

RISK PAYMENT PROCESSING METHOD AND APPARATUS, AND DEVICE

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to methods, apparatuses, and devices for processing risky payments.

BACKGROUND

[0002] With the development of Internet technologies, people are increasingly using various network-based services, and also increasingly using mobile payment means to perform payments, such as various electronic wallets. Online shopping transaction platforms can access electronic wallets provided by various service parties, and when a user needs to perform a payment, the user can select one electronic wallet thereof to perform the payment as required. However, such a payment processing manner may have a risk. With a possible risk, how to ensure the security without affecting payment experience of the user becomes a technical problem that needs to be resolved urgently.

SUMMARY

[0003] To overcome problems existing in the related art, this specification provides a method and apparatus, and a device for processing risky payments.

[0004] According to a first aspect of the embodiments of this specification, a method for processing risky payments is provided, which includes:

[0005] receiving a payment request, where the payment request indicates that a protocol payment is performed for a current payment using a third-party payment account;

[0006] initiating, if it is determined that the third-party payment account has a risk, a security verification request to a third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment; and

[0007] obtaining a security verification result from the third-party payment service party and executing a payment process according to the security verification result.

[0008] Optionally, the method further includes:

[0009] executing a protocol payment procedure to complete the payment process if it is determined that the third-party payment account has no risk.

[0010] Optionally, the security verification request carries payment information of the current payment, for the third-party payment service party to trigger a deduction procedure using the

payment information after it is determined that the third-party payment account has no risk.

[0011] Optionally, the executing a payment process according to the security verification result includes:

[0012] prohibiting the current payment if the security verification result indicates that the security verification for the current payment fails.

[0013] Optionally, the initiating a security verification request to a third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment includes:

[0014] invoking a security verification interface provided by the third-party payment service party, obtaining page link information of the third-party payment service party, and accessing a security verification page of the third-party payment service party according to the page link information, for the third-party payment service party to execute the security verification for the current payment through the security verification page.

[0015] Optionally, the initiating a security verification request to a third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment includes:

[0016] triggering to start a third-party payment application, for the third-party payment application to jump to a security verification page and to execute the security verification for the current payment through the security verification page.

[0017] According to a second aspect of the embodiments of this specification, a method for processing risky payments is provided, which includes:

[0018] receiving a security verification request sent from a transaction platform side for a current payment, where the security verification request is initiated by the transaction platform side after a user performs a protocol payment using a third-party payment account and determines that the third-party payment account has a risk;

[0019] executing a security verification procedure for the current payment; and

[0020] determining a verification result after execution of the security verification procedure and sending the verification result to the transaction platform side.

[0021] According to a third aspect of the embodiments of this specification, an apparatus for processing risky payments is provided, which includes:

[0022] a receiving module, configured to receive a payment request, where the payment request indicates that a protocol payment is performed for a current payment using a third-party payment account;

[0023] a security verification module, configured to initiate, if it is determined that the third-

party payment account has a risk, a security verification request to a third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment; and

[0024] a payment processing module, configured to obtain a security verification result from the third-party payment service party and execute a payment process according to the security verification result.

[0025] Optionally, the payment processing module is further configured to:

[0026] execute a protocol payment procedure to complete the payment process if it is determined that the third-party payment account has no risk.

[0027] Optionally, the security verification request carries payment information of the current payment, for the third-party payment service party to trigger a deduction procedure using the payment information after it is determined that the third-party payment account has no risk.

[0028] Optionally, the payment processing module is further configured to:

[0029] prohibit the current payment if the security verification result indicates that the security verification for the current payment fails.

[0030] Optionally, the security verification module is further configured to:

[0031] invoke a security verification interface provided by the third-party payment service party, obtain page link information of the third-party payment service party, and access a security verification page of the third-party payment service party according to the page link information, for the third-party payment service party to execute the security verification for the current payment through the security verification page.

[0032] Optionally, the security verification module is further configured to:

[0033] trigger to start a third-party payment application, for the third-party payment application to jump to a security verification page and to execute the security verification for the current payment through the security verification page.

