MERCHANT RISK MANAGEMENT METHOD, DEVICE, AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to a merchant risk management method, a device, and a storage medium.

BACKGROUND

[0002] With the rapid development of Internet technologies and the diversification of transactions, more types of merchants are providing transaction services for users, allowing the users to enjoy more convenient and abundant services. When conducting transactions with merchants, users can make payments for the transactions through wallet systems. Because some merchants may pose risks, the wallet systems need to manage the risks of the merchants to prevent these merchants from causing adverse impact to the wallet systems or ordinary users.

[0003] Content in the BACKGROUND section is merely information known to the inventor, and neither means that the information has been made available to the public prior to the application date of the present disclosure, nor means that the information can constitute prior art for the present disclosure.

SUMMARY

[0004] This specification provides a merchant risk management method, a device, and a storage medium. A wallet system can obtain more abundant and comprehensive merchant information, thereby avoiding a problem of high difficulty in merchant risk management due to insufficient merchant information, and improving accuracy of identifying a risky merchant.

[0005] According to a first aspect, this specification provides a merchant risk management method. The method includes: obtaining, in response to a risk identification request for a target merchant, basic merchant information that is returned by the target merchant through a target transaction, where the target transaction is a transaction associated with the target merchant;

querying at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant; and further determining a risk level of the target merchant based on the basic merchant information and the supplementary merchant information.

[0006] According to a second aspect, this specification further provides an electronic device. The electronic device includes: at least one storage medium, storing at least one instruction set for merchant risk management; and at least one processor, communicatively connected to the at least one storage medium, where the at least one processor reads the at least one instruction set when running, and performs the following operations based on an instruction of the at least one instruction set: obtaining, in response to a risk identification request for a target merchant, basic merchant information that is returned by the target merchant through a target transaction, where the target transaction is a transaction associated with the target merchant; querying at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant; and further determining a risk level of the target merchant based on the basic merchant information and the supplementary merchant information.

[0007] According to a third aspect, this specification provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set, and the at least one instruction set is executed by at least one processor to implement the merchant risk management method according to the first aspect.

[0008] Other functions of the merchant risk management method, the device, and the storage medium provided in this specification are partially listed in the following descriptions. Creative aspects of the merchant risk management method, the device, and the storage medium provided in this specification can be fully explained by practice or by using the methods, apparatuses, and combinations described in the following detailed examples.

BRIEF DESCRIPTION OF DRAWINGS

[0009] To describe the technical solutions in the embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following description show merely some

embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0010] FIG. 1 is a schematic diagram of a payment link according to an embodiment of this specification;

[0011] FIG. 2 is a schematic diagram of another payment link according to an embodiment of this specification;

[0012] FIG. 3 is a schematic diagram of a wallet system according to an embodiment of this specification;

[0013] FIG. 4 is a diagram of a hardware structure of an electronic device according to an embodiment of this specification;

[0014] FIG. 5 is a flowchart of a merchant risk management method according to an embodiment of this specification;

[0015] FIG. 6 is a schematic diagram of determining a risk level according to an embodiment of this specification; and

[0016] FIG. 7 is another schematic diagram of determining a risk level according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0017] Specific application scenarios and requirements of this specification are provided in the following descriptions, so that a person skilled in the art can manufacture and use content of this specification. For the person skilled in the art, various local modifications to the disclosed embodiments are apparent, and the general principles defined herein can be applied to other embodiments and applications without departing from the spirit and scope of this specification. Therefore, this specification is not limited to the shown embodiments, but has a widest scope consistent with the claims.

[0018] The terms used herein are merely intended to describe specific example embodiments, and impose no limitation. For example, unless otherwise explicitly stated in the context, the singular forms "one", "an", and "the" used herein may include plural forms. When used in this specification, the terms "include", "comprise", and/or "have" indicate/indicates existence of an associated integer, step, operation, element, and/or component, but does not exclude existence of

one or more other features, integers, steps, operations, elements, components, and/or groups, or another feature, integer, step, operation, element, component, and/or group can be added to the system/method.

[0019] In consideration of the following descriptions, these and other features of this specification, operations and functions of related components of the structure, and economy of combination and manufacturing of components can be significantly improved. With reference to the accompanying drawings, all of these form a part of this specification. However, it should be clearly understood that the accompanying drawings are merely used for the purpose of illustration and description, and are not intended to limit the scope of this specification. It should be further understood that the accompanying drawings are not drawn to scale.

[0020] The flowcharts used in this specification show operations implemented by the system according to some embodiments of this specification. It should be clearly understood that the operations in the flowcharts may not be implemented in sequence. On the contrary, the operations may be implemented in a reverse sequence or simultaneously. In addition, one or more other operations may be added to the flowcharts. One or more operations may be removed from the flowcharts.

[0021] With the diversification of transactions, payment scenarios for the transactions are gradually diversified. For example, the payment scenarios include, but are not limited to, cross-border payments and non-cross-border payments. Cross-border payments are, for example, payments for transactions between users and merchants that belong to different regions (countries or areas). Non-cross-border payments are, for example, payments for transactions between users and merchants that belong to the same region.

[0022] It can be understood that, payment links for transactions in different payment scenarios may be different. The following describes the payment links in different payment scenarios with reference to FIG. 1 and FIG. 2.

[0023] FIG. 1 is a schematic diagram of a payment link according to an embodiment of this specification.

[0024] As shown in FIG. 1, a user 100 executes a target transaction at a merchant 200. The merchant 200 may be a merchant having an independent transaction platform, may be a merchant residing on a transaction platform, or may be a physical merchant. This is not limited in this specification. After the user 100 initiates a payment operation for the target transaction, an

intermediary service system 300 may obtain transaction information of the target transaction, and forward the transaction information to a wallet system 400. The wallet system 400 may perform risk control on the merchant 200 based on merchant information in the transaction information, and may further perform risk control on payment for the target transaction.

[0025] The intermediary service system 300 is used to provide an intermediary service between the merchant 200 (or the transaction platform) and the wallet system 400. For example, the intermediary service system 300 is a financial institution or a payment service provider that is responsible for providing a payment processing service for the merchant (or the transaction platform). The intermediary service system 300 may serve as an intermediary between the merchant (or the transaction platform) and the wallet system, responsible for receiving a payment request (acquiring) initiated by the user at the merchant (or the transaction platform), and transferring transaction information corresponding to the payment request to the wallet system 400 for processing. The intermediary service system 300 is, for example, an acquiring system.

[0026] The following describes manners of obtaining the transaction information by the intermediary service system 300 in different cases.

