# FLEXIBLE TRANSACTION PROCESSING

## CROSS-REFERENCE TO RELATED APPLICATIONS

**[0001]** This application is a non-provisional application of and claims the benefit of U.S. Provisional Patent Application No. 63/569,597, filed on March 25, 2024, which is herein incorporated by reference in its entirety.

## BACKGROUND

**[0002]** Transaction processing networks rely on bank identification numbers (BIN) to identify card issuers and to route transactions to the appropriate network for processing. BINs have been categorized as binary, in that they identify a specific type of card product. In recent years, alternative ways to fund a transaction have surfaced, such as paying with loyalty points or paying with a short-term loan.

**[0003]** From a technical processing perspective, existing solutions which allow for user choice are inefficient, requiring either of the following: 1) A dual message approach for the network and the ecosystem, whereby a pre-authorization message is used to check for the appropriate source, followed by an authorization message for the actual transaction processing. At scale, this approach almost doubles the amount of real-time messages currently required to support purchases, requiring much higher bandwidth and capacity while increasing latency; and 2) Providing the consumer with multiple payment real credentials (e.g., account numbers associated with physical cards), which are costly (e.g., require physical creation, mailing and renewal of multiple credentials, along with associated efforts to issue multiple digital credentials), and increases fraud and authentication computation efforts in the network (e.g., multiple credentials are more likely to be lost or stolen).

**[0004]** Furthermore, the current BIN based payment network architecture leads to considerable network and ecosystem development efforts every time a new source is introduced since those are hard coded to credential types.

**[0005]** Additionally, the process utilized by users to select sources is inefficient since it places the burden on users to make optimal choices each time without access to full information set and a short time window at checkout to make decisions.

**[0006]** Embodiments of the disclosure address these problem and other problems individually and collectively.

## SUMMARY

**[0007]** One embodiment is related to a method comprising: receiving, by a server computer from a resource provider computer operated by a resource provider, an authorization request message comprising a flexible credential and an amount for a transaction conducted between a user and the resource provider, the flexible credential associated with multiple sources; determining, by the server computer, a subset of user rules of a set of user rules associated with the flexible credential to apply to the transaction; determining, by the server computer, a subset of resource provider rules of the resource provider, based on the subset of user rules to apply to the transaction; and applying, by the server computer, the subset of user rules and the subset of resource provider rules to the transaction.

**[0008]** Another embodiment is related to a server computer comprising: a processor; and a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising: receiving, from a resource provider computer operated by a resource provider, an authorization request message comprising a flexible credential and an amount for a transaction conducted between a user and the resource provider, the flexible credential associated with multiple sources; determining a subset of user rules of a set of user rules associated with the flexible credential to apply to the transaction; determining a subset of resource provider rules of the resource provider based on the subset of user rules to apply to the transaction; and applying the subset of user rules and the subset of resource provider rules to the transaction.

**[0009]** Another embodiment is related to a method comprising: receiving, by a resource provider computer from a user device, a flexible credential for a transaction conducted between a user and a resource provider, wherein the resource provider computer is operated by the resource provider, and wherein the flexible credential is associated with multiple sources; identifying, by the resource provider computer, the flexible credential as being associated with multiple sources using an identification table; determining, by the resource provider computer, one or more resource provider

rules for the transaction; generating, by the resource provider computer, an authorization request message for the transaction, wherein the authorization request message comprises the flexible credential and an amount; and providing, by the resource provider computer, the authorization request message and the one or more resource provider rules to a transport computer to request authorization of the transaction.

**[0010]** Further details regarding embodiments of the disclosure can be found in the Detailed Description and the Figures.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0011]** FIG. 1 shows a block diagram of a system according to embodiments.

**[0012]** FIG. 2 shows a block diagram of components of an example transport computer according to embodiments.

**[0013]** FIG. 3 shows a block diagram of components of an example network processing computer according to embodiments.

**[0014]** FIG. 4 shows a flow diagram illustrating a network processing computer based rule determination interaction processing method according to embodiments.

**[0015]** FIG. 5 shows a flow diagram illustrating an interaction processing method including an alternate network processing computer according to embodiments.

## DETAILED DESCRIPTION

**[0016]** Prior to discussing embodiments of the disclosure, some terms can be described in further detail.

**[0017]** A “user” may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer in some embodiments.

**[0018]** A “user device” may be a device that is operated by a user. Examples of user devices may include a mobile phone, a smart phone, a card, a personal digital

assistant (PDA), a laptop computer, a desktop computer, a server computer, a vehicle such as an automobile, a thin-client device, a tablet PC, etc. Additionally, user devices may be any type of wearable technology device, such as a watch, earpiece, glasses, etc. The user device may include one or more processors capable of processing user input. The user device may also include one or more input sensors for receiving user input. As is known in the art, there are a variety of input sensors capable of detecting user input, such as accelerometers, cameras, microphones, etc. The user input obtained by the input sensors may be from a variety of data input types, including, but not limited to, audio data, visual data, or biometric data. The user device may comprise any electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network.

**[0019]** An "access device" may be any suitable device that provides access to a remote system. An access device may also be used for communicating with a coordination computer, a communication network, or any other suitable system. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS or point of sale devices (e.g., POS terminals), cellular phones, personal digital assistants (PDAs), personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), vending machines, automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

**[0020]** An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a mobile communication or payment device. For example, access devices can have card readers that can include electrical contacts, radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with portable devices such as payment cards.

**[0021]** A "resource provider" may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of resource providers

includes merchants, data providers, transit agencies, governmental entities, venue and dwelling operators, etc.

**[0022]** An "interaction" may include a reciprocal action or influence. An interaction can include a communication, contact, or exchange between parties, devices, and/or entities. Example interactions include a transaction between two parties and a data exchange between two devices. In some embodiments, an interaction can include a user requesting access to secure data, a secure webpage, a secure location, and the like. In other embodiments, an interaction can include a payment transaction in which two devices can interact to facilitate a payment.

**[0023]** "Interaction data" can include data related to and/or recorded during an interaction. In some embodiments, interaction data can be transaction data of the network data. Transaction data can comprise a plurality of data elements with data values.

**[0024]** "Credentials" may comprise any evidence of authority, rights, or entitlement to privileges. For example, access credentials may comprise permissions to access certain tangible or intangible assets, such as a building or a file. Examples of credentials may include passwords, passcodes, or secret messages. In another example, payment credentials may include any suitable information associated with and/or identifying an account (e.g., a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include an "account identifier" such as a PAN (primary account number or "account number"), a token, a subtoken, a gift card number or code, a prepaid card number or code, a user name, an expiration date, a CVV (card verification value), a dCVV (dynamic card verification value), a CVV2 (card verification value 2), a CVC3 card verification value, etc. An example of a PAN is a 16-digit number, such as "4147 0900 0000 1234". In some embodiments, credentials may be considered sensitive information. A "flexible credential" may be one that is associated with multiple sources such as multiple payment account sources. A "flexible credential" may be in the form of a PAN or a token. A "real credential" may be an account number that identifies a specific account. For example, a real credential can be a primary account

number that is associated with an account maintained by an authorizing entity computer.

**[0025]** A "token" can include a substitute identifier for some information. For example, an interaction token may include an identifier for an interaction account that is a substitute for an account identifier, such as a primary account number (PAN). For instance, a token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing transaction processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be a random string of characters. In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a transaction. The token may also be used to represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

**[0026]** "Tokenization" can include a process by which data is replaced with substitute data. For example, an account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the account identifier with a substitute number (e.g., a token) that is associated with the account identifier. Further, tokenization may be applied to other information which may be replaced with a substitute value. Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.