[0034] According to a fourth aspect of the embodiments of this specification, an apparatus for processing risky payments is provided, which includes:

[0035] a receiving module, configured to receive a security verification request sent from a transaction platform side for a current payment, where the security verification request is initiated by the transaction platform side after a user performs a protocol payment using a third-party payment account and determines that the third-party payment account has a risk;

[0036] a security verification module, configured to execute a security verification procedure for the current payment; and

[0037] a sending module, configured to determine a verification result after execution of the

security verification procedure and send the verification result to the transaction platform side.

[0038] According to a fifth aspect of the embodiments of this specification, a computer device is provided, which includes a memory, a processor, and a computer program stored in the memory and executable on the processor, where the processor executes the program to implement the embodiment of the method for processing risky payments.

[0039] The technical solutions provided in the embodiments of this specification may include the following beneficial effects.

[0040] In the embodiments of this specification, if a transaction platform side detects that a third-party payment account has a risk, a security verification request can be initiated to a third-party payment service party to trigger the third-party payment service party to execute a security verification for the current payment. In this embodiment, a theft risk can be eliminated in the payment process by introducing an identity verification capability of a third-party payment service side. On one hand, the payment security can be ensured, and on the other hand, payment experience of a user can be ensured, and a payment success rate is improved.

[0041] It should be understood that the foregoing general description and detailed description in the following are merely exemplary and interpretive, but cannot constitute a limitation to this specification.

BRIEF DESCRIPTION OF THE DRAWINGS

[0042] The accompanying drawings herein, which are incorporated into the specification and constitute a part of this specification, illustrate embodiments consistent with this specification and, together with this specification, serve to explain the principles of this specification.

[0043] FIG. 1A is a flowchart of a method for processing risky payments according to an exemplary embodiment of this specification.

[0044] FIG. 1B is a flowchart of another method for processing risky payments according to an exemplary embodiment of this specification.

[0045] FIG. 2A is a flowchart of another method for processing risky payments according to an exemplary embodiment of this specification.

[0046] FIG. 2B is a schematic diagram of application pages according to an exemplary embodiment of this specification.

[0047] FIG. 3 is a block diagram of a device in which an apparatus for processing risky payments is disposed according to an exemplary embodiment of this specification is located.

[0048] FIG. 4 is a block diagram of an apparatus for processing risky payments according to

an exemplary embodiment of this specification.

[0049] FIG. 5 is a block diagram of another apparatus for processing risky payments according to an exemplary embodiment of this specification.

DETAILED DESCRIPTION

[0050] Exemplary embodiments are described in detail herein, and examples of the exemplary embodiments are shown in the accompanying drawings. When the following description involves the accompanying drawings, unless otherwise indicated, the same numerals in different accompanying drawings represent the same or similar elements. Implementations described in the following exemplary embodiments do not represent all implementations consistent with this specification. On the contrary, the implementations are merely examples of an apparatus and a method that are consistent with some aspects of this specification described in detail in claims.

[0051] The terms used in this specification are merely for the purpose of illustrating specific embodiments, and are not intended to limit this specification. The terms “a,” “said,” and “the” of singular forms used in this specification and the appended claims are also intended to include plural forms, unless otherwise specified in the context clearly. It should be further understood that the term “and/or” used herein indicates and includes any or all possible combinations of one or more associated listed items.

[0052] It should be understood that although the terms such as “first,” “second,” and “third,” may be used in this specification to describe various information, the information should not be limited to these terms. These terms are merely used to distinguish between information of the same type. For example, without departing from the scope of this specification, the first information may also be referred to as the second information, and similarly, the second information may also be referred to as the first information. Depending on the context, for example, the word “if” used herein may be interpreted as “while” or “when,” or “in response to determination.”

[0053] In an e-commerce payment scenario, generally, an e-commerce transaction platform can introduce other third-party electronic wallets to enrich payment channels of a user. Therefore, when the user uses a transaction service of the e-commerce transaction platform, the user may select to use a third-party electronic wallet to perform the payment. To improve user experience, some network service-based transaction platforms introduce a withhold service (also referred to as a protocol payment), in which the user needs to bind a third-party

electronic wallet account and a transaction platform account and signs a withhold agreement. When the user purchases a product or a service of the transaction platform, the transaction platform directly initiates a deduction request to the third-party electronic wallet to perform purchase bookkeeping, and the user does not need to input a password, thereby improving the user experience. For example, a transaction platform of an e-commerce company Lazada can access a Malaysian TnG wallet. Lazada and TnG may use a form of a protocol payment. The transaction platform may directly initiate a deduction request to the TnG wallet, and the TnG wallet may directly perform a deduction operation on a user account according to the deduction request without a payment verification operation such as a payment password verification performed by the user during the payment.