[0027] For example, the merchant 200 is a merchant having an independent transaction platform. The user 100 may initiate a payment operation for the target transaction on the transaction platform of the merchant 200, and the merchant 200 generates the transaction information. Therefore, the merchant 200 may send the transaction information to the intermediary service system 300.

[0028] For example, the merchant 200 is a merchant residing on a transaction platform, and the user 100 may initiate the target transaction with the merchant 200 on the transaction platform, and initiate a payment operation for the target transaction on the transaction platform. The transaction platform generates the transaction information of the target transaction and sends the transaction information to the intermediary service system 300.

[0029] For example, the merchant 200 is a physical merchant. The user 100 may initiate a payment operation through a payment device or payment code provided by the intermediary service system 300 for the merchant 200, and the intermediary service system 300 generates the transaction information. The merchant information in the transaction information may be actively reported by the merchant 200 to the intermediary service system 300 before the target transaction, or may be reported by the merchant 200 at the request of the intermediary service system 300

during the target transaction. This is not limited in this specification. When providing a payment processing service for the merchant, the intermediary service system 300 may request the merchant to report the merchant information. Alternatively, when requesting the intermediary service system 300 to provide a payment processing service for the merchant, the merchant may actively report the merchant information.

[0030] The payment link in the example in FIG. 1 may be applied to the non-cross-border payment scenario. To be specific, the user 100, the merchant 200, the intermediary service system 300, and the wallet system 400 belong to the same region (area or country).

[0031] FIG. 2 is a schematic diagram of another payment link according to an embodiment of this specification.

[0032] As shown in FIG. 2, a user 100 executes a target transaction at a merchant 200. After the user 100 initiates a payment operation for the target transaction, an intermediary service system 300 may obtain transaction information of the target transaction. The transaction information is sent to the wallet system 400 through nodes such as a payment network 500 and a payment system 600. The wallet system 400 may perform risk control on the merchant 200 based on merchant information in the transaction information, and may further perform risk control on payment for the target transaction. For a manner of obtaining the transaction information by the intermediary service system 300, reference is made to the foregoing description, and details are not described again.

[0033] The payment network 500 is a network for payment whose construction and operation are led or participated in by the country or area. The payment network 500 is managed by the country or area, and provides various payment solutions for users, merchants, and other payment service systems (such as the intermediary service system 300 or the payment system 600), to ensure secure, efficient, and reliable operation of the payment system in the country or area, and to facilitate and digitize payment within the country or area.

[0034] The payment network 500 may integrate a plurality of different intermediary service systems 300, and unify and standardize related processes of different intermediary service systems 300 for the payment processing services, and fields returned during transaction payment. Different intermediary service systems 300 may provide payment processing services for different merchants. Therefore, when different intermediary service systems 300 sign agreements with merchants, basic merchant information (such as a merchant name, a registered area or country, and

a legal representative) that the merchants need to return or report may be different. Due to the unification and standardization of the payment network, different intermediary service systems 300 may require merchants to return or report the same basic merchant information, thereby simplifying and standardizing the payment process.

[0035] The payment system 600 is a payment solution platform that may integrate a plurality of different wallet systems, helping merchants and users access payment methods corresponding to different wallet systems through one access point, and providing more convenient payment experience.

[0036] The payment link in the example in FIG. 2 may be applied to the cross-border payment scenario. For example, the user 100, the payment system 600, and the wallet system 400 belong to the same region (country or area), and the payment network 500, the intermediary service system 300, and the merchant 200 belong to another region. For example, after a user 100 from region A travels to region B and conducts a target transaction with a merchant in region B, a payment link for the target transaction is shown in FIG. 2.

[0037] In the payment links shown in FIG. 1 and FIG. 2, a merchant system usually returns little basic merchant information during a transaction. Main reasons are as follows: On the one hand, the merchant system is not keen on returning the merchant information, that is, the merchant system is unwilling to return comprehensive merchant information. On the other hand, due to the compliance requirements for data transfer between different regions, some merchant information is not allowed to be transferred across different regions.

[0038] For example, in the cross-border payment link shown in FIG. 2, risk control requirements of different regions are different. Therefore, basic merchant information that is returned or needs to be reported during a transaction is also different. However, after the unification and standardization of the payment network 500 (an intersection of the basic merchant information required by different regions is usually used), the merchant returns or reports less basic merchant information. As a result, the basic merchant information sent by the intermediary service system 300 to a downstream node is further reduced (some basic merchant information is not allowed to be returned due to cross-border issues). Consequently, the merchant information obtained by the wallet system 400 is quite limited, increasing difficulty in risk control.

[0039] In view of the foregoing description, embodiments of this specification provide a merchant risk management method, a device, and a storage medium, so as to enable a wallet system

to obtain more abundant and comprehensive merchant information in different payment scenarios, thereby better managing a merchant risk.

[0040] It can be understood that the payment link in the foregoing example is merely an example, and a payment link applicable to the merchant risk management method, the device, and the storage medium that are provided in embodiments of this specification is not limited thereto.

[0041] The merchant risk management method provided in the embodiments of this specification may be performed by a wallet system. The following describes a system architecture of the wallet system with reference to FIG. 3. FIG. 3 is a schematic diagram of a wallet system according to an embodiment of this specification.

[0042] As shown in FIG. 3, the wallet system 400 may include a wallet client and a wallet server 420. In some embodiments, the wallet system 400 may further include a risk control device 430.

[0043] The wallet client is deployed on a terminal device 410. In some embodiments, one or more applications (apps) may be installed in the terminal device 410. The apps include but are not limited to a web browser app program, a search app program, a chat app program, a shopping app program, a video app program, a financing app program, an instant messaging tool, a mailbox client, social platform software, etc. For example, a wallet system app (namely, a wallet client) is installed on the terminal device 410.

[0044] The terminal device 410 may include a mobile device, a tablet computer, a notebook computer, a built-in device in a motor vehicle or similar content, or any combination thereof. In some embodiments, the mobile device may include a smart home device, a smart mobile device, a virtual reality device, an augmented reality device or a similar device, or any combination thereof. In some embodiments, the smart home apparatus may include a smart television, a desktop computer, or any combination. In some embodiments, the smart mobile device may include a smartphone, a personal digital assistant, a game device, a navigation device, or any combination thereof. In some embodiments, the virtual reality device or the augmented reality device may include a virtual reality helmet, virtual reality glasses, a virtual reality patch, an augmented reality helmet, augmented reality glasses, an augmented reality patch or similar content, or any combination thereof. For example, the virtual reality device or the augmented reality device may include AR glasses, a head mounted display, or VR. In some embodiments, the built-in apparatus in the motor vehicle may include a vehicle-mounted computer, a vehicle-mounted television, or

the like.