**[0027]** A "token service provider" can include an entity including one or more server computers that generates, processes, and/or maintains tokens. A token service provider may include or be in communication with a token vault where the generated tokens are stored. Specifically, the token vault may maintain one-to-one mapping between a token and the data (e.g., a real account identifier) represented by the token.

A token service provider may provide reports or data output to reporting tools regarding approved, pending, and/or declined token requests. The token service provider may provide data output related to token-based transactions to reporting tools and applications and present the token and/or the data substituted by the token (e.g., real account identifiers) as appropriate in the reporting output.

**[0028]** A "token vault" can include a repository that maintains established token-to-PAN mappings. According to various embodiments, the token vault may also maintain other attributes of the token requestor that may be determined at the time of registration and that may be used by the token server to apply domain restrictions or other controls during transaction processing.

**[0029]** An "authorization request message" may be an electronic message that requests authorization for an interaction. In some embodiments, it is sent to a transaction processing computer and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with International Organization for Standardization (ISO) 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or "account number"), a payment token, a username, an expiration date, etc. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction value, merchant identifier, merchant location, acquirer bank identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

**[0030]** An "authorization response message" may be a message that responds to an authorization request. In some cases, it may be an electronic message reply to an authorization request message generated by an issuing financial institution or a

transaction processing computer. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the transaction processing computer) to the merchant's access device (e.g., POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization.

**[0031]** An "authorizing entity" may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An authorizing entity may operate an authorizing entity computer. An "issuer" may refer to a business entity (e.g., a bank) that issues and optionally maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer, or in some embodiments, a portable device.

**[0032]** A "rule" can include a procedure or set of explicit orders. A rule can indicate how an interaction is to be processed. A rule can depend upon another rule. A rule can be a user rule that is set by a user. A rule can be a resource provider rule that is set by a resource provider. For example, a user rule can indicate that if a transaction amount is above a threshold, then a first source such as a first funding source is to be utilized and if the transaction about is below the threshold, then a second source such as a second funding source is to be utilized. For example, a resource provider rule can be to utilize a first network processing computer if the transaction is a debit transaction and to utilize a second network processing computer if the transaction is a credit transaction.

**[0033]** A "source" can be a place where something is obtained. A "funding source" can include a place from which funds are obtained. A funding source can include an account, such as a user account. An account can be maintained by an issuer and authorizing entity. A funding source can be a particular type of funding source. For example, a funding source can be a credit funding source, a debit funding

source, a points funding source, an installment plan funding source, a cryptocurrency funding source, a rewards funding source, etc.

**[0034]** An "account issuer identification number" can include a value that represents an issuer of accounts. An account issuer identification number can include four to eight digits that can be used to identify an issuer. An account issuer identification number can be a bank identification number (BIN). An account issuer identification number can be included in a credential such as an account number. For example, an account issuer identification number can be the first N digits of an account number for an account that is issued by the an issuer. An account issuer identification number can correspond to a particular type of account issuer identification number. Each type of account issuer identification number can indicate how the related account number can be utilized in an interaction. For example, an account issuer identification number can be a flexible account issuer identification number that can be utilized in flexible interactions involving user rules and resource provider rules. An account issuer identification number can be a credit account issuer identification number, a debit account issuer identification number, a cryptocurrency account issuer identification number, etc. A type of account issuer identification number can be identified using an identification table.

**[0035]** An "identification table" can include a collection of data stored in memory as a series of records relating to identifying account issuer identification number types. An identification table can include a list of account issuer identification number ranges, where each account issuer identification number range corresponds to a type of account issuer identification number.

**[0036]** A "processor" may include a device that processes something. In some embodiments, a processor can include any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include a CPU comprising at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

**[0037]** A "memory" may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

**[0038]** A "server computer" may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

**[0039]** Embodiments allow for a new type of flexible credential including an account issuer identification number (e.g., bank identification number (BIN)), which allows for flexible funding sources based on the characteristics of a current interaction. During the interaction between a resource provider and a user, the user can select to use a credential associated with a flexible account issuer identification number that can relate to multiple funding sources. The resource provider may not know what funding source is to be utilized for the interaction when obtaining the credential but can be guaranteed payment in the interaction. This is a technical shift from how the industry operates today, whereby a BIN equates to specific processing and specific routing options, as it is linked to a specific card product. The new flexible account issuer identification number, according to embodiments, can be utilized as a user credential with an initially undetermined funding source, giving the user the ability to make a decision regarding funding sources prior to or at the time of purchase.

**[0040]** Currently, BINs are assigned by network processing computers to authorizing entities (e.g., issuers), where a BIN identifies a specific type of card product and funding source, such as debit, credit, prepaid, or charge cards. This information is recorded in a database in the network processing computer and made available to the whole processing system through a number of channels (e.g., using an API). The funding source of a BIN currently cannot be changed after it is assigned and is static,

which means that, for example, a user switching accounts from debit to credit must always be issued a new card number from a different BIN.

**[0041]** Embodiments solve such technical problems by creating and utilizing a flexible account issuer identification number in a flexible credential. When an interaction is processed, a system can determine, at any point in time, the funding source associated with the flexible credential through either 1) a rules engine and/or 2) requesting information from a computer in the system.

**[0042]** To solve the technical problem of limited use BINs and to create multiple routing options and funding sources, network processing computers and/or transport computers can route interactions to the appropriate network processing computers based on both resource providers' preferences and users' selections (e.g., as indicated by resource provider rules and user rules, respectively). For example, a resource provider may prefer to use, or is required to use, an unaffiliated domestic debit network for routing purposes, which can be set as a rule. If an authorization request message has a flexible credential, the resource provider computer can indicate the routing preference in the authorization request message. The routing preference can depend upon the user's preferred credential associated with the flexible credential. For example, if a debit funding source is selected as the user's funding choice according to the user rule, then the network processing computer can route the interaction including debit funding source details to the appropriate unaffiliated network for processing. Similarly, if a completely different funding source such as a cryptocurrency is requested, then the issuer/wallet can communicate directly with a cryptocurrency computer to facilitate the interaction.

**[0043]** Embodiments reduce the computational resource burden on the network processing computers and the ecosystem since interactions can be routed based on resource provider choice (e.g., resource provider rules) based on the funding source selected by the user (e.g., user rules), without the need for multiple messages that confirm rules from multiple parties prior to interacting. The reduction in the overall number of messages utilized provides for technical improvements in the latency of the overall network processing computers and reduce the total computational requirements of the system.

**[0044]** In some embodiments, the rules can be created and set by users, resource providers, acquirers, network processers, issuers, etc. In other embodiments, the rules can be generated using artificial intelligence models. For example, an artificial intelligence model, such as a recommendation engine, can provide funding source recommendations to users via smart rules, which can optimize choices and decrease checkout times, allowing for greater throughput in checkout lanes and less hardware. A machine learning model can be utilized to recommend regular interaction based rules. The machine learning model cans also be utilized to create rules recommendations which propose an appropriate funding source based on past behavior. Alternatively, the user can select to utilize custom set user rules or machine learning model created user rules (e.g., always pay for supermarket purchases with debit, always pay for Airline A purchases with the Airline A cobranded card, always apply cross border purchases to multi-currency account, etc.). The machine learning model can also implement a "decide for me" model where users give authority for the system to determine the appropriate account to apply a transaction to.

**[0045]** FIG. 1 shows a system 100 according to embodiments of the disclosure. The system 100 comprises a user device 102, an access device 104, a resource provider computer 106, a transport computer 108, a plurality of network processing computers 110, an authorizing entity computer 112, a user rules database 114, an identification table database 116, and a resource provider rules database 118.