[0054] In a payment scenario, a transaction platform is generally configured with a risk decision-making system, to determine whether the current payment has a risk. Since the verification on a payment password is not performed in the protocol payment scenario and a third-party electronic wallet is involved, if the transaction platform detects that the third-party electronic wallet has a risk, the transaction platform can directly intercept the payment to ensure the security. However, this manner affects payment experience of the user and may lead to loss of users. The transaction platform may also enable the current payment to pass the risk decision-making for the sake of payment experience. However, this manner introduces a certain risk and an actual risky payment may be allowed, bringing losses to the platform or the user.

[0055] Based on this, an embodiment of this specification provides a method for processing risky payments. On one hand, the payment security can be ensured, and on the other hand, payment experience of the user can be ensured, and a payment success rate is improved. The solution for processing risky payments relates to a processing method on a transaction platform side, and also relates to a processing method on a third-party payment product (that is, a third-party electronic wallet) side.

[0056] The method for processing risky payments is first described from the transaction platform side. FIG. 1A is a flowchart of a method for processing risky payments (e.g., payments have risks) according to an exemplary embodiment of this specification, and the method includes the following steps.

[0057] Step 102: Receiving a payment request, where the payment request indicates that a protocol payment is performed for a current payment using a third-party payment account.

[0058] Step 104: Initiating, if it is determined that the third-party payment account has a risk, a security verification request to a third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment.

[0059] Step 106: Obtaining a security verification result from the third-party payment service party and executing a payment process according to the security verification result.

[0060] In this embodiment, the user may register a transaction account on the transaction platform side, and obtain, by using the transaction account, a transaction service provided by the transaction platform party. In addition, the user also registers an account (referred to as a third-party payment account in this embodiment) on the third-party payment service party side, and obtains, by using the account, a payment service provided by the third-party payment service party. There is a cooperation relationship between the transaction platform party and the third-party payment service party. A third-party payment wallet provided by the third-party payment service party can access transaction products of the transaction platform party. When the user uses products on the transaction platform side and needs to perform a payment, the user may select to use the third-party payment product to perform a payment operation. The third-party payment service party in this embodiment may use a protocol payment manner. Therefore, the user does not need to perform a payment verification such as a password or a biometric feature recognition on the third-party payment service party side during the payment.

[0061] In an actual application, the transaction platform party can receive a payment request in a plurality of manners. For example, the user may obtain a transaction service by using a client that is provided by the transaction platform party, and the client provides a transaction function and a payment function. In an example, the client may provide a selection entry for payment manners. When the user performs the payment, the selection entry can be provided for the user to select to trigger one payment manner, and the client obtains a trigger operation of the user to determine the payment manner selected by the user. According to the trigger operation, it may be determined that the user selects a third-party payment manner with which the protocol payment is signed in advance, and the client may enable the payment request to carry information indicating that the protocol payment is performed for the current payment by using a third-party payment account, so that the transaction platform party can perform risk decision-making for the current payment after receiving the payment request.

[0062] In some other examples, the transaction platform may provide a website, and the user may log onto a service page provided by the transaction platform by using a browser. Similarly, the service page provides a transaction function and a payment function. When the user performs a payment, the service page may be provided for the user to select to trigger one of payment manners. The payment manner selected by the user is further determined by obtaining a trigger operation of the user. According to the trigger operation, it is determined that the user selects a third-party payment manner with which a protocol payment is signed in advance, and

the service page may enable the payment request to carry information indicating that the protocol payment is performed for the current payment using a third-party payment account, so that the transaction platform party can perform risk decision-making for the current payment. In an actual application, the payment request may further carry other customized information such as transaction order related information, a transaction amount, or a transaction time, which is not limited in this embodiment.

[0063] The transaction platform side may be configured with a risk control system to determine, when the user initiates a payment, whether the current payment has a risk. There may be a plurality of types of payment risks. For example, an account of the user on the transaction platform side is stolen, and in this case, the transaction platform party may execute a security verification on the user account. In an actual application, the payment risk may alternatively be that an account of the user on a third-party payment side is stolen, and in this case, the third-party payment service party performs a security verification on the user account in this embodiment.

