

PAYMENT METHOD, INTERMEDIATE SERVICE SYSTEM, WALLET SYSTEM, MERCHANT SYSTEM, AND STORAGE MEDIUM

TECHNICAL FIELD

5 **[0001]** This specification relates to the field of internet technologies, and in particular, to a payment method, an intermediate service system, a wallet system, a merchant system, and a storage medium.

BACKGROUND

10 **[0002]** In the transaction and payment field, when a terminal device displays an interaction page of a merchant system, a user can initiate a payment operation for a transaction in the merchant system, to trigger a wallet system to pay for the transaction. The wallet system needs to perform risk prevention and control on the transaction, to ensure payment security of the user. For example, a payment procedure is as follows: After the user initiates a payment operation for the transaction on an interaction page of the merchant system, the terminal device jumps to an interaction page of
15 the wallet system. After the terminal device jumps to the interaction page of the wallet system, the wallet system can collect device information of the terminal device, and perform risk prevention and control on the transaction based on the device information. For example, the wallet system can compare the device information with device information associated with a current account of the wallet system, to identify whether the current account is a stolen account. When identifying
20 that the current account is not a stolen account, the wallet system continues to perform a subsequent payment procedure. When identifying that the current account is a stolen account, the wallet system can refuse to pay, to implement risk prevention and control.

25 **[0003]** In the above-mentioned payment procedure, the terminal device needs to jump from the merchant system to the wallet system. In a jump process, a payment process consumes a relatively long time due to the need to load resources and the like, and a payment procedure with a cross-system jump is relatively cumbersome. Each time an additional jump is made, a payment

success probability may be affected due to a network or another reason, resulting in relatively poor user experience. To resolve the above-mentioned problem, there are currently some payment solutions in which in an entire payment procedure, the terminal device does not jump from the merchant system to the wallet system. However, in these payment solutions, there is an increase in difficulty of performing risk control by the wallet system. Therefore, when the terminal device does not jump to the wallet system, how to enable the wallet system to perform effective risk control is an urgent problem that needs to be currently resolved.

[0004] Content in the background is merely information known to the inventor, and neither means that the information has entered the public domain before the application date of this disclosure, nor means that the information can become the existing technology of this disclosure.

SUMMARY

[0005] This specification provides a payment method, an intermediate service system, a wallet system, a merchant system, and a storage medium, to implement effective risk control without a cross-system jump, and improve user experience.

[0006] According to a first aspect, this specification provides a payment method, applied to an intermediate service system that provides an intermediate service between a merchant system and a wallet system, and including: when a terminal device displays an interaction page of the merchant system, receiving device information and a payment request from the merchant system, where the device information is collected by the merchant system from the terminal device, and the payment request represents that a target account requests to pay for a target transaction in the merchant system by using the wallet system; sending the payment request and the device information to the wallet system, where the device information is used by the wallet system for a risk control procedure of the payment request; receiving a payment result corresponding to the payment request from the wallet system; and sending the payment result to the merchant system, so that the merchant system displays the payment result on an interaction page of the merchant system, where in a process of performing the payment method by the intermediate service system, the terminal device does not jump to an interaction page of the wallet system.

[0007] According to a second aspect, this specification provides a payment method, applied to a wallet system, and including: when a terminal device displays an interaction page of a merchant

system and a target account initiates a payment operation for a target transaction on an interaction page of the merchant system, receiving device information and a payment request from an intermediate service system, where the device information is collected by the merchant system from the terminal device, and the intermediate service system provides an intermediate service between the merchant system and the wallet system; performing a risk control procedure on the payment request based on the device information, to obtain a risk control result; determining a payment result corresponding to the payment request based on the risk control result; and sending the payment result to the intermediate service system, so that the payment result is displayed on an interaction page of the merchant system, where in a process of performing the payment method by the wallet system, the terminal device does not jump to an interaction page of the wallet system.

[0008] According to a third aspect, this specification provides a payment method, applied to a merchant system, and including: when a terminal device displays an interaction page of the merchant system, collecting device information of the terminal device; in response to detecting that a target account initiates a payment operation for a target transaction on an interaction page of the merchant system, sending the device information and a payment request to an intermediate service system, where the device information is used by a wallet system for a risk control procedure of the payment request, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; and receiving a payment result corresponding to the payment request from the intermediate service system, and displaying the payment result on an interaction page of the merchant system, where in a process of performing the payment method by the merchant system, the terminal device does not jump to an interaction page of the wallet system.

[0009] According to a fourth aspect, this specification further provides an intermediate service system, including: at least one storage medium that stores at least one instruction set used to make a payment; and at least one processor that is communicatively connected to the at least one storage medium. The at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set. The payment method includes: when a terminal device displays an interaction page of the merchant system, receiving device information and a payment request from the merchant system, where the device information is collected by the merchant system from the terminal device, and the payment request represents that a target account requests to make a payment in the merchant system by using the

wallet system; sending the payment request and the device information to the wallet system, where the device information is used by the wallet system for a risk control procedure of the payment request; receiving a payment result corresponding to the payment request from the wallet system; and sending the payment result to the merchant system, so that the merchant system displays the payment result on an interaction page of the merchant system, where in a process of performing the payment method by the intermediate service system, the terminal device does not jump to an interaction page of the wallet system.

[0010] According to a fifth aspect, this specification further provides a wallet system, including: at least one storage medium that stores at least one instruction set used to make a payment; and at least one processor that is communicatively connected to the at least one storage medium. The at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set. The payment method includes: when a terminal device displays an interaction page of a merchant system and a target account initiates a payment operation for a target transaction on an interaction page of the merchant system, receiving device information and a payment request from an intermediate service system, where the device information is collected by the merchant system from the terminal device, and the intermediate service system provides an intermediate service between the merchant system and the wallet system; performing a risk control procedure on the payment request based on the device information, to obtain a risk control result; determining a payment result corresponding to the payment request based on the risk control result; and sending the payment result to the intermediate service system, so that the payment result is displayed on an interaction page of the merchant system, where in a process of performing the payment method by the wallet system, the terminal device does not jump to an interaction page of the wallet system.

[0011] According to a sixth aspect, this specification further provides a merchant system, including: at least one storage medium that stores at least one instruction set used to make a payment; and at least one processor that is communicatively connected to the at least one storage medium. The at least one processor reads the at least one instruction set when running, and performs a payment method based on an indication of the at least one instruction set. The payment method includes: when a terminal device displays an interaction page of the merchant system, collecting device information of the terminal device; in response to detecting that a target account initiates a payment operation for a target transaction on an interaction page of the merchant system,

sending the device information and a payment request to an intermediate service system, where the device information is used by a wallet system for a risk control procedure of the payment request, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; and receiving a payment result corresponding to the payment request from the intermediate service system, and displaying the payment result on an interaction page of the merchant system, where in a process of performing the payment method by the merchant system, the terminal device does not jump to an interaction page of the wallet system.

[0012] According to a seventh aspect, this specification provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set. When the at least one instruction set is executed by at least one processor, the method according to the first aspect, the second aspect, or the third aspect is implemented.

[0013] Other functions of the payment method, the intermediate service system, the wallet system, the merchant system, and the storage medium provided in this specification are partially listed in the following descriptions. Creative aspects of the payment method, the intermediate service system, the wallet system, the merchant system, 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

[0014] 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 derive other drawings from these accompanying drawings without creative efforts.