**[0046]** The user device 102 can be in operative communication with the access device 104. The access device 104 can be in operative communication with the resource provider computer 106, which can be in operative communication with the transport computer 108. The transport computer 108 can be in operative communication with the plurality of network processing computers 110. The plurality of network processing computers can be in operative communication with the authorizing entity computer 112. Each network processing computer of the plurality of network processing computers can be in operative communication with one another.

**[0047]** The user rules database 114 can be in operative communication with the authorizing entity computer 112, the plurality of network processing computers 110, and the transport computer 108. The identification table database 116 can be in

operative communication with the authorizing entity computer 112, the plurality of network processing computers 110, the transport computer 108, and the resource provider computer 106. The resource provider rules database 118 can be in operative communication with plurality of network processing computers 110, the transport computer 108, and the resource provider computer 106.

**[0048]** For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1. For example, in some embodiments, there may be a plurality of authorizing entity computers.

**[0049]** Messages between the devices in the system 100 illustrated in FIG. 1 can be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), SSL, ISO (e.g., ISO 8583) and/or the like. The communications network may include any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like. The communications network can use any suitable communications protocol to generate one or more secure communication channels. A communications channel may, in some instances, comprise a secure communication channel, which may be established in any known manner, such as through the use of mutual authentication and a session key, and establishment of a Secure Socket Layer (SSL) session.

**[0050]** The user device 102 can include one or more computers, portable computers, laptop computers, tablet computers, mobile devices, cellular phones, wearable devices (e.g., watches, glasses, lenses, clothing, etc.), personal digital assistants (PDAs), Internet of Things (IoT) devices, and/or the like. The user device 102 can be operated by a user. The user device 102 can initiate interactions (e.g., transactions) with resource provider computers and/or access devices.

**[0051]** The access device 104 can include a device operated by a resource provider. The access device 104, for example, can include a mobile device, a point of sale (POS) terminal, a laptop computer, a desktop computer, etc. The access device 104 can communicate with another device (e.g., a user device 102) to perform an interaction. During the interaction, the access device 104 can receive credentials from the user device and can provide interaction data to the resource provider computer 106 for authorization of the interaction. In some embodiments, the access device 104 can generate an authorization request message comprising at least the interaction data. The access device 104 can provide the authorization request message to the resource provider computer 106.

**[0052]** The resource provider computer 106 can include any suitable computational apparatus operated by a resource provider (e.g., a merchant). In some embodiments, the resource provider computer 106 may include one or more server computers that may host one or more websites associated with the resource provider (e.g., a merchant). In some embodiments, the resource provider computer 106 may be configured to send data to the network processing computer 110 via the transport computer 108 as part of a payment verification and/or authentication process for a transaction between the user (e.g., consumer) and the resource provider. The resource provider computer 106 may also be configured to generate authorization request messages for interactions between a resource provider and a user and route the authorization request messages to the authorizing entity computer 112 for interaction processing.

**[0053]** The transport computer 108 can include a server computer. The transport computer 108 may be associated with an acquirer, which may be an entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers.

**[0054]** The plurality of network processing computers 110 can include network processing computers, which may be server computers. A network processing computer in the plurality of network processing computers 110 may be disposed between the transport computer 108 and the authorizing entity computer 112, as well as a number of other transport computers and authorizing entity computers (not

shown). The network processing computer may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For example, the network processing computer may comprise a server coupled to a network interface (e.g., by an external communication interface), and databases of information. The network processing computer may be representative of a transaction processing network. An exemplary transaction processing network may include VisaNet™. Transaction processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The network processing computer may use any suitable wired or wireless network, including the Internet.

**[0055]** The authorizing entity computer 112 can include a server computer operated by an authorizing entity. The authorizing entity computer 112 may be associated with an authorizing entity, which may be an entity that authorizes a request. An example of an authorizing entity may be an issuer, which may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue and manage an account associated with the user device 102.

**[0056]** The user rules database 114 can include a database that stores user rules. The user rules database 114 can store user rules in association with user credentials or other user identifying data, such as tokens, user identifiers, etc. The user rules database 114 can be a database that is maintained by the transport computer 108, a network processing computer of the plurality of network processing computers 110, or the authorizing entity computer 112.

**[0057]** The user rules database 114 can store user rules that are created by users. For example, a user can access a user rule creation platform via the authorizing entity computer 112, or other computer, to create, modify, and remove user rules.

**[0058]** User rules can relate to how an interaction with a flexible credential is to be processed. User rules can relate to selecting particular funding sources from multiple funding sources based on features of a current interaction. For example, a user rule can modify the funding source for an interaction based on an interaction

amount, a previous interaction, a date, a time, a location, a currency, an amount of current rewards, an amount of current points, and/or any other feature of the interaction and/or devices and entities involved in the interaction.

**[0059]** The identification table database 116 can include one or more identification tables. An identification table can be used to identify a type of account issuer identification number using account issuer identification number ranges. The identification table can store and map account issuer identification number ranges to specific types (e.g., flexible) of account issuer identification numbers. For example, an account issuer identification number range of 0000 to 2999 can be mapped to a type of flexible account issuer identification numbers. Whereas an account issuer identification number range of 3000 to 5999 can be mapped to a type of debit account issuer identification numbers.

**[0060]** The resource provider rules database 118 can include a database that stores resource provider rules. The resource provider rules database 118 can store resource provider rules in association with resource provider identifiers. The resource provider rules database 118 can be maintained by the transport computer 108 and can store resource provider rules for resource providers associated with the transport computer 108. Different transport computers can maintain different resource provider rules.

**[0061]** Resource provider rules can relate to how an interaction is to be processed based on a funding source determined by a user rule. A resource provider rule can depend on a user rule. Resource provider rules can relate to selecting a particular method of processing the interaction based on the funding source. In some cases, a resource provider rule can relate to any data included in the interaction. For example, a resource provider rule can modify the method of processing the interaction based on the funding source and can define which network processing computer among a plurality of network processing computers is to process the interaction. Resource provider rules can also include rules relating to how resource providers might wish to modify or add content to authorization request messages or authorization response messages, or how resource providers may wish to apply certain security rules (e.g., fraud rules) to authorization request messages.

**[0062]** The user rules database 114, the identification table database 116, and the resource provider rules database 118 can be accessible using API commands by the devices in FIG. 1. The user rules database 114, the identification table database 116, and the resource provider rules database 118 can be maintained by a network processing computer of the plurality of network processing computers 110. In some embodiments, the user rules database 114 can be maintained by the authorizing entity computer 112 that issues accounts to users, while the resource provider rules database 118 is maintained by the transport computer 108 for resource providers associated with the transport computer 108.

**[0063]** In some embodiments, there may be one or more of each database. For example, there may be a plurality user rules databases, where each user rules database is maintained by a different network processing computer of the plurality of network processing computers.

**[0064]** The user rules database 114, the identification table database 116, and the resource provider rules database 118 can include any suitable databases. The databases may be a conventional, fault tolerant, relational, scalable, secure database such as those commercially available from Oracle™ or Sybase™.

**[0065]** FIG. 2 shows a block diagram of a transport computer 108 according to embodiments. The exemplary transport computer 108 may comprise a processor 204. The processor 204 may be coupled to a memory 202, a network interface 206, and a computer readable medium 208. The computer readable medium 208 can comprise modules. The computer readable medium 208 can include a rule determination module 208A and a rule application module 208B.