[0045] In some embodiments, the terminal device 410 may perform the merchant risk management method described in this specification. The terminal device 410 may store data and instructions used to implement the merchant risk management method, and may execute or be configured to execute the data and instructions. In some embodiments, the terminal device 410 may include a hardware device with a data information processing function and a necessary program needed for driving the hardware device to work.

[0046] For example, in response to a risk identification request for a target merchant, the terminal device 410 obtains basic merchant information that is returned by the target merchant through a target transaction (a transaction associated with the target merchant); queries at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant; and further determines a risk level of the target merchant based on the basic merchant information and the supplementary merchant information. Specific implementation of each step is described in detail in the following method P100, and details are not described.

[0047] As shown in FIG. 3, the terminal device 410 may be communicatively connected to the wallet server 420. The wallet server 420 may be a server that provides a payment service. Specifically, the wallet server 420 is a backend server that provides a service for the wallet client deployed on the terminal device 410.

[0048] In some embodiments, the wallet server 420 may perform the merchant risk management method described in this specification. The wallet server 420 may store data and instructions used to implement the merchant risk management method, and may execute or be configured to execute the data and instructions. In some embodiments, the wallet server 420 may include a hardware device with a data information processing function and a necessary program needed for driving the hardware device to work.

[0049] For example, in response to a risk identification request for a target merchant, the wallet server 420 obtains basic merchant information that is returned by the target merchant through a target transaction (a transaction associated with the target merchant); queries at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant; and further determines a risk level of the target merchant based on the basic merchant information and the supplementary merchant

information.

[0050] The risk control device 430 is a computing device with a specific computing capability, and may provide risk control calculation for the wallet system 400. In some embodiments, the risk control device 430 may perform the merchant risk management method described in this specification. The risk control device 430 may store data and instructions used to implement the merchant risk management method, and may execute or be configured to execute the data and instructions. In some embodiments, the risk control device 430 may include a hardware device with a data information processing function and a necessary program needed for driving the hardware device to work.

[0051] For example, in response to a risk identification request for a target merchant, the risk control device 430 obtains, from the wallet server 420 or the terminal device 410, basic merchant information that is returned by the target merchant through a target transaction; queries at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant; and further can determine a risk level of the target merchant based on the basic merchant information and the supplementary merchant information. After determining the risk level of the target merchant, the risk control device 430 may send the risk level to the wallet server 420 and/or the terminal device 410. The terminal device 410 or the wallet server 420 manages, based on the risk level, a transaction that the target merchant subsequently participates in.

[0052] It should be understood that quantities of terminal devices 410, wallet servers 420, and risk control devices 430 in FIG. 3 are merely examples. Based on an implementation requirement, there may be any quantities of terminal devices 410, wallet servers 420, and risk control devices 430.

[0053] It should be noted that the merchant risk management method may be completely performed on the terminal device 410, may be completely performed on the wallet server 420, may be completely performed on the risk control device 430, may be partially performed on the terminal device 410 and partially performed on the wallet server 420, may be partially performed on the terminal device 410 and partially performed on the risk control device 430, may be partially performed on the wallet server 420 and partially performed on the risk control device 430, or may be performed in another manner. This is not limited in this embodiment of this specification.

[0054] FIG. 4 is a diagram of a hardware structure of an electronic device 700 according to an

embodiment of this specification. The electronic device 700 may serve as the terminal device 410 or the wallet server 420 in FIG. 3, or may serve as the risk control device 430 in FIG. 3.

[0055] As shown in FIG. 4, the electronic device 700 may include at least one storage medium 730 and at least one processor 720. In some embodiments, the electronic device 700 may further include a communication port 750 and an internal communication bus 710. In addition, the electronic device 700 may further include an I/O component 760.

[0056] The internal communication bus 710 may be connected to different system components. For example, the internal communication bus 710 may be connected to the storage medium 730, the processor 720, the communication port 750, and the I/O component 760.

[0057] The I/O component 760 supports an input/output between the electronic device 700 and another component.

[0058] The communication port 750 is used for data communication between the electronic device 700 and the outside. For example, the communication port 750 may be used for data communication between the electronic device 700 and a network. The communication port 750 may be a wired communication port, or may be a wireless communication port.

[0059] In some embodiments, the network may be any type of wired or wireless network, or a combination thereof. For example, the network may include a cable network, a wired network, an optical fiber network, a telecommunications network, an intranet, the Internet, a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), a metropolitan area network (MAN), a public switched telephone network (PSTN), a Bluetooth network TM, a short-range wireless network (ZigBeeTM), a near field communication (NFC) network, or a similar network.

[0060] In some embodiments, the network may include one or more network access points. For example, the network may include a wired or wireless network access point, for example, a base station or an Internet switching point. Through the access point, one or more components of the terminal device 410, the wallet server 420, and the risk control device 430 may be connected to the network to exchange data or information.

[0061] The storage medium 730 may include a data storage apparatus. The data storage apparatus may be a non-transitory storage medium, or may be a transitory storage medium. For example, the data storage apparatus may include one or more of a disk 732, a read-only storage medium (ROM) 734, or a random access storage medium (RAM) 736. The storage medium 730

further includes at least one instruction set stored in the data storage apparatus. The instruction set may include computer program code, and the computer program code may include a program, a routine, an object, a component, a data structure, a process, a module, and the like for performing the merchant risk management method provided in this specification.

[0062] The processor 720 may be communicatively connected to the storage medium 730. The processor 720 is configured to execute the at least one instruction set. When the electronic device 700 runs, the processor 720 reads the at least one instruction set, and performs, based on an indication of the at least one instruction set, the merchant risk management method provided in this specification.

[0063] The processor 720 may be in a form of one or more processors. In some embodiments, the processor 720 may include one or more hardware processors, for example, a microcontroller, a microprocessor, a reduced instruction set computer (RISC), an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a central processing unit (CPU), a graphics processing unit (GPU), a physical processing unit (PPU), a microcontroller unit, a digital signal processor (DSP), a field programmable gate array (FPGA), an advanced RISC machine (ARM), a programmable logic device (PLD), any circuit or processor that can perform one or more functions, or any combination thereof.

[0064] To describe a problem, only one processor 720 is shown in the electronic device 700 in the accompanying drawings. However, it should be noted that the electronic device 700 in this specification may further include a plurality of processors. Therefore, the operations and/or method steps disclosed in this specification may be performed by one processor, or may be jointly performed by a plurality of processors. For example, if the processor 720 in the electronic device 700 performs step A and step B, it should be understood as that step A and step B may be jointly or separately performed by two different processors 720 (for example, a first processor performs step A, and a second processor performs step B, or a first processor and a second processor jointly perform steps A and B).