[0015] FIG. 1 is a schematic diagram of a cross-system jump scenario according to an embodiment of this specification;

[0016] FIG. 2 is a schematic diagram of a non-cross-system jump scenario according to an embodiment of this specification;

[0017] FIG. 3 is a schematic diagram of a payment scenario according to an embodiment of

this specification;

[0018] FIG. 4 is a diagram of a hardware structure of a service system according to an embodiment of this specification;

5 **[0019]** FIG. 5 is a schematic flowchart of a payment method according to an embodiment of this specification;

[0020] FIG. 6 is a schematic diagram of an identity verification procedure according to an embodiment of this specification;

[0021] FIG. 7 is a schematic diagram of a payment result in a non-cross-system jump scenario according to an embodiment of this specification;

10 **[0022]** FIG. 8 is another schematic diagram of a payment result in a non-cross-system jump scenario according to an embodiment of this specification;

[0023] FIG. 9 is a schematic flowchart of another payment method according to an embodiment of this specification; and

15 **[0024]** FIG. 10 is a schematic diagram of another identity verification procedure according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0025] 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. Various local modifications to the disclosed embodiments are clear to a person skilled in the art. In addition, the general principles defined herein can be applied to other
20 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.

[0026] The terms used herein are merely intended to describe specific example embodiments,
25 and impose no limitation. For example, unless otherwise explicitly stated in the context, the singular forms "one", "an", and "the" used herein can include plural forms. When being used in this specification, the terms "include", "comprise", and/or "contain" mean existence of an associated integer, step, operation, element, and/or component, but does not preclude existence of one or more other features, integers, steps, operations, elements, components, and/or groups or

addition of other features, integers, steps, operations, elements, components, and/or groups to the system/method.

[0027] 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.

[0028] 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 sequentially implemented. On the contrary, the operations can be implemented in a reverse sequence or simultaneously. In addition, one or more other operations can be added to the flowchart, and one or more operations can be removed from the flowchart.

[0029] There is often an account takeover (ATO) risk on the internet, that is, a wrongdoer accesses an account by using a technical means without authorization of an authorized user. The ATO risk can also be referred to as an account theft risk. In the payment field, the ATO risk not only causes property losses to the authorized user, but also causes claim losses to a wallet system. Therefore, the wallet system needs to perform ATO risk identification before paying for a transaction, that is, identify whether a wallet account associated with the current transaction is a stolen account. If the wallet account is a stolen account, the wallet system can reject the current payment. If the wallet account is not a stolen account, the wallet system can pay for the current transaction.

[0030] Generally, when performing ATO risk identification, the wallet system can use a device consistency-based risk control solution. Specifically, the wallet system can maintain a database, and the database stores device information of a commonly used device corresponding to each wallet account. The commonly used device is a device that has been used once or more times by the wallet account in a historical time period. The device information can be a device parameter set that can uniquely identify a device. In some embodiments, the wallet system can perform a specific operation on the device information, to obtain an identifier that can uniquely represent the

device information, and store the identifier in the database. The identifier can also be referred to as a device fingerprint. In this case, the database stores a device fingerprint of the commonly used device corresponding to each wallet account. After receiving a payment request sent by a wallet account by using a terminal device, the wallet system can match device information of the terminal device with a device fingerprint corresponding to the wallet account in the database (for example, perform a specific operation on the device information of the terminal device, to obtain a target identifier, and match the target identifier with the device fingerprint corresponding to the wallet account in the database), and identify, based on a matching result, whether the terminal device is a commonly used device corresponding to the wallet account. For example, if the terminal device is a commonly used device, it is considered that the wallet account is not a stolen account, and there is no ATO risk; or if the terminal device is not a commonly used device, it is considered that the wallet account is a stolen account, and there is an ATO risk.

[0031] The following separately describes payment risk control solutions and payment procedures respectively corresponding to a cross-system jump scenario (that is, a terminal device jumps from a merchant system to a wallet system in a payment procedure) and a non-cross-system jump scenario (that is, a terminal device does not jump from a merchant system to a wallet system in a payment procedure).

[0032] Cross-system jump scenario

[0033] A merchant system outputs an interaction page through a terminal device, and a user can initiate a transaction on the interaction page by using a target account. For the transaction, after the user initiates a payment operation on the interaction page of the merchant system, the terminal device jumps from the interaction page of the merchant system to an interaction page of a wallet system. The user can perform a payment procedure in the wallet system through the interaction page output by the terminal device. After the terminal device jumps to the wallet system, the wallet system can collect device information of the terminal device, and execute a risk control solution (for example, the ATO risk identification solution described above) based on the device information, to obtain a risk control result. Further, the wallet system can determine a payment result of the transaction based on the risk control result. The wallet system can feed back the payment result to the merchant system, and the merchant system displays the payment result to the user through the terminal device.

[0034] For example, as shown in FIG. 1, the user initiates, on an interaction page A of the

merchant system by using the target account, a target transaction for purchasing a commodity 2. After the user taps "Settle", the terminal device displays an interaction page B of the merchant system to the user. The user can select a payment method on the interaction page B. For example, the user taps "Payment method 2". In this case, a page displayed on the terminal device jumps
5 from the interaction page B to an interaction page 1 of the wallet system, and the interaction page 1 displays "Payment service in progress..." to the user. The wallet system makes a risk control decision (for example, performs the ATO risk identification solution described above on) for the current transaction based on the device information of the terminal device, to obtain a risk control result. Further, the wallet system can determine a payment result based on the risk control result,
10 and feed back the payment result to the merchant system. The merchant system can output an interaction page D through the terminal device, to display the payment result to the user. The device information required in the above-mentioned risk control process is collected by the wallet system from the terminal device after the terminal device jumps from the merchant system to the wallet system.

15 **[0035]** However, in the payment solution in the cross-system jump scenario, a payment process consumes a relatively long time due to the need to load resources and the like, and a payment procedure with a cross-system jump is relatively cumbersome. Each time an additional jump is made, a payment success probability may be affected due to a network or another reason, resulting in relatively poor user experience.

20 **[0036]** Non-cross-system jump scenario

[0037] For the transaction, after the user initiates a payment operation on the interaction page of the merchant system, the terminal device does not jump from the interaction page of the merchant system to an interaction page of a wallet system. The merchant system can send a payment request corresponding to the target transaction to the wallet system. In response to the
25 payment request, the wallet system indicates the merchant system to perform a plurality of types of identity verification on the user.

[0038] For example, as shown in FIG. 2, for content before the user selects a payment method on an interaction page B, refer to the descriptions in the cross-system jump scenario. Details are not described again. After the user selects "Payment method 2" on the interaction page B, the
30 terminal device does not jump to the interaction page of the wallet system, that is, the terminal device subsequently displays the interaction page of the merchant system to the user. For example,

the merchant system displays an identity verification page to the user, and the user can enter a plurality of types of identity verification information in an identity verification information input area. Alternatively, the merchant system displays a plurality of identity verification pages to the user, and the user can enter one type of identity verification information in an identity verification information input area on each identity verification page. Subsequently, the merchant system displays a payment result to the user through an interaction page D.

[0039] Because the terminal device does not jump to the wallet system, it is difficult for the wallet system to collect device information of the terminal device. Therefore, the wallet system cannot perform ATO risk identification based on the device information, and consequently it is relatively difficult for the wallet system to implement payment risk control. To ensure payment security of the user, a risk control policy used by the wallet system is to enable the merchant system to perform indiscriminate enhanced identity verification on users of all transactions, for example, perform a plurality of dimensions of identity verification on the user. The plurality of dimensions include at least two of the following: a static password, a dynamic password (for example, a verification code), a face, a fingerprint, and other biometric information. In this risk control policy, the user needs to enter a plurality of different types of identity verification information for each payment. In this case, relatively poor experience is caused, and it is likely that the user cancels the payment, affecting a payment success rate. In addition, if all of the plurality of types of identity verification information of the user are stolen, effective risk control still cannot be implemented in this solution.