[0064] Specifically, there may be a plurality of risk types recognizable to the risk control system. In the payment scenario of this embodiment, two accounts of the user are involved: the transaction account on the transaction platform side and the payment account on the third-party payment side. A risk may be that the transaction account of the user on the transaction platform side is stolen, and a thief may log onto the transaction platform using the transaction account and perform a payment using the payment account associated with the transaction account. In this case, since the transaction account on the transaction platform side is involved, the transaction platform may execute a risk control and security verification on the transaction account. However, the risk may alternatively be that the payment account of the user on the third-party payment side is stolen, and the transaction platform has limited manners to execute the risk control and security verification for the third-party payment account. Therefore, in the solution of this embodiment, the transaction platform party may request the third-party payment service party to execute a security verification for the current payment behavior of the third-party payment account.

[0065] A risk determination procedure of the risk control system is not limited in this embodiment. In an example, the risk control system may determine whether the third-party payment account is at a risk of being stolen in combination with a plurality of factors. For example, the risk control system may determine whether the third-party payment account is at the risk of being stolen according to historical features such as a usual address, historical payment amounts, or historical payment frequency of the user in combination with addresses,

amounts, and frequency of the latest N payments.

[0066] If it is determined that the third-party payment account has no risk, the transaction platform side may execute a protocol payment procedure to complete the current payment process. If it is determined that the third-party payment account has a risk, since an account of another service party is involved, to ensure the security, the transaction platform may inform the third-party payment service party and initiate a security verification request to the third-party payment service party, to trigger the third-party payment service party to execute the security verification for the current payment.

[0067] Optionally, the transaction platform party and the third-party payment service party may agree on invoking an interface. After the transaction platform party detects that the third-party payment account is at the risk of being stolen, the transaction platform party may invoke the interface to inform the third-party payment service party and initiate a security verification request to the third-party payment service party. The third-party payment service party executes a security verification procedure after receiving the security verification request.

[0068] Since the user performs a transaction payment when using a product on the transaction platform side, to ensure the fluency of user operations and reduce operation complexity, an optional manner is to perform the security verification in the product of the transaction platform side currently used by the user. Based on this, this embodiment provides an optional implementation that can directly display a security verification page of the third-party payment service party in the product of the transaction platform side. The transaction platform side may obtain page link information of the third-party payment service party, and the page link information may include a page address or a uniform resource locator (URL) of the security verification page of the third-party payment service party. The URL address may be returned by the third-party payment service party to the transaction platform side after the interface is invoked, or may be provided to the transaction platform side by the third-party payment service party in advance. According to the information, the security verification page of the third-party payment service party may be directly accessed in the transaction platform, for the third-party payment service party to execute the security verification for the current payment through the security verification page. Optionally, the security verification page may be a page that conforms to implementation of HTML5 standards. In this embodiment, since the security verification page of the third-party payment service party may be directly displayed in the product of the transaction platform side, the user can perform a security verification conveniently, and this solution can improve user experience and improve payment processing efficiency.

[0069] In some other examples, an application provided by the transaction platform and a payment application provided by the third-party payment side may be installed in a user equipment at the same time, or it is also possible to directly jump to a security verification page of a third-party payment application. The third-party payment application may be triggered for the third-party payment application to directly jump to the security verification page, to start to execute the security verification for the current payment through the security verification page.

[0070] The third-party payment service party may implement security verification in a plurality of manners. In an example, the security verification may be implemented in a manner of verifying a payment password, and a payment password entry interface may be provided in the security verification page, for the user to enter a payment password to complete the verification. In some other examples, the verification may be implemented by using a message one-time password (OTP). Alternatively, the security verification may be performed through a biological feature recognition, for example, recognizing a fingerprint or a face of the user. This is not limited in this embodiment.

[0071] In this embodiment, to improve payment processing efficiency, when the transaction platform side invokes the interface to initiate a security verification request, the security verification request may carry payment information of the current payment. The payment information may include various types of information such as a user account, order-related information, a payment amount, and a payment address, for the third-party payment service party to trigger a deduction procedure using the payment information after it is determined that the third-party payment account has no risk. In a case that security verification is required, in this embodiment, the payment information is added to the security verification request, for the third-party payment service party to trigger a deduction in time in a case that the verification succeeds, thereby improving payment processing efficiency and reducing a payment processing time.