[0065] FIG. 5 is a flowchart of a merchant risk management method P100 according to an embodiment of this specification. As described above, the electronic device 700 in the wallet system may perform the merchant risk management method P100. Specifically, the processor 720 in the electronic device 700 may read the instruction set stored in the local storage medium of the electronic device 700, and then perform the merchant risk management method P100 based on a

stipulation of the instruction set.

[0066] As shown in FIG. 5, the merchant risk management method P100 may include the following steps.

[0067] S110: Obtain, in response to a risk identification request for a target merchant, basic merchant information that is returned by the target merchant through a target transaction, where the target transaction is a transaction associated with the target merchant.

[0068] The target transaction may be a transaction initiated by a target user, with the target merchant as the transaction counterparty. As described above, after the target user initiates the target transaction with the target merchant, the target merchant may return some information about the target merchant to the wallet system by using a payment link for the target transaction. In this specification, information about the target merchant that is returned by the target merchant through the target transaction is referred to as basic merchant information. In other words, the basic merchant information may be information about the target merchant that is carried in transaction information of the target transaction. The electronic device 700 may obtain the transaction information of the target transaction, and obtain the basic merchant information from the transaction information of the target transaction. For a manner of obtaining the transaction information by the electronic device 700, reference may be made to the foregoing description, and details are not described again.

[0069] The basic merchant information can be understood as a series of basic information of the merchant. The basic merchant information includes but is not limited to one or more of the following: a merchant name, merchant identification (ID), a merchant registration area or country, a merchant category code (MCC), and the like.

[0070] In some embodiments, in response to receiving a transaction request corresponding to the target transaction, the electronic device 700 obtains the basic merchant information that is returned by the target merchant through the target transaction. To be specific, the transaction request triggers risk identification for the target merchant.

[0071] The foregoing embodiment is applicable to a scenario in which risk management is performed on the merchant online. When detecting the transaction request, the electronic device 700 may analyze the target merchant in real time, so as to identify a potential risk of the target merchant, and therefore may respond to the target transaction (for example, intercept the current transaction) in a timely manner based on an identification result. The foregoing embodiment is

applicable to a risk control scenario that requires rapid identification and decision-making. Early warning and intervention may be performed before a risk occurs, and risk prevention and control measures may be taken in a timely manner, to prevent a risky merchant from causing losses or adverse impact to an ordinary user or the service platform.

[0072] The risky merchants in the embodiments of this specification include but are not limited to: a merchant that provides false merchant information, a merchant that does not actually exist, a merchant that provides an illegal service, and the like.

[0073] In some embodiments, in response to detecting a preset moment, the electronic device 700 obtains the basic merchant information that is returned by the target merchant through the target transaction. To be specific, the preset moment triggers risk identification for the target merchant.

[0074] In this embodiment, the target transaction is a transaction that has already been paid.

[0075] For example, the preset moment is 00:00 every day, or the preset moment is 00:00 every Sunday. This is not limited in this embodiment of this specification.

[0076] The foregoing embodiment is applicable to a scenario in which risk management is performed on the merchant offline. The electronic device 700 may perform in-depth analysis and mining based on a large quantity of historical transactions, to identify a potential risky merchant. This helps formulate a more proper and effective risk prevention and control policy for the risky merchant, and improve prevention and control efficiency and accuracy for the risky merchant.

[0077] S120: Query at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant.

[0078] The supplementary merchant information can be understood as a series of merchant information added on the basis of the basic merchant information. The supplementary merchant information includes but is not limited to: a merchant name, a merchant ID, a merchant registration area or country, an MCC, a merchant business scope, a merchant address, a merchant website, merchant business registration information, and the like.

[0079] In some embodiments, the basic merchant information includes at least one piece of identification information used to identify the target merchant. The electronic device 700 uses the at least one piece of identification information as a search keyword, and separately searches the at least one data source by using the search keyword, to obtain a search result corresponding to each

of the at least one data source; and further determines the supplementary merchant information based on the search result corresponding to each of the at least one data source.

[0080] For example, the at least one piece of identification information includes but is not limited to at least one of the following: a merchant name and merchant identification. Alternatively, the at least one piece of identification information may further include at least one of the following: a merchant registration area or country, and an MCC. More abundant content of the at least one piece of identification information leads to a more targeted search keyword, and easier obtaining of content related to the target merchant through searching from the data source.

[0081] For example, the at least one piece of identification information includes a name and a registration area of merchant ①. The electronic device 700 uses the name and registration area of merchant ① as a search keyword, and inputs the name and registration area of merchant ① into each of the at least one data source to obtain a search result output by each data source. The electronic device 700 may organize the search result output by each data source to obtain the supplementary merchant information of the target merchant.

[0082] For example, the merchant risk management method P100 provided in this specification is applied to a target service system, and the target service system may implement risk management on the target merchant by performing the merchant risk management method P100. The at least one data source includes at least one of an internal data source and an external data source. The internal data source is a data source inside the target service system, and the external data source is a data source outside the target service system.

[0083] For example, with reference to FIG. 4, the target service system may be a wallet system. In this case, the internal data source is a data source inside the wallet system, or the internal data source is a database of the wallet system. The external data source is a data source outside the wallet system.

[0084] In this example, in a process of obtaining the supplementary merchant information, the electronic device 700 may obtain more abundant and comprehensive merchant information through a plurality of channels of internal and external data sources. This provides sufficient basis for risk identification for the target merchant, and can improve accuracy of risk identification. This example mitigates, for example, a problem of high difficulty in risk identification due to insufficient merchant information that is returned through a transaction by using a payment link (for example, the payment link shown in FIG. 1 or FIG. 2).

[0085] The following provides description by using an example in which the target service system is a wallet system.

[0086] For example, the search result corresponding to the internal data source includes at least one of the following:

historical reporting information of the target merchant in the wallet system, historical transaction information associated with the target merchant, historical risk control information associated with the target merchant, and user feedback information associated with the target merchant.

[0087] The historical reporting information of the target merchant in the wallet system can be understood as merchant information that is actively reported by the target merchant to the wallet system or reported by the target merchant at the request of the wallet system when the target merchant resides on the wallet system or when the target merchant requests the wallet system to provide a payment service.

[0088] The historical transaction information associated with the target merchant can be understood as transaction information of a historical transaction in which the target merchant participates within the wallet system. The transaction information includes transaction information returned during execution of a historical transaction, or may include information about each user executing the historical transaction. The information about the user includes but is not limited to address information for initiating a historical transaction and operation information of the user (when the user is a legal representative).

[0089] The historical risk control information associated with the target merchant can be understood as information that is obtained by performing risk control on the target merchant by the wallet system during execution of the historical transaction. The historical risk control information includes but is not limited to a risk label of the target merchant, a risk level of the target merchant, and the like.