[0040] In view of this, this specification provides a payment method, an intermediate service system, a wallet system, a merchant system, and a storage medium, to enable the wallet system to implement effective risk control without a cross-system jump, and improve user experience.

[0041] FIG. 3 is a schematic diagram of a payment scenario according to an embodiment of this specification.

[0042] As shown in FIG. 3, a scenario 001 includes a current user 110, a terminal device 120, a merchant system 10, and a wallet system 20. The merchant system 10 includes a merchant client 122 and a merchant server 132. The wallet system 20 includes a wallet client 124 and a wallet server 134. As shown in FIG. 3, the merchant client 122 and the wallet client 124 are deployed in the terminal device 120. The current user 110 may be an authorized user, or may be a wrongdoer stealing information related to an authorized user.

[0043] In some embodiments, the scenario 001 further includes an intermediate service system 30. The intermediate service system 30 is configured to provide an intermediate service between the merchant system 10 and the wallet system 20. The intermediate service system 30 includes an intermediate server 136. In some embodiments, the intermediate service system 30 can further include an intermediate service client (not shown in FIG. 3), and the intermediate service client can be deployed in the terminal device 120. The intermediate service client provides a checkout counter to a user, and the user can initiate a payment in the checkout counter. In some embodiments, the intermediate service client can be integrated into the merchant client 122 in a form. For example, the checkout counter is integrated into the merchant client 122 in a form of a software development kit (SDK). When the user initiates a settlement for a transaction in the merchant client 122, the merchant client 122 invokes the SDK to render a checkout counter page, so that the user initiates a payment in the checkout counter page.

[0044] In some embodiments, one or more applications (app) can be installed in the terminal device 120. The app includes but is 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 financial app program, an instant messaging tool, a mailbox client, social platform software, or the like. For example, a merchant system app (that is, the merchant client 122) and a wallet system app (that is, the wallet client 124) are installed in the terminal device 120.

[0045] The terminal device 120 can 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 can 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 can include a smart television, a desktop computer, or any combination. In some embodiments, the smart mobile device can 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 can include a vehicle-mounted computer, a vehicle-mounted television, or the

like. In some embodiments, the terminal device 120 can be a device with a location technology, configured to locate the terminal device 120.

[0046] For example, the terminal device 120 can display an interaction page to the current user 110. The current user 110 can perform a corresponding operation on the interaction page, to implement interaction with the merchant system and/or the wallet system.

[0047] In some embodiments, the merchant system 10 and the wallet system 20 cooperate with each other to perform the payment method provided in the embodiments of this specification. In an execution process, the terminal device 120 displays an interaction page of the merchant system to the current user 110, that is, the terminal device does not jump to an interaction page of the wallet system.

[0048] In some embodiments, the merchant system 10, the wallet system 20, and the intermediate service system 30 cooperate with each other to perform the payment method provided in the embodiments of this specification. Similarly, in an execution process, the terminal device 120 displays an interaction page of the merchant system to the current user 110, that is, the terminal device does not jump to an interaction page of the wallet system.

[0049] Specifically, in a process of performing the payment method provided in the embodiments of this specification, operations specifically performed by the system and the client and the server in the system are described in detail in the following method P500. Details are not described again.

[0050] The merchant server 132 and/or the wallet server 134 can be various types of servers, for example, can be a cloud server or a local server.

[0051] A communication connection medium between the merchant client 122 and the merchant server 132, a communication connection medium between the wallet client 124 and the wallet server 134, and a communication connection medium between the wallet server 134 and each of the merchant server 132 and the intermediate server 136 each may be a network. The network can facilitate exchange of information or data.

[0052] In some embodiments, the network can be any type of wired or wireless network, or a combination thereof. For example, the network can 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), Bluetooth™, a short-range

wireless network (ZigBee™), a near field communication (NFC) network, or a similar network.

[0053] In some embodiments, the network can include one or more network access points. For example, the network can 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 120 and the merchant server 132 may be connected to a network to exchange data or information; one or more components of the terminal device 120 and the wallet server 134 may be connected to a network to exchange data or information; and one or more components of the merchant server 132, the wallet server 134, and the intermediate server 136 may be connected to a network to exchange data or information.

[0054] FIG. 4 is a diagram of a hardware structure of a service system 300 according to an embodiment of this specification. The service system 300 can be a merchant system 10, a wallet system 20, or an intermediate service system 30.

[0055] As shown in FIG. 4, the service system 300 can include at least one storage medium 303 and at least one processor 302. In some embodiments, the service system 300 can further include a communication port 304 and an internal communication bus 301. In some embodiments, the service system 300 can further include an I/O component 305.

[0056] The internal communication bus 301 can be connected to different system components. For example, the internal communication bus 301 can be connected to the storage medium 303, the processor 302, the communication port 304, and the I/O component 305.

[0057] The I/O component 305 supports an input/output between the service system 300 and another component.

[0058] The communication port 304 is used for data communication between the service system 300 and the outside. For example, the communication port 304 can be used for data communication between the service system 300 and a network. The communication port 304 can be a wired communication port, or can be a wireless communication port.

[0059] The storage medium 303 can include a data storage apparatus. The data storage apparatus can be a non-transitory storage medium, or can be a transitory storage medium. For example, the data storage apparatus can include one or more of a disk 3031, a read-only storage medium (ROM) 3032, or a random access storage medium (RAM) 3033. The storage medium 303 further includes at least one instruction set stored in the data storage apparatus. The instruction set includes computer program code, and the computer program code can include a program, a routine,

an object, a component, a data structure, a process, a module, and the like for performing the payment method provided in the embodiments of this specification.

[0060] The at least one processor 302 can be communicatively connected to the at least one storage medium 303. The at least one processor 302 is configured to execute the at least one instruction set. When the service system 300 runs, the at least one processor 302 reads the at least one instruction set, and performs, based on an indication of the at least one instruction set, the payment method provided in the embodiments of this specification. The processor 302 can perform all steps included in the payment method. The processor 302 can be in a form of one or more processors. In some embodiments, the processor 302 can 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, processor, or the like that can perform one or more functions, or any combination thereof.

[0061] To merely describe a problem, only one processor 302 is shown in the service system 300 in the accompanying drawings. However, it should be noted that the service system 300 in this specification can further include a plurality of processors. Therefore, the operations and/or method steps disclosed in this specification can be performed by one processor, or can be jointly performed by a plurality of processors. For example, if the processor 302 in the service system 300 described in this specification performs step A and step B, it should be understood as that step A and step B can be jointly or separately performed by two different processors 302 (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).

[0062] FIG. 5 is a schematic interaction diagram of a payment method P500 according to an embodiment of this specification. As shown in FIG. 5, the payment method P500 is cooperatively performed by a current user, a merchant system, an intermediate service system, and a wallet system. The intermediate service system provides an intermediate service to the merchant system and the wallet system, and can include an intermediate client and an intermediate server, or can include only an intermediate server. The intermediate service system is, for example, an acquiring system. The payment method P500 includes S510 to S590.

[0063] S510: When a terminal device displays an interaction page of the merchant system, the merchant system collects device information of the terminal device.

[0064] The interaction page of the merchant system can be understood as a page that is provided by the merchant system or output by the merchant system through the terminal device and that is used for interaction between the current user and the merchant system. The merchant system includes a merchant client and a merchant server.

[0065] For example, the interaction page is a page displayed by the merchant client to the current user through the terminal device. The current user can interact with the merchant client through the page, or can interact with the merchant server through the page.

[0066] Specifically, for interaction between the current user and the merchant system, refer to the part and related descriptions in FIG. 1 or FIG. 2. Details are not described again.