**[0066]** The memory 202 can be used to store data and code. For example, the memory 202 can store interaction data, routing tables, user rules, resource provider rules, etc. The memory 202 may be coupled to the processor 204 internally or externally (e.g., cloud based data storage), and may comprise any combination of volatile and/or non-volatile memory, such as RAM, DRAM, ROM, flash, or any other suitable memory device.

**[0067]** The computer readable medium 208 may comprise code, executable by the processor 204, for performing a method comprising: receiving, from a resource

provider computer operated by a resource provider, an authorization request message comprising a credential and an amount for a transaction conducted between a user and the resource provider, the credential associated with multiple funding sources; determining a subset of user rules of a set of user rules associated with the credential to apply to the transaction; determining a subset of resource provider rules of the resource provider based on the subset of user rules to apply to the transaction; and applying the subset of user rules and the subset of resource provider rules to the transaction.

**[0068]** The rule determination module 208A may comprise code or software, executable by the processor 204, for determining rules. The rule determination module 208A, in conjunction with the processor 204, can determine user rules and resource provider rules. The rule determination module 208A, in conjunction with the processor 204, can determine a subset of user rules of a set of user rules associated with a credential in an authorization request message to apply to an interaction. The rule determination module 208A, in conjunction with the processor 204, can determine a subset of resource provider rules of the resource provider, based on the subset of user rules to apply to the transaction.

**[0069]** To determine user rules, in some embodiments, the credential can include an account issuer identification number that can be located within a range of account issuer identification numbers in the identification table database 116. If the account issuer identification number is within a range that indicates that the account issuer identification number is a flexible account issuer identification number, then the rule determination module 208A, in conjunction with the processor 204, can determine to utilize user rules from the user rules database 114 for the current interaction. The rule determination module 208A, in conjunction with the processor 204, can search the user rules database 114 for a set of user rules that are associated with the credential. The rule determination module 208A, in conjunction with the processor 204, can evaluate the set of user rules to determine a subset of user rules that relate to the current interaction. For example, the current interaction can include an amount of $600, and the rule determination module 208A, in conjunction with the processor 204, can identify a subset of user rules that are satisfied by the amount of $600. For example, a first user rule can indicate to process interactions with an amount greater

than $500 using a first account maintained by an authorizing entity computer. The rule determination module 208A, in conjunction with the processor 204, can identify the first user rule for use in the current interaction.

**[0070]** In other embodiments, the rule determination module 208A, in conjunction with the processor 204, can identify one or more selected user rules in the authorization request message to utilize as the subset of user rules. For example, the user can select one or more user rules on the user device 102 and/or on the access device 104 when initiating the interaction. The one or more selected user rules can be added to the authorization request message or provided along with the authorization request message from the resource provider computer 106. The rule determination module 208A, in conjunction with the processor 204, can utilize the credential in the authorization request message to search the user rules database 114 for user preferences on rule priority. The rule determination module 208A, in conjunction with the processor 204, can determine that selected user rules during an interaction have priority over preselected and stored user rules. The rule determination module 208A, in conjunction with the processor 204, can determine to utilize the one or more selected user rules.

**[0071]** To determine resource provider rules, in some embodiments, the rule determination module 208A, in conjunction with the processor 204, can identify resource provider rules in the resource provider rules database 118. The authorization request message can comprise interaction data that includes a resource provider identifier. The rule determination module 208A, in conjunction with the processor 204, can use the resource provider identifier to identify a set of resource provider rules of the resource provider in the resource provider rules database 118. The rule determination module 208A, in conjunction with the processor 204, can identify a subset of resource provider rules of the set of resource provider rules based on the subset of user rules. The resource provider rules can be dependent on the user rules. For example, a user rule can indicate a funding source of a plurality of funding sources, while a resource provider rules indicates a network processing computer to utilized dependent on the indicated funding source.

**[0072]** In other embodiments, the rule determination module 208A, in conjunction with the processor 204, can identify a subset of resource provider rules

received in or along with the authorization request message received from the resource provider computer 106.

**[0073]** The rule application module 208B may comprise code or software, executable by the processor 204, for applying rules. The rule application module 208B, in conjunction with the processor 204, can apply user rules and resource provider rules to an interaction. The rule application module 208B, in conjunction with the processor 204, can apply user rules and resource provider rules to appropriately route the authorization request message to a network processing computer and authorizing entity computer for authorization.

**[0074]** In some embodiments, the rule application module 208B, in conjunction with the processor 204, can modify the authorization request message based on the user rules and/or the resource provider rules. For example, the rule application module 208B, in conjunction with the processor 204, can modify an authorizing entity identifier in the authorization request message based on a user rule that indicates a particular account to utilize for the interaction. As another example, the rule application module 208B, in conjunction with the processor 204, can modify a network processing computer identifier in the authorization request message based on a resource provider rule that indicates a particular network processing computer to utilize to process the interaction.

**[0075]** The network interface 206 may include an interface that can allow the transport computer 108 to communicate with external computers. The network interface 206 may enable the transport computer 108 to communicate data to and from another device (e.g., the resource provider computer 106, a network processing computer of the plurality of network processing computers 110, etc.). Some examples of the network interface 206 may include a modem, a physical network interface (such as an Ethernet card or other Network Interface Card (NIC)), a virtual network interface, a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, or the like. The wireless protocols enabled by the network interface 206 may include Wi-Fi™. Data transferred via the network interface 206 may be in the form of signals which may be electrical, electromagnetic, optical, or any other signal capable of being received by the external communications interface (collectively referred to as “electronic signals” or “electronic messages”). These electronic

messages that may comprise data or instructions may be provided between the network interface 206 and other devices via a communications path or channel. As noted above, any suitable communication path or channel may be used such as, for instance, a wire or cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, a WAN or LAN network, the Internet, or any other suitable medium.

**[0076]** FIG. 3 shows a block diagram of a network processing computer 300 according to embodiments. The exemplary network processing computer 300 may comprise a processor 304. The processor 304 may be coupled to a memory 302, a network interface 306, and a computer readable medium 308. The computer readable medium 308 can comprise modules. The computer readable medium 308 can include a rule determination module 308A, a rule application module 308B, a tokenization module 308C, and a routing module 308D. The network processing computer 300 can be in operative communication with a database 310.

**[0077]** The memory 302 can be used to store data and code. For example, the memory 302 can store interaction data, routing tables, user rules, resource provider rules, etc. The memory 302 may be coupled to the processor 304 internally or externally (e.g., cloud based data storage), and may comprise any combination of volatile and/or non-volatile memory, such as RAM, DRAM, ROM, flash, or any other suitable memory device.

**[0078]** The computer readable medium 308 may comprise code, executable by the processor 304, for performing a method comprising: receiving, from a resource provider computer operated by a resource provider, an authorization request message comprising a credential and an amount for a transaction conducted between a user and the resource provider, the credential associated with multiple funding sources; determining a subset of user rules of a set of user rules associated with the credential to apply to the transaction; determining a subset of resource provider rules of the resource provider based on the subset of user rules to apply to the transaction; and applying the subset of user rules and the subset of resource provider rules to the transaction.

**[0079]** The rule determination module 308A can be similar to the rule determination module 208A, the rule application module 308B can be similar to the rule application module 208B, and will not be repeated.

**[0080]** The tokenization module 308C can, in conjunction with the processor 304, perform tokenization, de-tokenization, cryptogram verification, etc.