[0090] The user feedback information associated with the target merchant can be understood as related information that is filled in or fed back to the wallet system by the user during or after execution of the historical transaction. The related information includes but is not limited to image information of the target merchant, whether the target merchant is engaged in an illegal service, and the like.

[0091] In this example, the electronic device 700 may query the internal data source of the

wallet system based on the search keyword to check whether the target merchant already exists. For example, if the target merchant already exists, at least one of the foregoing information may be found. Alternatively, if the target merchant does not exist, the search result based on the internal data source is empty.

[0092] For example, the search result corresponding to the external data source includes at least one of the following:

information about the target merchant that is found through searching from a website exposed to the Internet; information about the target merchant that is found through searching from an official website on the Internet; and information about the target merchant that is obtained from a partner of the wallet system.

[0093] The website exposed to the Internet may be a plurality of types of websites. The plurality of types include but are not limited to a tourism type, a retrieval type, a navigation type, and the like. For example, the electronic device 700 may input the search keyword into each website exposed to the Internet, or the electronic device 700 obtains, through a crawler, a search result for the target merchant from each website exposed to the Internet.

[0094] The official website on the Internet can be understood as an authoritative website with an official background or official authorization. Generally, merchant information obtained from an official website is relatively accurate, and may be used to verify authenticity of the target merchant. The official website includes but is not limited to a business registration website, and the like. For example, the electronic device 700 may input the search keyword into each official website on the Internet, or the electronic device 700 obtains, through a crawler, a search result for the target merchant from each official website on the Internet.

[0095] The partner of the wallet system can be understood as a data provider that provides data. The data provider may collect merchant information of different merchants through a plurality of channels. For example, the electronic device 700 may provide the search keyword to each data provider, and obtain a search result for the target merchant from each data provider.

[0096] In this example, the electronic device 700 considers different types of external data sources based on a search result obtained from an external data source, thereby further improving richness and comprehensiveness of the supplementary merchant information.

[0097] S130: Determine a risk level of the target merchant based on the basic merchant information and the supplementary merchant information.

[0098] The electronic device 700 may learn more comprehensive merchant information related to the target merchant based on the basic merchant information and the supplementary merchant information, and further determine the risk level of the target merchant based on the more comprehensive merchant information. This can improve accuracy of the risk level of the target merchant.

[0099] In some embodiments, the electronic device 700 obtains M field dimensions used for merchant risk identification, where M is an integer greater than or equal to 1; separately determines a field value corresponding to each of the M field dimensions from the basic merchant information and the supplementary merchant information; and further determines the risk level of the target merchant based on the field value corresponding to each of the M field dimensions.

[0100] The M field dimensions may be preset and stored in the electronic device 700. The M field dimensions include but are not limited to a merchant name, a merchant ID, an MCC, a merchant registration region (country or area), a merchant address, a merchant business scope, a merchant website, merchant business registration information, and the like.

[0101] The field values corresponding to the M field dimensions determined by the electronic device 700 may be presented in a plurality of forms. One of the forms is used below as an example. This embodiment of this specification is not limited thereto.

[0102] For example, the electronic device 700 obtains the field values corresponding to the M field dimensions shown in Table 1.

Table 1

	Basic merchant information	Supplementary merchant information
Merchant name	Name 1	Name 1
Merchant registration region	Region 1	Empty
…	…	…
Merchant business scope	Scope 1	Scope 2

[0103] As shown in Table 1, the electronic device 700 determines a field value of each field dimension based on the basic merchant information and the supplementary merchant information. If the field values of the same field dimension obtained by the electronic device 700 based on the

basic merchant information and the supplementary merchant information are different, the different field values are filled in corresponding locations. Specifically, the electronic device 700 fills the field value obtained based on the basic merchant information into the column of basic merchant information, and fills the field value obtained based on the supplementary merchant information into the column of supplementary merchant information.

[0104] If the field values of a specific field dimension (for example, the merchant name) obtained by the electronic device 700 based on the basic merchant information and the supplementary merchant information are the same, there may be one field value corresponding to the field dimension. Alternatively, as shown in Table 1, the electronic device 700 fills the same field value into different locations.

[0105] If the electronic device 700 does not find a related result for a specific field dimension (for example, the merchant registration region) based on the basic merchant information or the supplementary merchant information, the field value of the field dimension is filled as "empty" at the corresponding location. It can be understood that, in Table 1, one specific field value from the basic merchant information or the supplementary merchant information is used as an example, but this embodiment of this specification is not limited thereto. For example, there may be a plurality of field values of a specific field dimension that are obtained by the electronic device 700 based on the supplementary merchant information.

[0106] There are a plurality of manners in which the electronic device 700 determines the risk level of the target merchant based on the field value corresponding to each of the M field dimensions. Three of the manners are used below as examples, but this embodiment of this specification is not limited thereto.

[0107] Manner 1

[0108] For example, the electronic device 700 inputs the field value corresponding to each of the M field dimensions into a preset risk identification model, to obtain the risk level of the target merchant.

[0109] The risk identification model may be a pre-trained risk identification model. In a process of performing risk identification on the target merchant, the electronic device 700 may invoke the risk identification model.

[0110] For example, the electronic device 700 inputs the field value corresponding to each of the M field dimensions shown in Table 1 into the risk identification model, to obtain an

identification result output by the risk identification model. The identification result may represent a possibility that the target merchant is a risky merchant, and the electronic device 700 may determine the risk level of the target merchant based on the identification result. Alternatively, the identification result may directly represent the risk level of the target merchant.

[0111] In this embodiment, the electronic device 700 inputs the obtained field value corresponding to each of the M field dimensions into the risk identification model to obtain the risk level of the target merchant. The implementation is simple with high efficiency, and is applicable to a scenario in which risk identification is performed on the target merchant online.

[0112] The risk identification model may alternatively be understood as a qualification hierarchical model. The risk level (negative description of the merchant) output by the risk identification model may be inversely correlated with the merchant qualification (positive description of the merchant). For example, a lower risk level indicates higher merchant qualification, or a higher risk level indicates lower merchant qualification.

[0113] Manner 2

[0114] For example, some field dimensions in the M field dimensions correspond to a plurality of field values. For each of the some field dimensions, the electronic device 700 determines a matching result of a plurality of field values of the field dimension; and further determines the risk level of the target merchant based on the matching result corresponding to each of the some field dimensions.