[0067] For example, when the terminal device displays the interaction page of the merchant system, the merchant client can collect the device information of the terminal device. In some embodiments, the intermediate service system can provide a checkout counter service to the merchant system. An SDK corresponding to the checkout counter service can be integrated into the merchant client, and the merchant client can collect the device information of the terminal device by using the SDK. In some embodiments, when detecting that a target user initiates a settlement in a transaction page of the merchant system, the merchant client renders a checkout counter page by using the SDK, and collects the device information of the terminal device by using the SDK.

[0068] In some embodiments, the device information of the terminal device includes at least one of the following:

a hardware parameter of the terminal device, a software parameter of the terminal device, a network parameter of the terminal device, and a behavior feature of the current user of the terminal device.

[0069] For example, the hardware parameter includes but is not limited to a central processing unit (CPU) type, a memory capacity, a hard disk serial number, a media access control (MAC) address, a universal serial bus (USB) device, and graphics card information. The software parameter includes but is not limited to an operating system type, an operating system version, a font, screen resolution, a time zone, a language setting, and the like. The network parameter includes but is not limited to an internet protocol (IP) address, a network location, internet service

provider (ISP) information, a network connection type (for example, Wi-Fi or cellular data), and the like. The behavior feature includes but is not limited to a browsing habit, a tap frequency, a dwell time, and the like.

[0070] In this embodiment, the device information collected by the merchant system is relatively comprehensive, to subsequently provide a basis to a risk control procedure of a payment request.

[0071] S520: The current user initiates a payment operation for a target transaction on an interaction page of the merchant system by using a target account.

[0072] The target account is an account registered with or applied for from the merchant system by an authorized user, can be used to initiate the target transaction in the merchant system, and the like. The current user may be the authorized user, or may be a wrongdoer stealing information related to the authorized user.

[0073] For example, the current user initiates, by using the target account, a payment operation for the target transaction on the interaction page displayed by the merchant client. For example, as shown in FIG. 1, a virtual button such as "Payment method 2" is tapped to initiate a payment operation. It can be understood that the interaction page of the merchant system in S510 and the interaction page of the merchant system in S520 can be a same page or different pages. This is not limited in this embodiment of this specification.

[0074] S530: In response to detecting the payment operation, the merchant system sends the device information and a payment request to the intermediate service system (for example, the intermediate server).

[0075] The payment request can include information related to the target transaction, for example, a payment amount and a payment account.

[0076] There can be a plurality of implementations in which the merchant system sends the payment request and the device information to the intermediate service system. In some embodiments, the merchant system can simultaneously send the payment request and the device information. That is, the merchant system sends the payment request and the device information by including the payment request and the device information in a same message. In this case, the message sent by the merchant system to the intermediate service system includes the payment request and the device information. For example, in S510, after collecting the device information of the terminal device, the merchant system can first store the device information. After detecting

the payment operation, the merchant system sends the payment request and the device information to the intermediate service system. In some embodiments, the merchant system can sequentially send the payment request and the device information. For example, the merchant system first sends the payment request and then sends the device information, or the merchant system first sends the device information and then sends the payment request. For example, in S510, after collecting the device information of the terminal device, the merchant system can immediately send the device information to the intermediate service system, and after detecting the payment operation, send the payment request to the intermediate service system. That is, the payment request and the device information can be respectively carried in different messages and sent by the merchant system.

[0077] In addition, when sending the device information, the merchant system can send the device information itself, or can send related information that can represent the device information. When the merchant system sends the related information that can represent the device information, a form of the related information is not limited in this specification. For example, the merchant system can process or perform a specified operation on the device information, to obtain result information, and send the result information to the intermediate service system. After receiving the result information, the intermediate service system or the wallet system can calculate the device information based on the result information. For another example, the merchant system can process the device information by using a specific tool, to obtain an identifier (that is, a device fingerprint) that can uniquely represent the device information, and send the identifier to the intermediate service system. The specific tool can be a device fingerprint software development kit (SDK).

[0078] In some embodiments, the device information sent by the merchant system to the intermediate service system in S530 can be a part of the device information collected by the merchant system in S510.

[0079] For example, the merchant client or the merchant server selects some representative parameters in the device information that do not involve device privacy, and sends the parameters to the intermediate service system.

[0080] In the above-mentioned embodiment, the merchant system tries to transfer some information that can be used for payment risk control to the intermediate service system while considering a privacy problem, to provide a basis for payment risk control performed by a downstream system (for example, the intermediate service system or the wallet system), so as to

improve accuracy of risk control performed by the downstream system.

[0081] For example, in S510, after collecting the device information of the terminal device, the merchant client can send the device information to the merchant server. In S520, the merchant client generates the payment request in response to detecting the payment operation. The merchant client sends the payment request to the merchant server. After receiving the payment request, the merchant server sends the payment request and the device information to the intermediate service system (the intermediate server).

[0082] In some embodiments, before performing S530, the merchant system can further perform risk control on the target transaction, to obtain risk control advice information. In this way, in S530, in response to the payment operation, the merchant system can further send the risk control advice information to the intermediate service system. The risk control advice information is used by the downstream system (the intermediate service system or the wallet system) for a risk control procedure of the payment request. For example, the merchant system can simultaneously send the risk control advice information, the payment request, and the device information, or can sequentially send the risk control advice information, the payment request, and the device information.

[0083] For example, the merchant system performs risk identification on the target transaction based on at least one of internal information of the merchant system and the device information, to generate the risk control advice information.

[0084] The internal information of the merchant system includes at least one of the following: transaction information of the target transaction and user information corresponding to the target account.

[0085] The transaction information of the target transaction includes but is not limited to a transaction amount, a transaction object, a transaction time, a logistics address, and the like.

[0086] The user information corresponding to the target account includes but is not limited to information about registration of the target account with the merchant system; and user behavior data of the target account in the merchant system. The user behavior data includes but is not limited to a browsing habit, a tap frequency, a preference, a dwell time, a transaction frequency, and the like.

[0087] The merchant system can perform risk identification on the target transaction in a plurality of manners. The following uses several manners as examples. This is not limited in this

embodiment of this specification.

[0088] For example, after obtaining the internal information or the device information, a risk controller of the merchant system obtains a risk identification result based on manual experience, and enters the risk identification result in the merchant system. The merchant system generates the risk control advice information based on the risk identification result.

[0089] For example, the merchant system presets a risk identification model, and inputs the internal information and/or the device information to the risk identification model to obtain the risk control advice information.

[0090] For example, the merchant system presets a plurality of risk identification conditions (or risk identification rules), and obtains the risk control advice information based on the internal information and/or the device information, and the plurality of risk identification conditions. The risk identification condition is, for example, whether a recent transaction frequency of the target account exceeds a threshold.

[0091] In a risk identification process, the merchant system can identify at least one risk. The at least one risk includes but is not limited to a risk of whether the target account is stolen, a root risk, a jailbreak risk, a hijacking injection risk, a simulator risk, and the like. The root risk is a related security risk, for example, a risk that the terminal device or a system installed on the terminal device is granted superuser permission. The jailbreak risk is a risk of bypassing operating system restrictions on the terminal device to obtain root-level system access permission. The hijacking injection risk means that the terminal device allows an attacker to manipulate or deceive a user or a system by injecting malicious code or tampering with a data flow. The simulator risk is a risk that on the terminal device, there may be a simulator that can be used to obtain access permission to a host system.

[0092] It can be understood that the risk identification process can be performed on the merchant client, or can be performed on the merchant server. This is not limited in this embodiment of this specification.