**[0081]** The database 310 can store mappings of real credentials to flexible credentials, as well as the real credentials and the flexible credentials and associated rules and routing information. The database 310 can store a plurality of real credentials and a plurality of flexible credentials. Each real credential and each flexible credential can be stored in association with user identification data, which can include a user identifier, a user device identifier, a username, or other information that uniquely identifies the user. Each flexible credential of the plurality of flexible credentials can be associated with one or more real credentials based on user rules. The database 310 can be a credential mapping database and can be a conventional, fault tolerant, relational, scalable, secure database such as those commercially available from Oracle™ or Sybase™.

**[0082]** The routing module 308D may comprise code or software, executable by the processor 304, for routing authorization request messages and authorization response messages to and from alternate network processing computers, authorizing entity computers, and transport computers. The routing module 308D, in conjunction with the processor 304, can determine a destination computer based on the current message as well as user rules and/or resource provider rules. For example, a resource provider rule for a current interaction can indicate that the interaction is to be processed by an alternate network processing computer that processes cryptocurrency based interactions. The routing module 308D, in conjunction with the processor 304, can format the authorization request message such that the authorization request message is readable by the alternate network processing computer. The routing module 308D, in conjunction with the processor 304, can provide the authorization request message to the alternate network processing computer based on the resource provider rule, rather than forwarding the authorization request message to the authorizing entity computer.

**[0083]** The network interface 306 may include an interface (similar to or different than network interface 206 in FIG. 2) that can allow the network processing computer 300 to communicate with external computers.

**[0084]** FIG. 4 shows a flow diagram illustrating an interaction processing method according to embodiments. The method illustrated in FIG. 4 will be described in the context of a user, operating the user device 102, performing an interaction with a resource provider that operates the resource provider computer 106. The interaction can be a transaction for the user to obtain a particular resource from the resource provider. However, it is understood that other types of interactions can be processed by the system. For example, the interaction can include a request to access a secure webpage, a request to access and transfer data, a request to access a secure location, etc.

**[0085]** Unlike the existing BIN ranges, the new flexible account issuer identification number ranges would not have pre-defined product-level characteristics. Flexible credentials with flexible account issuer identification numbers are not directly assigned in a one-to-one manner with user accounts. A computer that examines the flexible account issuer identification number would not be able to make any assumption about how the interaction would be funded, thus providing for the advantage of user privacy. Computers in the system that store or maintain databases of user rules can determine how the interaction would be funded. The user can determine the funding source, either at the point of sale, or via a pre-defined configuration of user rules that assigns the funding source based on the characteristics of the interaction. For example, the user could set up their credential with the following rules: 1) if an interaction includes an amount less than $50, then pay with a credit account; 2) if the interaction includes an amount between $50 and $500, then pay with an installment plan; and 3) if the interaction includes an amount over $500, then pay with credit account.

**[0086]** In some embodiments, prior to the interaction, the resource provider computer 106 can obtain one or more identification tables from one or more network processing computers including the network processing computer 300. An identification table can indicate account issuer identification number ranges for account issuer identification numbers. Each account issuer identification number range can correspond to a different type of account issuer identification number. For example, a first account issuer identification number range can correspond to a flexible account issuer identification number, a second account issuer identification number

range can correspond to an installment plan account issuer identification number, and a third account issuer identification number range can correspond to a credit account issuer identification number. During an interaction, a credential can indicate a particular type of account issuer identification number for the interaction.

**[0087]** For example, at step 402, identification table database 116 can provide an identification table to the transport computer 108 in response to a request for an identification table. In some embodiments, the identification table can be pushed to the transport computer 108 from the identification table database 116 by the network processing computer 300.

**[0088]** At step 404, the transport computer 108 can provide the identification table to the resource provider computer 106 for use in interactions to determine a type of account issuer identification number for each interaction.

**[0089]** At step 406, the user device 102 can initiate an interaction with the resource provider computer 106. For example, the user device 102 can initiate the interaction via a webpage hosted by the resource provider computer 106. In some embodiments, the user device 102 can communicate with an access device (not shown). The user device 102 can provide a flexible credential to the resource provider computer 106. The user device 102 can indicate a particular resource to obtain from the resource provider for the interaction.

**[0090]** The flexible credential can be issued by an authorizing entity of the authorizing entity computer 112 to the user of the user device 102. The flexible credential can comprise an account issuer identification number for the authorizing entity. In some embodiments, the account issuer identification number can be a flexible account issuer identification number (e.g., a flexible BIN). A flexible account issuer identification number can indicate that the flexible credential is associated with one or more funding sources (e.g., associated with a first debit account, a second debit account, a first credit account, second credit account, a loyalty points account, etc.). The flexible account issuer identification number can be a portion of an account number such as a primary account number (PAN) included in the flexible credential. For example, the flexible account issuer identification number can include a first 4, 5, 6, 7, 8, 10, 14, etc. numbers of an account number.

**[0091]** In some embodiments, the flexible credential can include a token rather than a primary account number to increase security. The token can be assigned to a token based account issuer identification number range, which can act similarly to account number based account issuer identification number ranges. The token account issuer identification number ranges can have the same characteristics of the underling account number, thus allowing the resource provider computer to route the interaction similarly to non-tokenized interactions.

**[0092]** In some embodiments, when interacting with the resource provider computer via a digital wallet application installed on the user device 102, the user can be prompted to select a funding source within the digital wallet application during the interaction. Alternatively, the user may be prompted to select a funding source on an access device. There can be different ways in which the user of the user device 102 can indicate how the interaction is to be funded or processed based on selected user rules.

**[0093]** At step 408, after receiving the flexible credential from the user device 102 for the interaction, the resource provider computer 106 can compare the account issuer identification number from the flexible credential to the identification tables. The resource provider computer 106 can store one or more identification tables, where each identification table can be created by and received from a different network processing computer from different networks via the transport computer 108. The resource provider computer 106 can determine that the account issuer identification number is a flexible account issuer identification number and corresponds to multiple sources (e.g., multiple funding sources).

**[0094]** At step 410, the resource provider computer 106 can generate an authorization request message comprising the flexible credential and an amount for the interaction conducted between the user and the resource provider. The resource provider computer 106 can provide the authorization request message to the transport computer 108.

**[0095]** The authorization request message can also include interaction data. The interaction data can include a resource provider identifier, an amount, a time, a date, a transport computer identifier, a resource identifier, etc.

**[0096]** In some embodiments, the authorization request message can further include resource provider rules. The resource provider rules can indicate rules for how the interaction is to be processed. For example, the resource provider computer 106 can include a resource provider rule to inform the transport computer 108 that if the interaction is a debit transaction (e.g., the flexible account issuer identification number is determined to be used with a funding source that corresponds to a debit account) that the interaction should be routed to an alternative network processing computer. The resource provider rules can also indicate that if the interaction is a credit transaction (e.g., the flexible account issuer identification number is determined to be used with a funding source that corresponds to a credit account) that the interaction should be routed to a particular network processing computer (e.g., the network processing computer 300). The resource provider rules can be in the form of codes, which represent rules which are stored at the network processing computer 300.

**[0097]** Resource provider rules can be created by resource providers and can indicate how the interaction is to be processed. The resource provider rules can depend on the user rules. For example, a resource provider rule can indicate to process the interaction with a first network processing computer based in a first geographic location if the interaction is in a first currency and process the interaction with a second network processing computer based in a second geographic location if the interaction is in a second currency.

**[0098]** In some embodiments, the resource provider computer 106 can provide the resource provider rules to the transport computer 108 prior to the interaction, where the transport computer 108 stores the resource provider rules for utilization during interactions into the resource provider rules database 118.

**[0099]** For example, at step 412, after receiving the authorization request message, the transport computer 108 can identify resource provider rules in the resource provider rules database 118 using a resource provider identifier included in the authorization request message. The transport computer 108 can obtain a superset of resource provider rules that relate to the resource provider computer 106. The transport computer 108 can identify resource provider rules that relate to the current interaction and can create a set of resource provider rules therefrom.