[0115] For example, as shown in FIG. 6, a quantity of field values corresponding to each of the some field dimensions is two, but this embodiment of this specification is not limited thereto. For example, the quantity of field values corresponding to each field dimension may be another quantity, or the quantity of field values corresponding to each field dimension may vary. Referring to FIG. 6, the electronic device 700 obtains two field values corresponding to each field dimension, where the two field values may come from search results of different data sources. For example, of two field values corresponding to a field dimension 1, a field value 1a comes from the basic merchant information, and a field value 1b comes from the supplementary merchant information. Alternatively, the field value 1a comes from a search result obtained based on the internal data source, and the field value 1b comes from a search result obtained based on the external data source. Alternatively, both the field value 1a and the field value 1b come from search results obtained based on different external data sources. This is not limited in this embodiment of this specification.

[0116] The electronic device 700 may determine a matching result corresponding to two field values of the same field dimension through vector comparison. For example, the electronic device 700 obtains vector representations of the two field values, determines a distance between the two vector representations, and determines the matching result based on the distance. Each field dimension may have a corresponding weight. After obtaining the matching result corresponding to each field dimension, the electronic device 700 may determine the risk level of the target merchant based on the matching result and the weight that correspond to each field dimension. Alternatively, the electronic device 700 may further determine the risk level of the target merchant in another manner. This is not limited in this embodiment of this specification.

[0117] Manner 3

[0118] For example, each field dimension corresponds to a preset risk control condition. For each field dimension, the electronic device 700 determines a risk identification result corresponding to the field dimension based on the field value corresponding to the field dimension and the preset risk control condition corresponding to the field dimension; and further determines the risk level of the target merchant based on the risk identification result corresponding to each of the M field dimensions.

[0119] The preset risk control condition may be determined based on risk control experience.

[0120] For example, as shown in FIG. 7, a field dimension 1 is used as an example. The electronic device 700 determines a risk identification result 1 based on a field value 1 corresponding to the field dimension 1 and a preset risk control condition 1. The field value 1 may be one or more field values (another field value in FIG. 7 is understood in the same manner).

[0121] If the field dimension 1 is a merchant address, the field value 1 is empty. The risk control condition 1 is "Does the merchant address exist?". In this case, the electronic device 700 may determine, based on the field value 1 and the risk control condition 1, that the risk identification result 1 indicates a risk.

[0122] If the field dimension 1 is a merchant registration region, the field value 1 includes region 1 and region 2. Region 1 and region 2 differ greatly, and region 1 is obtained based on the basic merchant information, and region 2 is obtained based on a search result from an official website. The risk control condition 1 is "Is the merchant registration region accurate?". In this case, the electronic device 700 may determine, based on the field value 1 and the risk control condition 1, that the risk identification result 1 indicates a risk.

[0123] If the field dimension 1 is a business scope, the field value 1 includes a business scope 1 and a transaction item corresponding to a target transaction, and the transaction item does not fall within the business scope 1. The risk control condition 1 is "Does the transaction item corresponding to the target transaction fall within the business scope?". In this case, the electronic device 700 may determine, based on the field value 1 and the risk control condition 1, that the risk identification result 1 indicates a risk.

[0124] Other preset risk control conditions are not listed one by one, and the electronic device 700 may obtain the risk identification result corresponding to each field dimension in a similar manner. Further, the electronic device 700 may determine the risk level of the target merchant based on the risk identification result corresponding to each field dimension. For example, the electronic device 700 may determine the risk level of the target merchant based on a quantity of "risks" in the risk identification result. Alternatively, the electronic device 700 may determine the risk level of the target merchant based on the risk identification result and a weight that correspond to each field dimension.

[0125] In manner 2 and manner 3, the electronic device 700 may perform adequate risk identification on the target merchant by using one or more field values corresponding to each field dimension. Because field dimensions and field values are relatively comprehensive, the obtained risk level of the target merchant is highly accurate.

[0126] It should be noted that the electronic device 700 may alternatively obtain the risk level of the target merchant with reference to one or more of the foregoing three manners.

[0127] In some embodiments, after determining the risk level of the target merchant in the foregoing manner, the electronic device 700 may further determine a transaction limit of the target merchant based on the risk level. The transaction limit is used to manage a transaction in which the target merchant participates. To be specific, the electronic device 700 may set different transaction limits for merchants of different risk levels, to avoid a large transaction limit of a merchant of a high risk level, thereby causing large risk exposure of the merchant and causing adverse impact to more ordinary users.

[0128] The transaction limit of the target merchant may be a daily transaction limit, a monthly transaction limit, or an annual transaction limit, but this embodiment of this specification is not limited thereto. The daily transaction limit represents an upper limit of an accumulated amount of daily transaction of the target merchant. The monthly transaction limit represents an upper limit of

an accumulated amount of monthly transaction of the target merchant. The annual transaction limit is deduced by analogy.

[0129] For example, the transaction limit is the daily transaction limit. The electronic device 700 may intercept payment for the target transaction when the sum of the transaction amount of the target transaction and the accumulated transaction amount of other historical transactions conducted by the target merchant on the current day exceeds the daily transaction limit.

[0130] For example, the risk level represents severity of the risk. The transaction limit is inversely correlated with the risk severity represented by the risk level.

[0131] For example, if the risk level is a first risk level, the electronic device 700 determines that the transaction limit is a first limit. Alternatively, if the risk level is a second risk level, the electronic device 700 determines that the transaction limit is a second limit. The risk severity represented by the first risk level is higher than the second risk level, and the second limit is higher than the first limit.

[0132] The foregoing division of the risk level and the transaction limit is merely an example, and this embodiment of this specification is not limited thereto. For example, the electronic device 700 may alternatively divide the risk level into another quantity of risk levels that represent different risk severity. The electronic device 700 may alternatively divide the transaction limit into more limit levels such as an infinite limit, a medium limit, and a small limit. Each limit level may correspond to one upper limit of the accumulated transaction amount.

[0133] In a word, a higher risk level indicates higher risk severity, lower qualification of the merchant, and a lower transaction limit that is set for the merchant. Conversely, a lower risk level indicates lower risk severity, higher qualification of the merchant, and a higher transaction limit that is set for the merchant. For some merchants with high qualification (which indicates an extremely low risk level), the electronic device 700 may not set a transaction limit for these merchants, that is, the transaction limit of these merchants may be an infinite limit.

[0134] In some embodiments, in a scenario in which risk management is performed on a merchant online, the electronic device 700 may manage the target transaction based on the transaction limit corresponding to the target merchant. In this embodiment, the electronic device 700 may perform risk control on the target transaction in a timely manner, and provide a risk control decision, thereby reducing a loss of the user.

[0135] For example, the electronic device 700 determines, based on the transaction limit

corresponding to the target merchant, to intercept the target transaction. Alternatively, the electronic device 700 determines, based on the transaction limit corresponding to the target merchant, to release the target transaction.