[0093] For example, the merchant system can alternatively determine the risk control advice information based on the device information. For example, the merchant system can perform ATO risk identification on a merchant side based on the device information, to obtain the risk control advice information. A process of performing ATO risk identification by the merchant system is similar to the process of performing ATO risk identification by the wallet system described above.

For example, the merchant system obtains device information of a commonly used device corresponding to the target account from a database, matches the device information of the commonly used device with the device information of the current terminal device, to obtain a matching result, and further obtains the risk control advice information based on the matching
5 result.

[0094] In this embodiment, the merchant system can collect relatively comprehensive device information, and has relatively rich internal information, so that a behavior trace of a wrongdoer can be obtained. Some of the information involves privacy and cannot be transmitted to the downstream system. Therefore, the merchant system performs risk identification on the target
10 transaction in advance based on the multi-dimensional information, to transfer the risk control advice information to the intermediate service system. In this manner, a problem that the downstream system cannot accurately perform risk control because the device information cannot be collected can be resolved. In addition, in this embodiment, the risk control advice information is transferred by the merchant system to the downstream system. This can assist the downstream
15 system in performing the risk control procedure on the payment request, to achieve a purpose of joint prevention and control by the merchant system, the intermediate service system, and the wallet system, and improve accuracy of payment risk control in a non-jump scenario.

[0095] In some embodiments, the risk control advice information represents at least a risk level of the target transaction.

[0096] The risk level reflects a level/severity of a risk corresponding to the target transaction. For example, the risk level of the target transaction can be a high risk, a medium risk, or a low risk. Alternatively, the risk level of the target transaction can be "risky" or "risk-free".

[0097] In some embodiments, the risk control advice information can further represent a risk control policy corresponding to the target transaction.

[0098] For example, if the risk level represented by the risk control advice information is a high risk, the risk control policy corresponding to the target transaction can be interception. Alternatively, if the risk level represented by the risk control advice information is a medium risk, the risk control policy corresponding to the target transaction can be enhanced identify verification. For example, identity verification is performed on the current user by using a plurality of identity
25 verification methods, or identity verification is performed on the current user by using a specific
30 identity verification method. Alternatively, if the risk level represented by the risk control advice

information is a low risk, the risk control policy corresponding to the target transaction can be release, that is, a payment for the target transaction can be completed without identity verification.

[0099] S540: The intermediate service system sends the device information and the payment request to the wallet system. Correspondingly, the wallet system receives the device information and the payment request. The device information can be used by the wallet system (for example, the wallet server) for the risk control procedure of the payment request.

[0100] In some embodiments, before S530, the merchant system can further perform risk identification on the target transaction based on at least one of the internal information of the merchant system and the device information, to generate the risk control advice information. In S530, in response to the payment operation, the merchant system can send the payment request, the device information, and the risk control advice information to the intermediate service system. In S540, the intermediate service system sends the payment request, the device information, and the risk control advice information to the wallet system. Both the device information and the risk control advice information can be used by the wallet system for the risk control procedure of the payment request.

[0101] In some embodiments, the intermediate service system can have a capability to provide a risk control service. In S530, in response to the payment operation, the merchant system sends the payment request and the device information to the intermediate service system. After receiving the payment request and the device information, the intermediate service system can perform risk identification on the target transaction based on at least one of internal information of the intermediate service system, the payment request, and the device information, to obtain the risk control advice information. In S540, the intermediate service system can simultaneously send the payment request, the device information, and the risk control advice information to the wallet system, or sequentially send the risk control advice information, the payment request, and the device information. In this embodiment, the risk control advice information is provided by the intermediate service system. In this way, joint risk control by the intermediate service system and the wallet system is implemented, to improve accuracy of a risk control result.

[0102] The internal information of the intermediate service system includes at least one of the following: historical transaction information corresponding to the target account. The historical transaction information is transaction information of a historical transaction that the target account participates in a historical time period. The transaction information of the historical transaction

includes but is not limited to a transaction amount, a transaction object, a transaction time, a logistics address, and the like.

[0103] For example, the intermediate service system can perform risk identification on the target transaction in a plurality of manners. The following uses several manners as examples. This is not limited in this embodiment of this specification.

[0104] For example, after obtaining the internal information, the payment request, and the device information, a risk controller of the intermediate service system obtains a risk identification result based on manual experience, and enters the risk identification result in the intermediate service system. The intermediate service system generates the risk control advice information based on the risk identification result.

[0105] For example, the intermediate service system presets a risk identification model, and inputs at least one of the internal information, the payment request, and the device information to the risk identification model, to obtain the risk control advice information.

[0106] For example, the intermediate service system presets a plurality of risk identification conditions (or risk identification rules), and obtains the risk control advice information based on at least one of the internal information, the payment request, and the device information, and the plurality of risk identification conditions. The risk identification condition is, for example, whether a recent transaction frequency of the target account exceeds a threshold.

[0107] For at least one risk that can be identified by the intermediate service system in a risk identification process, refer to the above-mentioned descriptions. Details are not described again.

[0108] It can be understood that the risk identification process can be performed on the intermediate server. This is not limited in this embodiment of this specification.

[0109] For example, the intermediate service system can alternatively determine the risk control advice information based on the device information. For example, the intermediate service system can perform ATO risk identification based on the device information, to obtain the risk control advice information. A process of performing ATO risk identification by the intermediate service system is similar to the process of performing ATO risk identification by the wallet system described above. Details are not described again.

[0110] In the above-mentioned embodiment, the wallet system can determine the severity of the risk corresponding to the target transaction by using the risk control advice information, and can further determine whether risk identification needs to be further performed on the target

transaction, to implement strict risk control, so as to avoid a problem that a target transaction with a high risk cannot be accurately identified. In addition, the wallet system can further determine, based on the risk level represented by the risk control advice information, a level of an identity verification method to be used for the payment for the target transaction, to perform targeted
5 identity verification on the current user.

[0111] S550: The wallet system performs the risk control procedure on the payment request based on the device information, to obtain a risk control result.

[0112] For example, the wallet system performs risk identification on the target transaction based on the device information, to obtain the risk level of the target transaction. For a manner in
10 which the wallet system performs risk identification based on the device information, refer to the above-mentioned descriptions. Details are not described again.

[0113] In some embodiments, when the wallet system further receives the risk control advice information provided by the merchant system or the intermediate service system, the wallet system can perform the risk control procedure on the payment request based on the risk control advice
15 information and the device information, to obtain the risk control result.

[0114] In this embodiment, in a payment risk control process, in addition to considering the risk control advice information, the wallet system further performs risk identification based on the available information. That is, the merchant system, the intermediate service system, and the wallet system perform joint prevention and control. As information available to two or more systems is
20 used as a basis for risk control, a more comprehensive dimension is considered, and accuracy of risk control can be improved.

[0115] It can be understood that the risk identification process can be performed on the wallet server, or can be performed by a risk control service provider that cooperates with the wallet system. This is not limited in this embodiment of this specification. The following uses execution by the
25 wallet server as an example for description.

[0116] For example, the wallet server determines a first risk level corresponding to the target transaction based on the risk control advice information; performs risk identification on the target transaction based on the device information, to obtain a second risk level corresponding to the target transaction; and determines the risk control result based on the first risk level and the second
30 risk level.

[0117] The wallet server can determine the second risk level in the following manner.

[0118] For example, the wallet server performs risk identification on the target transaction based on the device information, to obtain the second risk level. For a manner in which the wallet server performs risk identification based on the device information, refer to the above-mentioned descriptions. Details are not described again.

5 **[0119]** For another example, the wallet server performs risk identification on the target transaction based on internal information of the wallet system and the device information, to obtain the second risk level. The internal information of the wallet system includes at least one of the following: user information corresponding to the payment request and transaction information corresponding to the target transaction.