**[0100]** At step 414, after receiving the authorization request message, the transport computer 108 can provide the authorization request message including the amount, the flexible credential, and the set of resource provider rules to the network processing computer 300.

**[0101]** At step 416, the network processing computer 300 can determine a subset of user rules of a set of user rules associated with the flexible credential to apply to the interaction. The network processing computer 300 can store and maintain user rules the user rules database 114.

**[0102]** For example, the network processing computer 300 can identify a set of user rules associated with the flexible credential. For example, the network processing computer 300 can request the set of user rules that are stored in association with the credential from the user rules database 114. The user rules database 114 can provide the set of user rules related to the credential to the network processing computer 300.

**[0103]** After obtaining the set of user rules, the network processing computer 300 can determine the subset of user rules from the set of user rules. The subset of user rules can include user rules that are applicable to the current interaction. For example, a user rule may be applicable to an interaction based on information about the interaction, such as a date, a time, an amount of the interaction, a location of the interaction, a currency of the interaction, etc.

**[0104]** For example, a first rule can be: every interaction on a first credential associated with a flexible account issuer identification number should be processed on a second credential that is associated with a specific account issuer identification number associated with a debit account. A second rule can be: if an interaction includes an amount above $200 on a first credential associated with a flexible account issuer identification number, then the interaction should be processed on a second credential that is associated with a specific account issuer identification number associated with a debit account, else the interaction should be processed on a third credential that is associated with a specific account issuer identification number associated with a credit account. A third rule can be: if an interaction is in a currency of Great Britain Pounds (GBP) on a first credential associated with a flexible account issuer identification number, then the interaction should be processed on a second credential that is associated with a specific account issuer identification number

associated with a debit account that relates to a currency of GBP, else the interaction should be processed on a third credential that is associated with a specific account issuer identification number associated with a debit account that relates to a currency of United States Dollar (USD). A fourth rule can be: for a next interaction with a first credential associated with a flexible account issuer identification number, the interaction should be processed on a second credential that is associated with a specific account issuer identification number associated with a debit account, and then revert back to a third credential that is associated with a specific account issuer identification number associated with a credit account.

**[0105]** The network processing computer 300 can select a real credential associated with an identified source (e.g., a funding source), and may replace the flexible credential with the real credential in the authorization request message before forwarding the authorization request message to the authorizing entity computer 112 associated with the flexible credential and the real credential. the network processing computer 300 can store a mapping of the flexible credential to the real credentials it is associated with in a database (e.g., 310 in FIG. 3). For example, the network processing computer 300 can modify the authorization request message by removing the flexible credential from the authorization request message and adding the real credential into the authorization request message.

**[0106]** In some embodiments, user rules related to interaction processing for different users can be stored and/or determined by a rules engine that includes a machine learning model. The rules engine can be maintained by the network processing computer 300. The rules engine can store dynamic rules pertaining to funding source(s).

**[0107]** As an example, the rules engine can be a recommendation engine that can recommend user rules to users. The recommendation engine can be an artificial intelligence system that that recommends things to users. The recommendation engine can utilize machine learning models to determine patterns in interactions, user behavior, user preferences, etc. to recommend user rules for users.

**[0108]** The recommendation engine can be trained with data such as ratings, reviews, interaction success rates, user behaviors and/or any other data related to interactions and/or the devices and entities involved in the interactions. The user

behaviors can include, for example, comments, likes, browsing history, digital cart events, past interactions, search history, etc.

**[0109]** The recommendation engine can be a collaborative filtering system, a content-based filtering system, or a hybrid recommendation system, which is a hybrid of the collaborative filtering system and the content-based filtering system.

**[0110]** A collaborative filtering system can filter recommendations based on a particular user's likeness to other users. Collaborative recommender systems can rely on explicit and implicit data and assume that users with comparable preferences will likely be interested in the same items and potentially interact with them in similar ways in the future. There are two main kinds of collaborative filtering systems, which can be utilized by embodiments to determine user rule recommendations: memory-based and model-based. Memory-based systems can represent users and items as a matrix and can be an extension of the k-nearest neighbors (KNN) algorithm, since the aim of the memory-based system is to find nearest neighbors, which can be similar users or similar user rules. Model-based systems create and utilize a predictive machine learning model of the data. A user-item matrix can serve as a training data set for the machine learning model, which can generate predictions for missing values, that is, user rules that a user has not yet utilize and will therefore be recommended.

**[0111]** A content-based filtering system can filter recommendations based on features of a user rule. Content-based recommender systems can assume that if a user is associated with a particular user rule, then the user can also be associated with another similar user rule. Content-based filtering considers item descriptions such as category, price, and other metadata assigned by keywords and tags, along with explicit and implicit data. Content-based filtering systems can represent user rules and users as vectors in a vector space. Proximity is used to determine the similarity between user rules. The closer two vectors are in space, the more similar they are considered to be. Vectors similar to previous user rules according to their supplied features will be recommended to the user. Content-based recommenders can apply a user-based classifier or regression model.

**[0112]** At step 418, after determining the subset of user rules, the network processing computer 300 can determine a subset of resource provider rules of the resource provider rules based on the subset of user rules to apply to the interaction.

The network processing computer 300 can determine the subset of resource provider rules based on 1) the interaction, 2) the subset of user rules, and 3) a set of resource provider rules received from the transport computer 108.

**[0113]** For example, the network processing computer 300 can analyze the set of resource provider rules to determine if one or more resource provider rules are applicable to both the interaction and the user rules of the subset of user rules. The network processing computer 300 can filter the set of resource provider rules using features of the interaction, such as interaction amount, date, time, involved devices and entities, location, currency type, etc. For example, a current interaction can take place in California. The set of resource provider rules can include a different resource provider rule for different states in the United States. The network processing computer 300 can filter the set of resource provider rules by the location. The network processing computer 300 can further filter the set of resource provider rules using the subset of user rules. For example, a user rule can indicate that the interaction is to be processed using a particular cryptocurrency. The network processing computer 300 can filter the resource provider rules based on the use of the cryptocurrency. For example, the network processing computer 300 can determine that a resource provider rule of processing cryptocurrency based interaction using an alternate network processing computer can be selected as a resource provider rule that is applicable to the current interaction and is to be included in the subset of resource provider rules.

**[0114]** As another example, the subset of user rules can include a rule that the interaction is to be processed using a debit account maintained by the authorizing entity computer 112 if the interaction amount is less than $10. The network processing computer 300 can also determine that a resource provider rule of “process debit account related interactions using the network processing computer 300” is applicable to the current interaction if the current interaction has an interaction amount less than $10.

**[0115]** At step 420, the network processing computer 300 can apply the subset of user rules and the subset of resource provider rules to the interaction. As an example, the subset of user rules can include a user rule that indicates to process the interaction using a first account, which can be a loyalty points account, that is

maintained by the authorizing entity computer 112. The subset of resource provider rules can include a resource provider rule that indicates to use the network processing computer 300 to process the interaction if the interaction relates to loyalty points. As such, the network processing computer 300 can process the interaction and can prepare to provide the authorization request message to the authorizing entity computer 112. In some embodiments, applying a rule to an interaction can include executing logic included in the rule to modify how the interaction itself is processed.