[0136] The daily transaction limit is used as an example. The electronic device 700 may intercept payment for the target transaction when the sum of the transaction amount of the target transaction and the accumulated transaction amount of other historical transactions conducted by the target merchant on the current day exceeds the daily transaction limit. The electronic device 700 may release payment for the target transaction when the sum of the transaction amount of the target transaction and the accumulated transaction amount of other historical transactions conducted by the target merchant on the current day is less than or equal to the daily transaction limit.

[0137] It should be noted that, as the target merchant participates in more transactions, the risk level or the transaction limit corresponding to the target merchant may change. For example, as the target merchant participates in more transactions, the risk level corresponding to the target merchant decreases. In this case, the transaction limit corresponding to the target merchant may be increased. Alternatively, as the target merchant participates in more transactions, the risk level corresponding to the target merchant increases. In this case, the transaction limit corresponding to the target merchant may be reduced.

[0138] In some embodiments, in a scenario in which risk management is performed on the merchant offline, the electronic device 700 adds a merchant whose risk level is higher than a preset level to a risky merchant list. Subsequently, the electronic device 700 may intercept payment for a transaction in which a merchant in the risky merchant list participates. The electronic device 700 may further update the merchant information of the target merchant in the internal data source of the wallet system based on the supplementary merchant information, to provide a basis for subsequent risk control.

[0139] In conclusion, according to the merchant risk management method, the device, and the storage medium that are provided in this specification, the electronic device 700 may enrich the merchant information of the target merchant by using the supplementary merchant information. In particular, for the payment link shown in FIG. 2, the solution provided in this specification can resolve a problem of difficulty in merchant risk identification due to insufficient merchant information, thereby improving accuracy of a merchant risk identification result. This helps the

wallet system effectively perform risk management on the merchant, thereby preventing a risky merchant from causing adverse impact to ordinary users and the wallet system. In addition, according to the solution provided in this specification, the transaction limit may be further set based on the risk level, so that an accumulated transaction amount that can be conducted by the risky merchant is controllable, thereby avoiding a greater loss.

[0140] Another aspect of this specification provides a computer-readable non-transitory storage medium, storing at least one group of executable instructions used to perform merchant risk management. When the executable instructions are executed by a processor, the executable instructions instruct the processor to implement the steps of the method P100 described in this specification. In some possible implementations, aspects of this specification may alternatively be implemented in a form of a program product, including program code. When the program product runs on an electronic device 700, the program code is used to enable the electronic device 700 to perform the steps of the method P100 described in this specification. The program product configured to implement the foregoing method may be a portable compact disc read-only memory (CD-ROM) that includes program code, and may run on the electronic device 700. However, the program product in this specification is not limited thereto. In this specification, a readable storage medium may be any tangible medium that includes or stores a program, and the program may be used by or in combination with an instruction execution system. The program product may be any combination of one or more readable media. The readable medium may be a readable signal medium or a readable storage medium. For example, the readable storage medium may be but is not limited to an electrical, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus or device, or any combination thereof. More specific examples of the readable storage medium include: an electrical connection including one or more conducting wires, a portable disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any proper combination thereof. The computer-readable storage medium may include a data signal propagated in a baseband or as a part of a carrier, and carries readable program code. Such a propagated data signal may take a plurality of forms, including but not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium may alternatively be any readable medium other than the readable storage medium, and

the readable medium may be used to send, propagate, or transmit a program used by or in combination with an instruction execution system, apparatus, or device. The program code included in the readable storage medium may be transmitted in any proper medium, including but not limited to a wireless medium, a wired medium, an optical cable, an RF medium, and the like, or any proper combination thereof. The program code for performing operations in this specification may be written in any combination of one or more program design languages. The program design language includes an object-oriented program design language, such as Java or C++, and further includes a conventional procedural program design language, such as a "C" language or a similar program design language. The program code may be completely executed on the electronic device 700, partially executed on the electronic device 700, executed as an independent software package, partially executed on the electronic device 700 and partially executed on a remote computing device, or completely executed on a remote computing device.

[0141] The term "and/or" in the embodiments of this specification describes an association relationship between associated objects, and indicates that three relationships may exist. For example, A and/or B may indicate the following three cases: Only A exists, both A and B exist, and only B exists. The character "/" generally indicates an "or" relationship between associated objects.

[0142] The terms "first", "second", and the like in this specification are used to distinguish between objects or entities that are similar to each other or of a same type, and do not necessarily imply a specific sequence or order.

[0143] "Plurality of" mentioned in this specification shall be understood as two or more unless otherwise specified.

[0144] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims may be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular order or consecutive order to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

[0145] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the foregoing detailed disclosure may be presented only in an example manner, and may impose no limitation. Although it is not explicitly stated herein, a person skilled in the art

can understand that the requirements of this specification include various proper changes, improvements, and modifications to the embodiments. These changes, improvements, and modifications are intended to be proposed in this specification, and fall within the spirit and scope of the example embodiments of this specification.

[0146] In addition, some terms in this specification are used to describe the embodiments of this specification. For example, "an embodiment", "embodiments", and/or "some embodiments" mean that a particular feature, structure, or characteristic described with reference to the embodiments may be included in at least one embodiment of this specification. Therefore, it can be emphasized and understood that two or more of "an embodiment", "one embodiment", or "alternative embodiments" referred to in parts of this specification do not necessarily indicate the same embodiment. In addition, particular features, structures, or characteristics may be properly combined in one or more embodiments of this specification.

[0147] It should be understood that in the foregoing descriptions of the embodiments of this specification, to help understand a feature, for the purpose of simplifying this specification, various features are combined in a single embodiment, accompanying drawing, or description thereof in this specification. However, this does not mean that the combination of these features is necessary. It is entirely possible for a person skilled in the art to mark some devices and understand the devices as separate embodiments when reading this specification. In other words, the embodiments in this specification can alternatively be understood as an integration of a plurality of secondary embodiments. Content of each secondary embodiment is also true when features are less than all features in one of the foregoing disclosed embodiments.

[0148] Each patent, patent application, publication of a patent application, and other materials, for example, articles, books, instructions, publications, documents, and products, that are cited in this specification and that are other than any document that is inconsistent or conflict with this document or that imposes limiting impact on the widest scope of the claims can be incorporated here by reference and used for all purposes now or later associated with this document. In addition, the term in this document shall prevail when there is any inconsistency or conflict between the description, definition and/or use of a related term in any material and the description, definition and/or use of a related term in this document.