10 **[0120]** The user information corresponding to the payment request can be understood as information related to a payment account associated with the target account in the wallet system. The user information includes but is not limited to user registration information, historical payment information, and historical device information of the payment account. The historical device information is device information of a terminal device involved in a historical payment process of
15 the payment account. The wallet server can search a database of the wallet system based on the payment request, to obtain the internal information. A manner in which the wallet server performs risk identification based on the internal information and/or the device information is similar to the manner in which the merchant system or the intermediate service system performs risk identification. References can be made to the above-mentioned descriptions. Details are not
20 described again.

[0121] The wallet server can determine the risk control result in the following manner.

[0122] For example, if the first risk level is higher than the second risk level, the wallet server uses the first risk level as the risk control result; if the first risk level is lower than the second risk level, the wallet server uses the second risk level as the risk control result; or if the first risk level
25 is equal to the second risk level, the wallet server uses the first risk level or the second risk level as the risk control result.

[0123] In this example, the wallet system uses a risk identification result with a high risk level as a final risk control result. More strict risk control is implemented, to effectively protect payment security of the user.

30 **[0124]** S560: The wallet system determines a payment result corresponding to the payment request based on the risk control result.

[0125] For example, if a risk level corresponding to the risk control result is higher than or equal to a first preset risk level, the wallet server determines that the payment result is a payment failure; or if a risk level corresponding to the risk control result is lower than or equal to a second preset risk level, the wallet server determines to perform a payment procedure to obtain the payment result.

[0126] A risk degree of the first preset risk level is higher than that of the second preset risk level. For example, the first preset risk level is a high risk, and the second preset risk level is a low risk.

[0127] For example, if the risk level corresponding to the risk control result is lower than the first preset risk level and higher than the second preset risk level, before the payment result is determined, the payment method P500 further includes an identity verification step shown in FIG. 6.

[0128] S5610: The wallet system sends an identity verification instruction to the intermediate service system. Correspondingly, the intermediate service system receives the identity verification instruction.

[0129] In some embodiments, the identity verification instruction includes a target identity verification method.

[0130] For example, the target identity verification method includes but is not limited to one or more of the following: password-based identity verification, verification code-based identity verification, face-based identity verification, iris-based identity verification, fingerprint-based identity verification, and the like.

[0131] S5620: The intermediate service system sends the identity verification instruction to the merchant system. Correspondingly, the merchant system receives the identity verification instruction.

[0132] For example, the intermediate server sends the identity verification instruction to the merchant server, and the merchant server sends the identity verification instruction to the terminal device or the merchant client.

[0133] S5630: In response to the identity verification instruction, the merchant system displays an identity verification page on an interaction page of the merchant system, and obtains identity verification information collected through the identity verification page.

[0134] In some embodiments, the merchant system displays, on the interaction page of the

merchant system, an identity verification page corresponding to the target identity verification method.

[0135] For example, as shown in FIG. 7 or FIG. 8, the merchant client in the merchant system displays the identity verification page to the current user, and the identity verification page displays the target identity verification method and an identity verification information input area. The current user enters, in the input area, identity verification information corresponding to the target identity verification method. For example, if the identity verification method displayed on the identity verification page is password-based identity verification, the current user needs to enter a password in the input area, and so on.

[0136] S5640: The merchant system sends the identity verification information to the intermediate service system. Correspondingly, the intermediate service system receives the identity verification information.

[0137] For example, after the identity verification information is entered, the merchant client or the terminal device can send the identity verification information to the merchant server, and the merchant server can send the identity verification information to the intermediate server.

[0138] S5650: The intermediate service system sends the identity verification information to the wallet system, so that the wallet system performs identity verification based on the identity verification information. Correspondingly, the wallet system receives the identity verification information.

[0139] For example, the intermediate server can send the identity verification information to the wallet server, and the wallet server performs identity verification on the current user based on the identity verification information.

[0140] S5660: The wallet system determines the payment result based on the identity verification information.

[0141] For example, if the wallet server determines that the identity verification succeeds, the payment procedure is performed to obtain the payment result; or if the wallet server determines that the identity verification does not succeed, it is determined that the payment result is a payment failure.

[0142] In this case, identity verification in a case in which the risk level corresponding to the risk control result is lower than the first preset risk level and higher than the second preset risk level is completed, and the payment result is obtained.

[0143] S570: The wallet system sends the payment result to the intermediate service system. Correspondingly, the intermediate service system receives the payment result.

[0144] S580: The intermediate service system sends the payment result to the merchant system. Correspondingly, the merchant system receives the payment result.

5 **[0145]** For example, the intermediate server sends the payment result to the merchant server, and the merchant server sends the payment result to the merchant client or the terminal device.

[0146] S590: The merchant system displays the payment result on an interaction page.

[0147] For example, as shown in FIG. 7 or FIG. 8, after the current user enters the identity verification information, the merchant client jumps to an interaction page E, and displays
10 "Payment service in progress..." to the current user. As shown in FIG. 7, if the identity verification succeeds, the merchant client displays an interaction page D1, and displays a payment result of "Payment successful!" to the current user. As shown in FIG. 8, if the identity verification does not succeed, the merchant client displays an interaction page D2, and displays a payment result of "Unable to make a payment!" or "Payment failed!" to the current user.

15 **[0148]** It should be noted that the payment method P500 can have other variations. For example, in S530, the merchant system simultaneously or sequentially sends the payment request and the risk control advice information to the intermediate service system, but does not send the device information. In S540, the intermediate service system simultaneously or sequentially sends the payment request and the risk control advice information to the wallet system, but does not send
20 the device information. In this case, S550 can be replaced with that the wallet system performs the risk control procedure on the payment request based on the risk control advice information, to obtain a risk control result. For example, the wallet system directly uses the risk control advice information as a final risk control result. For another example, the wallet system determines a third risk level based on the internal information of the wallet system; determines a first risk level based
25 on the risk control advice information; and further determines the risk control result based on the first risk level and the third risk level. For a specific implementation of determining the risk control result by the wallet system, refer to the above-mentioned descriptions. Details are not described again.

[0149] FIG. 9 is a schematic interaction diagram of a payment method P900 according to an
30 embodiment of this specification. As shown in FIG. 9, the payment method P900 is cooperatively performed by a current user (a current user of a terminal device or a current user of a target account),

a merchant system, and a wallet system. The payment method P900 includes S910 to S970.

[0150] S910: When the terminal device displays an interaction page of the merchant system, the merchant system collects device information of the terminal device.

[0151] S920: The current user initiates a payment operation for a target transaction on an interaction page of the merchant system by using the target account.

[0152] S910-S920 are similar to S510-S520. References can be made to the above-mentioned descriptions. Details are not described again.

[0153] S930: In response to detecting the payment operation, the merchant system sends the device information and a payment request to the wallet system. The device information can be used by the wallet system for a risk control procedure of the payment request.

[0154] S930 is similar to S530, except that the device information and the payment request are received by a different body. For other content, refer to the above-mentioned descriptions. Details are not described again.

[0155] S940: The wallet system performs the risk control procedure on the payment request based on the device information, to obtain a risk control result.

[0156] It should be noted that S940 is similar to S550. References can be made to the above-mentioned descriptions. Details are not described again.

[0157] S950: The wallet system determines a payment result corresponding to the payment request based on the risk control result.

[0158] For example, if a risk level corresponding to the risk control result is higher than or equal to a first preset risk level, the wallet server determines that the payment result is a payment failure; or if a risk level corresponding to the risk control result is lower than or equal to a second preset risk level, the wallet server determines to perform a payment procedure to obtain the payment result.