[0072] The method for processing risky payments is then described from a third-party payment product side. FIG. 1B is a flowchart of a method for processing risky payments according to another exemplary embodiment of this specification, and the method includes the following steps.

[0073] Step 112: Receiving a security verification request sent from a transaction platform side for a current payment, where the security verification request is initiated by the transaction platform side after a user performs a protocol payment using a third-party payment account and determines that the third-party payment account has a risk.

[0074] Step 114: Executing a security verification procedure for the current payment.

[0075] Step 116: Determining a verification result after execution of the security verification procedure and sending the verification result to the transaction platform side.

[0076] This embodiment describes the procedure for processing risky payments from the third-party payment product side. Corresponding to the foregoing embodiment, after the security verification request initiated by the transaction platform side is received, a security verification procedure may be executed for the current payment. In an example, security verification may be implemented in a manner of verifying a payment password, and a payment password entry interface may be provided in the security verification page, for the user to enter a payment password to complete the verification. In some other examples, verification may be implemented by using a message OTP. Alternatively, security verification may be performed through a biological feature recognition, for example, recognizing a fingerprint or a face of the user. This is not limited in this embodiment. After the execution of the payment verification procedure, a verification result is determined, and the verification result is sent to the transaction platform side, for the transaction platform side to execute a subsequent payment process.

[0077] The following describes a solution for processing risky payments of this specification by using an embodiment. As shown in FIG. 2A, the solution of this embodiment involves an e-commerce transaction platform Lazada, a payment processing system ECPay configured by the transaction platform side, and a product on the third-party payment side including a TnG wallet. The Lazada may sign a protocol payment with the TnG wallet, that is, the Lazada directly initiates a deduction request to the TnG, and the TnG directly executes a deduction operation according to the deduction request, while a payment verification operation such as entering a password by the user is not required during the deduction. Such a protocol payment does not require the TnG on the third-party payment side to execute the payment verification. This embodiment provides a payment processing solution that ensures the payment security in a case that a risky transaction occurs.

[0078] In this embodiment, the transaction platform Lazada processes payment matters of the user using the ECPay payment system. After the user trades on the transaction platform side and initiates a payment request, the ECPay payment system invokes an ECPay risk control system to perform risk decision-making. If the ECPay risk control system detects that the current payment is secure, a decision for a protocol payment is outputted, and the ECPay payment system triggers a protocol payment procedure to complete the current payment process. If the ECPay risk control system detects that a TnG account is at a risk of being stolen, a decision for a security verification is outputted.

[0079] After receiving the decision for a security verification, in a manner of jumping to a payment verification, the ECPay payment system may request the TnG to perform a security verification for the current payment. Optionally, the Lazada side may invoke a security verification interface provided by the TnG side, to directly jump to a security verification page on the TnG side from a product on the Lazada side. FIG. 2B is a schematic diagram of a security verification page according to an exemplary embodiment of this specification. In this page, the user may enter a payment password or a message OTP, for the TnG wallet to execute a security verification, and if the security verification succeeds, the TnG wallet executes a deduction procedure, and the payment for a Lazada order succeeds. If the security verification fails, the TnG wallet informs the Lazada side of the verification failure, and the payment for the order on the Lazada side fails.

[0080] In this embodiment, when payment is performed by using the TnG wallet in an e-commerce scenario, if a conventional solution supports the protocol payment, after detecting that the third-party payment account is at the risk of being stolen, the ECPay system generally intercepts the transaction or allows the transaction. After the decision of jumping to a payment verification of this embodiment is introduced, an identity verification capability of the TnG may be used to eliminate a theft risk of the TnG. A payment success rate of the Lazada orders and payment experience of the user are both greatly increased. Generally, a plurality of third-party payment products are provided in the e-commerce scenario, and a theft risk can be eliminated by using the identity verification capability of the third-party payment service party in the solution of this embodiment. Payment experience of the user can be improved and a payment success rate is improved while the risk is controllable.

[0081] Corresponding to the embodiment of the foregoing method for processing risky payments, this specification further provides embodiments of an apparatus for processing risky payments and a terminal to which the apparatus is applied.