**[0116]** At step 422, after applying the subset of user rules and the subset of resource provider rules to the interaction, the network processing computer 300 can provide the authorization request message comprising the transaction amount and the real credential associated with the selected funding source to the authorizing entity computer 112. As such, the network processing computer 300 can provide the real credential to the authorizing entity computer 112 for authorization rather than the flexible credential. The real credential can indicate a particular funding source such as a particular account that is maintained by the authorizing entity computer 112. The real credential can be a primary account number that identifies the account.

**[0117]** At step 424, after receiving the authorization request message comprising the transaction amount and the real credential associated with the selected funding source from the network processing computer 300, the authorizing entity computer 112 can determine whether or not to authorize the interaction. The authorizing entity computer 112 can determine whether or not to authorize the interaction based on any criteria related to the user, the user device 102, the resource provider, the resource provider computer 106, the account, the interaction, a determined risk score, etc. The authorizing entity computer 112 can generate an indication of whether or not the interaction is authorized.

**[0118]** The authorizing entity computer 112 can generate an authorization response message comprising the indication of whether or not the interaction is authorized. The authorizing entity computer 112 can also include an indication of how the interaction was processed and/or authorized. For example, the authorizing entity computer 112 can include information related to the type of account utilized for the interaction (e.g., a loyalty points account). As such, the authorization response message can indicate which type of funding source was utilized for the interaction and

can include the real credential. Such information can be beneficial for the resource provider computer 106, since at this point in the process, the resource provider computer 106 may not know what type of source (e.g., funding source) is being utilized for the interaction (e.g., funding source data).

**[0119]** At step 426, after generating the authorization response message, the authorizing entity computer 112 can provide the authorization response message to the network processing computer 300.

**[0120]** At step 428, after receiving the authorization response message, the network processing computer 300 can provide the authorization response message to the transport computer 108. The network processing computer 300 can replace the real credential with the flexible credential. For example, the network processing computer 300 can identify the flexible credential based on the real credential. The network processing computer 300 can modify the authorization response message to remove the real credential and add the flexible credential. By doing so, the system can solve a technical problem of real credential security, by switching the real credential with the flexible credential when communicating with the transport computer 108 and the resource provider computer 106.

**[0121]** At step 430, the transport computer 108 can provide the authorization response message to the resource provider computer 106.

**[0122]** At step 432, after receiving the authorization response message from the transport computer 108, the resource provider computer 106 can provide the authorization response message and/or the indication of whether or not the interaction is authorized to the user device 102.

**[0123]** FIG. 5 shows a flow diagram illustrating an interaction processing method including an alternate network processing computer according to embodiments. The method illustrated in FIG. 5 will be described in the context of a user, operating the user device 102, performing an interaction with a resource provider that operates the resource provider computer 106. The interaction can be a transaction for the user to obtain a particular resource from the resource provider. For the interaction, a user rule can indicate to utilize an installment plan, while a resource

provider rule can indicate to process installment plans with an alternate network processing computer 500.

**[0124]** Steps 502-514 are similar to steps 402-414 that are described in reference to FIG. 4 and will not be repeated here.

**[0125]** In some embodiments, at step 516, after receiving an authorization request message comprising a flexible credential and an amount as well as receiving one or more resource provider rules for the interaction, the network processing computer 300 can verify that the flexible credential relates to a flexible account issuer identification number. The network processing computer 300 can obtain an account issuer identification number from the credential (e.g., a first six numbers of the credential). The network processing computer 300 can search the identification table database 116 to determine an account issuer identification number range that encompasses the account issuer identification number from the credential. The network processing computer 300 can determine the type of the account issuer identification number based on the account issuer identification number range. For example, the network processing computer 300 can determine that the account issuer identification number from the credential is a flexible account issuer identification number and the interaction can be processed using user rules and resource provider rules.

**[0126]** At step 518, after identifying the user credential as being associated with a flexible account issuer identification number, the network processing computer 300 can generate a user rule request message comprising the credential. The network processing computer 300 can provide the user rule request message to the authorizing entity computer 112.

**[0127]** At step 520, the authorizing entity computer 112 can determine a subset of user rules from a set of user rules stored in the user rule database 114 and are associated with the credential.

**[0128]** At step 522, the authorizing entity computer 112 can generate a user rule response message comprising the subset of user rules. The authorizing entity computer 112 can provide the user rule response message to the network processing computer 300.

**[0129]** At step 524, after receiving the user rule response message, the network processing computer 300 can determine which, if any, of the resource provider rules are relevant to the subset of user rules that are to be applied to the interaction. The network processing computer 300 can apply the subset of user rules and a subset of resource provider rules to the interaction. In some embodiments, applying a rule to an interaction can modify how the interaction is processed by the interaction processing system. Additionally, apply rules can modify which computers in the interaction processing system are to process the interaction.

**[0130]** For example, the subset of user rules can include a rule to utilize an installment plan for the current interaction. The subset of resource provider rules can include a rule to utilize the alternate network processing computer if the current interaction is processed using installment plans.

**[0131]** The network processing computer 300 can apply the user rules and the resource provider rules to the interaction by routing the authorization request message to the alternate network processing computer 500. In some embodiments, the network processing computer 300 can include the subset of user rules and the subset of resource provider rules into the authorization request message.

**[0132]** The network processing computer 300 can also replace the flexible credential with the real credential in the authorization request message and provide the authorization request message comprising the transaction amount and the real credential associated with the selected funding source to the authorizing entity computer 112. For example, the network processing computer 300 can identify a real credential that is indicated in a particular user rule. The network processing computer 300 can remove the flexible credential from the authorization request message and can include the real credential into the authorization request message.

**[0133]** At step 526, the network processing computer 300 can provide the authorization request message comprising the real credential and the transaction amount to the alternate network processing computer 500.

**[0134]** At step 528, after receiving the authorization request message, the alternate network processing computer 500 can perform any additional processing for the interaction and/or the authorization request message. For example, the alternate

network processing computer 500 can authenticate the user of the user device 102 using an additional communication channel (e.g., email, text message, etc.). The alternate network processing computer 500 can then provide the authorization request message to the authorizing entity computer 112 for authorization.

**[0135]** At step 530, the authorizing entity computer 112 can determine whether or not to authorize the interaction and can generate an authorization response message. For example, after receiving the authorization request message, the authorizing entity computer 112 can determine whether or not to authorize the interaction. The authorizing entity computer 112 can generate an indication of whether or not the interaction is authorized. The authorizing entity computer 112 can generate an authorization response message comprising the real credential and the indication of whether or not the interaction is authorized. In some embodiments, the authorization response message can further include information related to how the interaction was processed (e.g., the interaction was processed as a debit interaction, as a credit interaction, as an installment plan interaction, etc.).

**[0136]** At step 532, the authorizing entity computer 112 can provide the authorization response message to the alternate network processing computer 500.

**[0137]** At step 534, after receiving the authorization response message from the authorizing entity computer 112, the alternate network processing computer 500 can replace the real credential with the flexible credential and provide the authorization response message to the network processing computer 300.

**[0138]** At step 536, the network processing computer 300 can provide the authorization response message to the transport computer 108 in response to the authorization request message.

**[0139]** At step 538, the transport computer 108 can provide the authorization response message to the resource provider computer 106.

**[0140]** At step 540, after receiving the authorization response message from the transport computer 108, the resource provider computer 106 can provide the authorization response message and/or the indication of whether or not the interaction is authorized to the user device 102. After receiving the authorization response message, the resource provider computer 106 can identify the funding source utilized

in the interaction based on funding source data included in the authorization response message by the authorizing entity computer 112.