[0159] A risk degree of the first preset risk level is higher than that of the second preset risk level. For example, the first preset risk level is a high risk, and the second preset risk level is a low risk.

[0160] For example, if the risk level corresponding to the risk control result is lower than the first preset risk level and higher than the second preset risk level, before the payment result is determined, the payment method P900 further includes an identity verification step shown in FIG. 10.

[0161] S9510: The wallet system sends an identity verification instruction to the merchant system. Correspondingly, the merchant system receives the identity verification instruction.

[0162] S9520: In response to the identity verification instruction, the merchant system displays an identity verification page on an interaction page of the merchant system, and obtains identity verification information collected through the identity verification page.

[0163] S9530: The merchant system sends the identity verification information to the wallet system, so that the wallet system performs identity verification based on the identity verification information. Correspondingly, the wallet system receives the identity verification information.

[0164] S9540: The wallet system determines the payment result based on the identity verification information.

[0165] S960: The wallet system sends the payment result to the merchant system. Correspondingly, the merchant system receives the payment result.

[0166] S970: The merchant system displays the payment result on an interaction page of the merchant system.

[0167] S950-S970 are similar to S560-S590, except that a message transmitted between the merchant system and the wallet system does not need to be forwarded by an intermediate service system. For other content, refer to the above-mentioned descriptions. Details are not described again.

[0168] It should be noted that the payment method P900 can have other variations. For example, in S930, the merchant system sends the payment request and risk control advice information to the wallet system, but does not send the device information. In this case, S940 can be replaced with that the wallet system performs the risk control procedure on the payment request based on the risk control advice information, to obtain a risk control result. For a subsequent implementation, refer to the above-mentioned descriptions. Details are not described again.

[0169] In conclusion, according to the payment method, the intermediate service system, the wallet system, the merchant system, and the storage medium provided in this specification, in a payment scenario in which the terminal device does not make a cross-system jump, the merchant system can collect the device information of the terminal device, and transfer the device information to the wallet system, so that the wallet system can obtain the device information of the terminal device, and perform payment risk control based on the device information. In this way, a problem that the wallet system cannot perform effective risk control because the device

information cannot be collected (for example, a problem that the wallet system cannot intercept a risky transaction in a timely manner when a wrongdoer uses a stolen account to make a payment) can be avoided. In addition, the intermediate service system can further make a risk control decision based on rich information that can be collected by the merchant system, and provide risk control advice information to the wallet system, to implement joint risk control between the intermediate service system and the wallet system, so as to improve accuracy and control of risk control. Further, the wallet system can further use different identity verification policies for users of transactions with different risk levels based on a risk control result, to avoid disturbing a low-risk user and improve user experience.

[0170] According to another aspect of this specification, a computer-readable non-transitory storage medium is provided, and stores at least one group of executable instructions used to make a payment. When the executable instructions are executed by a processor, the executable instructions instruct the processor to implement the steps in the method P500 or P900 described in this specification. In some possible implementations, various aspects of this specification can be further implemented in a form of a program product, including program code. When the program product runs on the service system 300, the program code is used to enable the service system 300 to perform the steps in the method P500 or P900 described in this specification. The program product configured to implement the above-mentioned method can be a portable compact disc read-only memory (CD-ROM) that includes program code, and can run in the service system 300. However, the program product in this specification is not limited thereto. In this specification, the readable storage medium can be any tangible medium that includes or stores a program, and the program can be used by or in combination with an instruction execution system. The program product can be any combination of one or more readable media. The readable medium can be a readable signal medium or a readable storage medium. For example, the readable storage medium can be but is not limited to an electrical system, apparatus, or device, a magnetic system, apparatus, or device, an optical system, apparatus, or device, an electromagnetic system, apparatus, or device, an infrared system, apparatus, or device, or a 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 a 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 can include a data signal propagated in a baseband or as part of a carrier, and carries readable program code. The propagated data signal can be in a plurality of forms, including but not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium can alternatively be any readable medium other than the readable storage medium, and the readable medium can 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 can be transmitted by using any proper medium, including but not limited to a wireless medium, a wired medium, an optical cable, an RF medium, or any proper combination thereof. Program code for performing the operations in this specification can be written by using any combination of one or more program design languages. The program design language includes an object-oriented program design language, for example, Java or C++, and further includes a conventional procedural program design language, for example, "C" language, or a similar program design language. The program code can be completely executed on the service system 300, partially executed on the service system 300, executed as an independent software package, partially executed on the service system 300 and partially executed on a remote computing device, or completely executed on a remote computing device.

[0171] The term "and/or" in the embodiments of this specification describes an association relationship between associated objects, and indicates that three relationships can exist. For example, A and/or B can indicate the following three cases: Only A exists, both A and B exist, and only B exists. The character "/" usually indicates an "or" relationship between associated objects.

[0172] 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.

[0173] "Plurality of" in the embodiments of this specification shall be understood as two or more unless otherwise specified.

[0174] 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 can be performed in a sequence different from that in the embodiments and desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular sequence or consecutive sequence to achieve the desired results. In

some implementations, multitasking and parallel processing are possible or may be advantageous.

[0175] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the detailed disclosure can be presented only by using an example, and can 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 provided in this specification, and fall within the spirit and scope of the example embodiments of this specification.

[0176] In addition, some terms in this specification are used to describe the embodiments of this specification. For example, "one embodiment", "embodiments", and/or "some embodiments" mean/means that specific features, structures, or characteristics described with reference to the embodiment can be included in at least one embodiment of this specification. Therefore, it can be emphasized and understood that two or more of "embodiments", "one embodiment", or "alternative embodiments" in each part of this specification do not necessarily indicate a same embodiment. In addition, specific features, structures, or characteristics can be properly combined in one or more embodiments of this specification.

[0177] It should be understood that in the above-mentioned 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 drawings, or descriptions 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 label some devices and understand the devices as separate embodiments when reading this specification. That is, the embodiments of this specification can also be understood as an integration of a plurality of secondary embodiments. The content of each secondary embodiment is also true when a quantity of features is less than a quantity of all features in a single previously disclosed embodiment.

[0178] 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 herein by reference and used for all purposes now or later associated with this document. In addition, the terms in this document shall prevail if there is any inconsistency or conflict between

the descriptions, definitions, and/or use of the related terms in any material and the descriptions, definitions, and/or use of the related terms in this document.

[0179] 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.

10

CLAIMS

What is claimed is:

1. A payment method, applied to an intermediate service system that provides an intermediate service between a merchant system and a wallet system, wherein the method comprises:

5 when a terminal device displays an interaction page of the merchant system, receiving device information and a payment request from the merchant system, wherein the device information is collected by the merchant system from the terminal device, and the payment request represents that a target account requests to pay for a target transaction in the merchant system by using the wallet system;

10 sending the payment request and the device information to the wallet system, wherein the device information is used by the wallet system for a risk control procedure of the payment request; receiving a payment result corresponding to the payment request from the wallet system; and sending the payment result to the merchant system, so that the merchant system displays the payment result on an interaction page of the merchant system, wherein

15 in a process of performing the payment method by the intermediate service system, the terminal device does not jump to an interaction page of the wallet system.

2. The method according to claim 1, wherein before the receiving the payment result, the method further comprises:

20 sending risk control advice information to the wallet system, wherein the risk control advice information is used by the wallet system for the risk control procedure of the payment request.

3. The method according to claim 2, wherein before the sending risk control advice information to the wallet system, the method further comprises:

25 performing risk identification on the target transaction based on at least one of internal information of the intermediate service system and the device information, to generate the risk control advice information, wherein the internal information of the intermediate service system comprises at least historical transaction information corresponding to the target account.