[0082] The embodiment of the apparatus for processing risky payments in this specification may be applied to a computer device, such as a server or a terminal device. The device embodiments may be implemented by using software, hardware, or in a manner of a combination of software and hardware. Taking software implementation as an example, an apparatus in a logical aspect is formed by reading corresponding computer program instructions in a nonvolatile memory into an internal memory for execution by a file processing processor in which the apparatus resides. On a hardware level, as shown in FIG. 3, which is a hardware structural diagram of a computer device in which an apparatus for processing risky payments according to this specification is located, in addition to a processor 310, a memory

330, a network interface 320, and a nonvolatile memory 340 shown in FIG. 3, the server or the electronic device in which the apparatus 331 is located in this embodiment may usually further include other hardware according to actual functions of the computer device. Details are not described herein.

[0083] As shown in FIG. 4, FIG. 4 is a block diagram of an apparatus for processing risky payments according to an exemplary embodiment of this specification, and the apparatus includes:

[0084] a receiving module 41, configured to receive a payment request, where the payment request indicates that a protocol payment is performed for a current payment using a third-party payment account;

[0085] a security verification module 42, configured to initiate, if it is determined that the third-party payment account has a risk, a security verification request to a third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment; and

[0086] a payment processing module 43, configured to obtain a security verification result from the third-party payment service party and execute a payment process according to the security verification result.

[0087] Optionally, the payment processing module is further configured to:

[0088] execute a protocol payment procedure to complete the current payment process if it is determined that the third-party payment account has no risk.

[0089] Optionally, the security verification request carries payment information of the current payment, for the third-party payment service party to trigger a deduction procedure using the payment information after it is determined that the third-party payment account has no risk.

[0090] Optionally, the payment processing module is further configured to:

[0091] prohibit the current payment if the security verification result indicates that the security verification for the current payment fails.

[0092] Optionally, the security verification module is further configured to:

[0093] invoke a security verification interface provided by the third-party payment service party, obtain page link information of the third-party payment service party, and access a security verification page of the third-party payment service party according to the page link information, for the third-party payment service party to execute a security verification for the current payment through the security verification page.

[0094] Optionally, the security verification module is further configured to:

[0095] trigger to start a third-party payment application, for the third-party payment

application to jump to a security verification page and to execute the security verification for the current payment through the security verification page.

[0096] As shown in FIG. 5, FIG. 5 is a block diagram of an apparatus for processing risky payments according to an exemplary embodiment of this specification, and the apparatus includes:

[0097] a receiving module 51, configured to receive a security verification request sent from a transaction platform side for a current payment, where the security verification request is initiated by the transaction platform side after a user performs a protocol payment using a third-party payment account and determines that the third-party payment account has a risk;

[0098] a security verification module 52, configured to execute a security verification procedure; and

[0099] a sending module 53, configured to determine a verification result after execution of the security verification procedure and send the verification result to the transaction platform side.

[00100] Correspondingly, this specification further provides a computer device, including a memory, a processor, and a computer program stored in the memory and executable on the processor, where the processor executes the program to implement the embodiment of the method for processing risky payments.

[00101] For details about the implementation processes of the functions and effects of the modules in the foregoing apparatus for processing risky payments, refer to the implementation processes of the corresponding steps in the foregoing method for processing risky payments. Details are not described herein again.

[00102] Because the apparatus embodiments basically correspond to the method embodiments, for related parts, reference may be made to the descriptions in the method embodiments. The described apparatus embodiment is merely an example. The modules described as separate parts may or may not be physically separated, and parts displayed as modules may or may not be physical modules. They may be located in one position, or may be distributed on a plurality of network modules. Some or all of the modules may be selected according to actual requirements to achieve the objectives of the solutions of the present specification. A person of ordinary skill in the art may understand and implement the embodiments without creative efforts.

[00103] Embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some embodiments, the actions or steps recorded in the claims may be performed in sequences different from those in the embodiments, and an

expected result may still be achieved. In addition, the processes depicted in the accompanying drawings are not necessarily performed in the specific order or successively to achieve an expected result. In some implementations, multitasking and parallel processing may be feasible or beneficial.