**[0141]** In some embodiments, a user of the user device 102 can perform an interaction with a resource provider that operates the resource provider computer 106. The interaction can be a transaction for the user to obtain a particular resource from the resource provider. The transport computer 108 can access user rules and resource provider rules that can influence the processing of the interaction. For example, the transport computer 108 can obtain one or more user rules for the interaction from a user rule database using an API call, where the user rule database is maintained by the transport computer 108, the network processing computer 300, or the authorizing entity computer 112.

**[0142]** In some embodiments, the transport computer 108 can obtain and store a set of user rules associated with the credential to apply to the interaction. The transport computer 108 can determine a subset of user rules of a set of user rules associated with the credential, determine a subset of resource provider rules of the resource provider, based on the subset of user rules, and apply the subset of user rules and the subset of resource provider rules to the transaction.

**[0143]** Embodiments of the disclosure have a number of advantages. For example, embodiments reduce network bandwidth and latency. Embodiments reduce the number of real-time messages currently required in the ecosystem to support user choice purchases, which require higher bandwidth and capacity while increasing latency.

**[0144]** Embodiments provide for additional advantages. For example, embodiments reduce credential issuance efforts, fraud, and computational resources for authentication. Embodiments reduce efforts associated with physical and digital issuance of multiple credentials to user, along with reduce fraud and authentication efforts in the network.

**[0145]** Embodiments provide for a technical improvement in data privacy and a reduction in fraud. For example, by switching between a flexible credential and a real credential, the real credential can be kept private from not only computers and devices present in the system (e.g., in FIG. 1), but also from man-in-the-middle cyberattacks

against the system. The exposure of a real credential is minimized due to the flexible credential. As another example, the real credential can be kept private from the resource provider during an interaction.

**[0146]** Embodiments provide for additional advantages. For example, embodiments reduce recurring development efforts. Embodiments also reduce future network and ecosystem development actions, allowing for the introduction/usage of new funding sources on an ongoing basis (e.g., cryptocurrencies, points, etc.) without major network and ecosystem changes.

**[0147]** Although the steps in the flowcharts and process flows described above are illustrated or described in a specific order, it is understood that embodiments of the invention may include methods that have the steps in different orders. In addition, steps may be omitted or added and may still be within embodiments of the invention.

**[0148]** Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions or commands on a computer readable medium for storage and/or transmission, suitable media include random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

**[0149]** Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g., a hard drive, a CD, or an entire computer system), and may be present on or within

different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

**[0150]** The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

**[0151]** One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

**[0152]** As used herein, the use of "a," "an," or "the" is intended to mean "at least one," unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a server computer from a resource provider computer operated by a resource provider, an authorization request message comprising a flexible credential and an amount for a transaction conducted between a user and the resource provider, the flexible credential associated with multiple sources;

determining, by the server computer, a subset of user rules of a set of user rules associated with the flexible credential to apply to the transaction;

determining, by the server computer, a subset of resource provider rules of the resource provider, based on the subset of user rules to apply to the transaction; and

applying, by the server computer, the subset of user rules and the subset of resource provider rules to the transaction.

2. The method of claim 1, wherein the server computer is a network processing computer or is a transport computer.

3. The method of claim 1, wherein the subset of user rules comprises use of a first type of card for the transaction, and the subset of resource provider rules comprises use of a first network processing computer of a plurality of network processing computers to process the transaction.

4. The method of claim 1, wherein a machine learning model determines the subset of user rules and the subset of resource provider rules.

5. The method of claim 1, wherein determining the subset of user rules of the set of user rules associated with the flexible credential comprises:

identifying, by the server computer, the subset of user rules in a user rules database using the flexible credential.

6. The method of claim 1, wherein the flexible credential comprises a flexible account issuer identification number corresponding to an authorizing entity.

7. The method of claim 1 further comprising:

providing, by the server computer, an identification table to the resource provider computer, wherein the identification table includes account issuer identification number ranges that identify one or more types of account issuer identification numbers.

8. The method of claim 7, wherein the resource provider computer identifies the flexible credential as corresponding to a flexible account issuer identification number using the identification table, determines one or more resource provider rules for the transaction based on the flexible account issuer identification number, and includes the one or more resource provider rules in the authorization request message.

9. The method of claim 1, wherein the authorization request message further comprises one or more resource provider rules, and wherein determining the subset of resource provider rules comprises:

selecting, by the server computer, the subset of resource provider rules from the one or more resource provider rules using subset of user rules.

10. The method of claim 1, wherein applying the subset of user rules and the subset of resource provider rules to the transaction comprises:

routing, by the server computer, the authorization request message to an alternate network processing computer.

11. The method of claim 1, wherein applying the subset of user rules and the subset of resource provider rules to the transaction comprises:

modifying, by the server computer, the authorization request message to include an indication of a source of the multiple sources based on the subset of user rules.

12. The method of claim 1 further comprising:

removing, by the server computer, the flexible credential from the authorization request message; and

including, by the server computer, a real credential in place of the flexible credential into the authorization request message.

13. The method of claim 1, wherein determining the subset of user rules comprises:

generating, by the server computer, a user rule request message comprising the flexible credential;

providing, by the server computer, the user rule request message to an authorizing entity computer, wherein the authorizing entity computer determines the subset of user rules from the set of user rules stored in a user rule database in association with the flexible credential; and

receiving, by the server computer, a user rule response message comprising the subset of user rules from the authorizing entity computer.

14. A server computer comprising:

a processor; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising:

receiving, from a resource provider computer operated by a resource provider, an authorization request message comprising a flexible credential and an amount for a transaction conducted between a user and the resource provider, the flexible credential associated with multiple sources;

determining a subset of user rules of a set of user rules associated with the flexible credential to apply to the transaction;

determining a subset of resource provider rules of the resource provider based on the subset of user rules to apply to the transaction; and

applying the subset of user rules and the subset of resource provider rules to the transaction.

15. The server computer of claim 14, wherein the server computer is a network processing computer that stores an identification table and a user rules database, wherein applying the subset of user rules and the subset of resource provider rules to the transaction comprises:

modifying the authorization request message to include an indication of a source of the multiple sources based on the subset of user rules;

determining an alternate network processing computer based on the subset of resource provider rules; and

providing the authorization request message to the alternate network processing computer.

16. The server computer of claim 14, wherein the server computer is a transport computer that stores an identification table and a user rules database, wherein applying the subset of user rules and the subset of resource provider rules to the transaction comprises:

modifying the authorization request message to include an indication of a source of the multiple sources based on the subset of user rules;

determining a network processing computer based on the subset of resource provider rules; and

providing the authorization request message to the network processing computer.

17. The server computer of claim 14, wherein a user rule of the subset of user rules indicates a source of the multiple sources.

18. The server computer of claim 14, wherein the flexible credential is a token, the server computer is a network processing computer, and wherein the method further comprises:

providing the token to a token service provider computer, wherein the token service provider computer determines an account number associated with the token; and

receiving the account number from the token service provider computer.

19. A method comprising:

receiving, by a resource provider computer from a user device, a flexible credential for a transaction conducted between a user and a resource provider, wherein the resource provider computer is operated by the resource provider, and wherein the flexible credential is associated with multiple sources;

identifying, by the resource provider computer, the flexible credential as being associated with multiple sources using an identification table;

determining, by the resource provider computer, one or more resource provider rules for the transaction;

generating, by the resource provider computer, an authorization request message for the transaction, wherein the authorization request message comprises the flexible credential and an amount; and

providing, by the resource provider computer, the authorization request message and the one or more resource provider rules to a transport computer to request authorization of the transaction.

20. The method of claim 19 further comprising:

receiving, by the resource provider computer, a selected user rule from the user device; and

providing, by the resource provider computer, the selected user rule to the transport computer.