4. The method according to claim 2, wherein the risk control advice information represents at least a risk level of the target transaction.

30 5. The method according to claim 1, wherein before the receiving the payment result, the method further comprises:

receiving an identity verification instruction from the wallet system;

sending the identity verification instruction to the merchant system, so that the merchant system collects identity verification information through an identity verification page;

receiving the identity verification information from the merchant system; and

5 sending the identity verification information to the wallet system, so that the wallet system performs identity verification based on the identity verification information.

6. The method according to claim 5, wherein the identity verification instruction comprises a target identity verification method, so that the merchant system displays an identity verification page corresponding to the target identity verification method.

10 7. The method according to claim 1, wherein the device information comprises at least one of the following:

a hardware parameter of the terminal device;

a software parameter of the terminal device;

a network parameter of the terminal device; and

15 a behavior feature of a current user of the terminal device.

8. A payment method, applied to a wallet system, wherein the method comprises:

when a terminal device displays an interaction page of a merchant system and a target account initiates a payment operation for a target transaction on an interaction page of the merchant system, receiving a payment request and device information from an intermediate service system, wherein
20 the device information is collected by the merchant system from the terminal device, and the intermediate service system provides an intermediate service between the merchant system and the wallet system;

performing a risk control procedure on the payment request based on the device information, to obtain a risk control result;

25 determining a payment result corresponding to the payment request based on the risk control result; and

sending the payment result to the intermediate service system, so that the payment result is displayed on an interaction page of the merchant system, wherein

in a process of performing the payment method by the wallet system, the terminal device does
30 not jump to an interaction page of the wallet system.

9. The method according to claim 8, wherein the method further comprises:

receiving risk control advice information from the intermediate service system; and
the performing a risk control procedure on the payment request based on the device
information, to obtain a risk control result comprises:

performing the risk control procedure on the payment request based on the risk control advice
5 information and the device information, to obtain the risk control result.

10. The method according to claim 9, wherein the risk control advice information represents
at least a risk level of the target transaction, and the performing the risk control procedure on the
payment request based on the risk control advice information and the device information, to obtain
the risk control result comprises:

10 determining a first risk level corresponding to the target transaction based on the risk control
advice information;

performing risk identification on the target transaction based on the device information, to
obtain a second risk level corresponding to the target transaction; and

determining the risk control result based on the first risk level and the second risk level.

15 11. The method according to claim 10, wherein the performing risk identification on the target
transaction based on the device information, to obtain a second risk level corresponding to the
target transaction comprises:

performing risk identification on the target transaction based on internal information of the
wallet system and the device information, to obtain the second risk level, wherein the internal
20 information of the wallet system comprises at least user information corresponding to the payment
request.

12. The method according to claim 10, wherein the determining the risk control result based
on the first risk level and the second risk level comprises:

if the first risk level is higher than the second risk level, using the first risk level as the risk
25 control result;

if the first risk level is lower than the second risk level, using the second risk level as the risk
control result; or

if the first risk level is equal to the second risk level, using the first risk level or the second
risk level as the risk control result.

30 13. The method according to claim 8, wherein the determining a payment result
corresponding to the payment request based on the risk control result comprises any one of the

following:

if a risk level corresponding to the risk control result is higher than or equal to a first preset risk level, the payment result is a payment failure;

5 if a risk level corresponding to the risk control result is lower than or equal to a second preset risk level, performing a payment procedure to obtain the payment result; or

if a risk level corresponding to the risk control result is lower than the first preset risk level and higher than the second preset risk level, sending an identity verification instruction to the intermediate service system, receiving, from the intermediate service system, identity verification information collected by the merchant system through an identity verification page, and
10 determining the payment result based on the identity verification information.

14. The method according to claim 8, wherein the device information comprises at least one of the following:

a hardware parameter of the terminal device;

a software parameter of the terminal device;

15 a network parameter of the terminal device; and

a behavior feature of a current user of the terminal device.

15. A payment method, applied to a merchant system, wherein the method comprises:

when a terminal device displays an interaction page of the merchant system, collecting device information of the terminal device;

20 in response to detecting that a target account initiates a payment operation for a target transaction on an interaction page of the merchant system, sending a payment request and the device information to an intermediate service system, wherein the device information is used by a wallet system for a risk control procedure of the payment request, and the intermediate service system is configured to provide an intermediate service between the merchant system and the
25 wallet system; and

receiving a payment result corresponding to the payment request from the intermediate service system, and displaying the payment result on an interaction page of the merchant system, wherein

in a process of performing the payment method by the merchant system, the terminal device
30 does not jump to an interaction page of the wallet system.

16. An intermediate service system, configured to provide an intermediate service between a

merchant system and a wallet system, and comprising:

at least one storage medium that stores at least one instruction set used to make a payment;
and

at least one processor that is communicatively connected to the at least one storage medium,
5 wherein the at least one processor reads the at least one instruction set when running, and performs
a payment method based on an indication of the at least one instruction set, and the payment
method comprises:

when a terminal device displays an interaction page of the merchant system, receiving device
information and a payment request from the merchant system, wherein the device information is
10 collected by the merchant system from the terminal device, and the payment request represents
that a target account requests to make a payment in the merchant system by using the wallet system;

sending the payment request and the device information to the wallet system, wherein the
device information is used by the wallet system for a risk control procedure of the payment request;

receiving a payment result corresponding to the payment request from the wallet system; and

15 sending the payment result to the merchant system, so that the merchant system displays the
payment result on an interaction page of the merchant system, wherein

in a process of performing the payment method by the intermediate service system, the
terminal device does not jump to an interaction page of the wallet system.

17. The intermediate service system according to claim 16, wherein before the payment result
20 is received, the at least one processor further performs the following step:

sending risk control advice information to the wallet system, wherein the risk control advice
information is used by the wallet system for the risk control procedure of the payment request.

18. A wallet system, comprising:

at least one storage medium that stores at least one instruction set used to make a payment;
25 and

at least one processor that is 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
a payment method based on an indication of the at least one instruction set, and the payment
method comprises:

30 when a terminal device displays an interaction page of a merchant system and a target account
initiates a payment operation for a target transaction on an interaction page of the merchant system,

receiving a payment request and device information from an intermediate service system, wherein the device information is collected by the merchant system from the terminal device, and the intermediate service system provides an intermediate service between the merchant system and the wallet system;

5 performing a risk control procedure on the payment request based on the device information, to obtain a risk control result;

determining a payment result corresponding to the payment request based on the risk control result; and

10 sending the payment result to the intermediate service system, so that the payment result is displayed on an interaction page of the merchant system, wherein

in a process of performing the payment method by the wallet system, the terminal device does not jump to an interaction page of the wallet system.

19. A merchant system, comprising:

at least one storage medium that stores at least one instruction set used to make a payment;

15 and

at least one processor that is 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 a payment method based on an indication of the at least one instruction set, and the payment method comprises:

20 when a terminal device displays an interaction page of the merchant system, collecting device information of the terminal device;

in response to detecting that a target account initiates a payment operation for a target transaction on an interaction page of the merchant system, sending a payment request and the device information to an intermediate service system, wherein the device information is used by a wallet system for a risk control procedure of the payment request, and the intermediate service system is configured to provide an intermediate service between the merchant system and the wallet system; and

25 receiving a payment result corresponding to the payment request from the intermediate service system, and displaying the payment result on an interaction page of the merchant system, wherein

in a process of performing the payment method by the merchant system, the terminal device

does not jump to an interaction page of the wallet system.

20. A computer-readable non-transitory storage medium, wherein the computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the method according to any one of claims 1 to 15 is implemented.

5