[00104] After considering this specification and practicing this application, a person of ordinary skill in the art can easily conceive other implementations of this specification. This specification is intended to cover any variation, use, or adaptive change of this specification following the general principles thereof, and include well-known knowledge and conventional technical means in the technical field that are not disclosed in this specification. It is intended that this specification and embodiments be considered as exemplary only. A true scope and spirit of this specification are indicated by the following claims.

[00105] It will be appreciated that this specification is not limited to the exact construction that has been described above and illustrated in the accompanying drawings, and that various modifications and changes can be made without departing from the scope thereof. It is intended that the scope of this specification only be limited by the appended claims.

[00106] The foregoing descriptions are merely exemplary embodiments of this specification, but are not intended to limit this specification. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of this specification shall fall within the protection scope of this specification.

CLAIMS

What is claimed is:

1. A method for processing risky payments, comprising:
 - receiving, by a transaction platform, a payment request, wherein the payment request indicates that a protocol payment is requested for a current payment using a third-party payment account that is associated with a third-party payment service party;
 - determining, by the transaction platform, whether the third-party payment account has a risk according to the payment request; and
 - in response to determining that the third-party payment account has no risk, executing, by the transaction platform, a protocol payment procedure for the current payment, and
 - in response to determining that the third-party payment account has a risk:
 - initiating, by the transaction platform, a security verification request to the third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment to generate a security verification result indicating whether the third-party payment account has a risk;
 - obtaining, by the transaction platform, the security verification result from the third-party payment service party; and in response to the security verification result indicating that the third-party payment account has no risk, executing, by the transaction platform, the protocol payment procedure for the current payment, and
 - in response to the security verification result indicating that the third-party payment account has a risk, prohibiting, by the transaction platform, the protocol payment procedure to be executed.
2. The method according to claim 1, wherein the security verification request carries payment information of the current payment, and
 - wherein in response to the security verification result indicating that the third-party payment account has no risk, executing, by the transaction platform, the protocol payment procedure for the current payment comprises: triggering the third-party payment service party to perform a deduction procedure using the payment information.
3. The method according to claim 1, wherein in response to determining that the third-party payment account has a risk, the initiating, by the transaction platform, a security

verification request to a third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment to generate a security verification result indicating that the third-party payment account has a risk comprises:

invoking, by the transaction platform, a security verification interface provided by the third-party payment service party, obtaining page link information of the third-party payment service party, and accessing a security verification page of the third-party payment service party according to the page link information, for the third-party payment service party to execute the security verification for the current payment through the security verification page.

4. The method according to claim 1, wherein in response to determining that the third-party payment account has a risk, the initiating, by the transaction platform, a security verification request to a third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment to generate a security verification result indicating that the third-party payment account has a risk comprises:

triggering, by the transaction platform, a third-party payment application, for the third-party payment application to jump to a security verification page and to execute the security verification for the current payment through the security verification page.

5. The method according to claim 1, further comprising:

in response to determining that the third-party payment account has a risk, receiving, by the third-party payment service party, the security verification request sent from the transaction platform side for the current payment, wherein the security verification request is initiated by the transaction platform side after the user requesting the protocol payment for the current payment using the third-party payment account;

executing, by the third-party payment service party, the security verification procedure for the current payment; and

generating, by the third-party payment service party, the verification result after execution of the security verification procedure, and sending the verification result to the transaction platform side.

6. An apparatus for processing risky payments, comprising:

a receiving module, configured to receive a payment request, wherein the payment request indicates that a protocol payment is requested for a current payment using a third-party payment account that is associated with a third-party payment service party;

a security verification module, configured to:

- determine whether the third-party payment account has a risk according to the payment request; and

- in response to determining that the third-party payment account has no risk, execute a protocol payment procedure for the current payment, and

- in response to determining that the third-party payment account has a risk:

- initiate a security verification request to the third-party payment service party, to trigger the third-party payment service party to execute a security verification for the current payment to generate a security verification result indicating whether the third-party payment account has a risk; and

a payment processing module, configured to:

- obtain the security verification result from the third-party payment service party; and

- in response to the security verification result indicating that the third-party payment account has no risk, execute the protocol payment procedure for the current payment, and

- in response to the security verification result indicating that the third-party payment account has a risk, prohibit the protocol payment procedure to be executed.

7. A computer device, comprising a memory, a processor, and a computer program stored in the memory and executable on the processor, wherein the processor executes the program to implement the method according to any one of claims 1 to 5.