprising an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

14. The method of claim 13, further comprising, before communicating the authentication request to the authentication system:

determining, with at least one processor, the at least one payment enabler system based on the first portion of the merchant identifier;

transmitting, with at least one processor, a verification request to the at least one payment enabler system based on the second portion of the merchant identifier; and

receiving, with at least one processor, a verification response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.

15. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

receive a transaction request from a mobile device, the transaction request comprising a merchant identifier, an account identifier, and a transaction value;

communicate an authentication request to an authentication system, the authentication request configured to cause the authentication system to prompt the user for a proof of identity;

receive the proof of identity from the mobile device;

in response to receiving the proof of identity, identify at least one payment enabler system based on the transaction request; and

initiate a pull payment transaction, via the at least one payment enabler system, to transfer the transaction value from an account associated with the account identifier to a merchant account associated with the merchant identifier.

16. The computer program product of claim 15, wherein the transaction request is initiated by the mobile device in response to the mobile device scanning encoded indicia, and wherein the encoded indicia scanned by the mobile device comprises the merchant identifier.

17. The computer program product of claim 16, wherein the transaction request initiated by the mobile device is associated with a pull payment transaction type, the transaction request configured at least partly based on the encoded indicia.

18. The computer program product of claim 16, wherein the encoded indicia comprises a two-dimensional barcode, and wherein the merchant identifier is encoded in the two-dimensional barcode.

19. The computer program product of claim 15, wherein the merchant identifier comprises a first portion and a second portion, the first portion comprising an identifier associated with the at least one payment enabler system, and the second portion comprising an identifier associated with a merchant configured to receive payment via the at least one payment enabler system.

20. The computer program product of claim 19, wherein the program instructions further cause the at least one processor to, before communicating the authentication request to the authentication system:

determine the at least one payment enabler system based on the first portion of the merchant identifier;

transmit a verification request to the at least one payment enabler system based on the second portion of the merchant identifier; and

receive a verification response from the at least one payment enabler system, the verification response indicative of the merchant being configured to receive the transaction value from the pull payment transaction via the at least one payment enabler system.