[0149] Finally, it should be understood that the principles of the implementation solutions of this specification are described in the implementation solutions of the application disclosed in this

specification. Other modified embodiments also fall within the scope of this specification. Therefore, the embodiments disclosed in this specification are merely examples and not limitations. A person skilled in the art can use an alternative configuration according to the embodiments of this specification to implement the application in this specification. Therefore, the embodiments of this specification are not limited to the embodiments accurately described in the application.

CLAIMS

What is claimed is:

1. A merchant risk management method, comprising:

obtaining, in response to a risk identification request for a target merchant, basic merchant information that is returned by the target merchant through a target transaction, wherein the target transaction is a transaction associated with the target merchant;

querying at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant; and

determining a risk level of the target merchant based on the basic merchant information and the supplementary merchant information.

2. The method according to claim 1, wherein the basic merchant information comprises at least one piece of identification information used to identify the target merchant, and the querying at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant comprises:

using the at least one piece of identification information as a search keyword, and separately searching the at least one data source by using the search keyword, to obtain a search result corresponding to each of the at least one data source; and

determining the supplementary merchant information based on the search result corresponding to each of the at least one data source.

3. The method according to claim 2, wherein the method is applied to a target service system, and the at least one data source comprises at least one of an internal data source and an external data source, wherein

the internal data source is a data source inside the target service system, and the external data source is a data source outside the target service system.

4. The method according to claim 3, wherein the search result corresponding to the internal data source comprises at least one of the following:

historical reporting information of the target merchant in the target service system;

historical transaction information associated with the target merchant;

historical risk control information associated with the target merchant; and

user feedback information associated with the target merchant.

5. The method according to claim 3, wherein the search result corresponding to the external data source comprises at least one of the following:

information about the target merchant that is found through searching from a website exposed to the Internet;

information about the target merchant that is found through searching from an official website on the Internet; and

information about the target merchant that is obtained from a partner of the target service system.

6. The method according to claim 1, wherein the determining a risk level of the target merchant based on the basic merchant information and the supplementary merchant information comprises:

obtaining M field dimensions used for merchant risk identification, wherein M is an integer greater than or equal to 1;

separately determining a field value corresponding to each of the M field dimensions from the basic merchant information and the supplementary merchant information; and

determining the risk level of the target merchant based on the field value corresponding to each of the M field dimensions.

7. The method according to claim 6, wherein the determining the risk level of the target merchant based on the field value corresponding to each of the M field dimensions comprises:

inputting the field value corresponding to each of the M field dimensions into a preset risk identification model, to obtain the risk level of the target merchant.

8. The method according to claim 6, wherein some field dimensions in the M field dimensions correspond to a plurality of field values, and the determining the risk level of the target merchant based on the field value corresponding to each of the M field dimensions comprises:

for each of the some field dimensions, determining a matching result of a plurality of field values of the field dimension; and

determining the risk level of the target merchant based on the matching result corresponding to each of the some field dimensions.

9. The method according to claim 6, wherein each field dimension corresponds to a preset risk control condition, and the determining the risk level of the target merchant based on the field value corresponding to each of the M field dimensions comprises:

for each field dimension, determining a risk identification result corresponding to the field dimension based on the field value corresponding to the field dimension and the preset risk control condition corresponding to the field dimension; and

determining the risk level of the target merchant based on the risk identification result corresponding to each of the M field dimensions.

10. The method according to claim 1, wherein the method further comprises:

determining a transaction limit of the target merchant based on the risk level, wherein the transaction limit is used to manage a transaction in which the target merchant participates.

11. The method according to claim 10, wherein the determining a transaction limit of the target merchant based on the risk level comprises any one of the following:

if the risk level is a first risk level, the transaction limit is a first limit; or

if the risk level is a second risk level, the transaction limit is a second limit, wherein the first risk level is higher than the second risk level, and the second limit is higher than the first limit.

12. The method according to claim 10, wherein the responding to a risk identification request for a target merchant comprises responding to receiving a transaction request corresponding to the target transaction; and

after the determining a transaction limit of the target merchant, the method further comprises: determining, based on the transaction limit, to intercept the target transaction or release the target transaction.

13. An electronic device, comprising:

at least one storage medium, storing at least one instruction set for merchant risk management; and

at least one processor, communicatively connected to the at least one storage medium, wherein the at least one processor reads the at least one instruction set when running, and performs the following operations based on an instruction of the at least one instruction set:

obtaining, in response to a risk identification request for a target merchant, basic merchant information that is returned by the target merchant through a target transaction, wherein the target transaction is a transaction associated with the target merchant;

querying at least one data source for information about the target merchant based on the basic merchant information to obtain supplementary merchant information of the target merchant; and

determining a risk level of the target merchant based on the basic merchant information and

the supplementary merchant information.

14. The electronic device according to claim 13, wherein the basic merchant information comprises at least one piece of identification information used to identify the target merchant, and in order to obtain the supplementary merchant information of the target merchant, the at least one processor performs the following operations:

using the at least one piece of identification information as a search keyword, and separately searching the at least one data source by using the search keyword, to obtain a search result corresponding to each of the at least one data source; and

determining the supplementary merchant information based on the search result corresponding to each of the at least one data source.

15. The electronic device according to claim 14, wherein the target merchant is a merchant providing a service in a target service system, and the at least one data source comprises at least one of an internal data source and an external data source, wherein

the internal data source is a data source inside the target service system, and the external data source is a data source outside the target service system.

16. The electronic device according to claim 15, wherein

the search result corresponding to the internal data source comprises at least one of the following:

historical reporting information of the target merchant in the target service system;

historical transaction information associated with the target merchant;

historical risk control information associated with the target merchant; and

user feedback information associated with the target merchant.

17. The electronic device according to claim 15, wherein the search result corresponding to the external data source comprises at least one of the following:

information about the target merchant that is found through searching from a website exposed to the Internet;

information about the target merchant that is found through searching from an official website on the Internet; and

information about the target merchant that is obtained from a partner of the target service system.

18. The electronic device according to claim 13, wherein in order to determine the risk level

of the target merchant, the at least one processor performs the following operations:

obtaining M field dimensions used for merchant risk identification, wherein M is an integer greater than or equal to 1;

separately determining a field value corresponding to each of the M field dimensions from the basic merchant information and the supplementary merchant information; and

determining the risk level of the target merchant based on the field value corresponding to each of the M field dimensions.

19. The electronic device according to claim 18, wherein in order to determine the risk level of the target merchant, the at least one processor performs the following operation:

inputting the field value corresponding to each of the M field dimensions into a preset risk identification model, to obtain the risk level of the target merchant.

20. A computer-readable non-transitory storage medium, wherein the computer-readable non-transitory storage medium stores at least one instruction set, and the at least one instruction set is executed by at least one processor to implement the method according to any one of claims 1 to 12.