# RISKY MERCHANT IDENTIFICATION METHOD, ACQUIRING SYSTEM, AND STORAGE MEDIUM

## TECHNICAL FIELD

**[0001]** This specification relates to the field of Internet technologies, and in particular, to a risky merchant identification method, an acquiring system, and a storage medium.

## BACKGROUND

**[0002]** With the development of Internet technologies, electronic payments are widely applied. For example, transactions between users and merchants can be paid by using an electronic payment method, bringing convenience to the users and the merchants. In addition, there are some unauthorized persons in a network. They use the convenience of electronic payments to conduct illegal transactions and illegal fund transfers in the network. For example, a network gambling group can direct users to pay specified merchants, to collect gambling funds.

**[0003]** To improve transaction concealment, the unauthorized persons usually conduct services by using shells, to avoid check by a risk control party. For example, the unauthorized persons embed websites of illegal merchants into websites of compliant merchants. This is equivalent to putting shells of the compliant merchants on the illegal merchants. When performing risk scanning on merchants, the risk control party can obtain only the compliant merchants through scanning, and cannot obtain the illegal merchants through scanning, which brings some difficulties to risk identification of the merchants. Therefore, there is a need for a solution that can accurately identify a merchant with a shell service conduction risk.

**[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 risky merchant identification method, an acquiring system,

and a storage medium, to accurately identify a merchant with a shell service conduction risk in a transaction payment process.

**[0006]** According to a first aspect, this specification provides a risky merchant identification method, applied to an acquiring system. The acquiring system provides an acquiring service to a target merchant through a checkout counter. The method includes: receiving a payment request corresponding to a target transaction, where the target transaction is a transaction between a target user and the target merchant, and the payment request is a request triggered by a payment operation performed by the target user on a first merchant page integrated with the checkout counter by using a terminal device; obtaining a page web address of a second merchant page from the payment request, where the second merchant page is a previous hop of page of the first merchant page; and determining, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant.

**[0007]** According to a second aspect, this specification further provides an acquiring system. The acquiring system provides an acquiring service to a target merchant through a checkout counter. The acquiring system includes: at least one storage medium that stores at least one instruction set for identifying a risky merchant; and at least one processor that is communicatively connected to the at least one storage medium. When the risky merchant identification system runs, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set: receiving a payment request corresponding to a target transaction, where the target transaction is a transaction between a target user and the target merchant, and the payment request is a request triggered by a payment operation performed by the target user on a first merchant page integrated with the checkout counter by using a terminal device; obtaining a page web address of a second merchant page from the payment request, where the second merchant page is a previous hop of page of the first merchant page; and determining, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant.

**[0008]** According to a third aspect, this specification further provides a computer-readable nonvolatile storage medium. The computer-readable nonvolatile storage medium stores at least one instruction set, and the at least one instruction set is executed by at least one processor to implement the method according to any implementation of the first aspect.

**[0009]** Other functions of the risky merchant identification method provided in this

specification are partially listed in the following descriptions. Creative aspects of the risky merchant identification method 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

**[0010]** To describe the technical solutions in the embodiments of this specification more clearly, the following briefly describes the accompanying drawings required for describing the embodiments. Clearly, the accompanying drawings in the following description show merely some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

**[0011]** FIG. 1 is a schematic diagram of a payment scenario according to an embodiment of this specification;

**[0012]** FIG. 2 is a schematic diagram of conducting a service through illegal web address embedding in a payment scenario according to an embodiment of this specification;

**[0013]** FIG. 3 is a schematic diagram of a principle of identifying a risky merchant according to an embodiment of this specification;

**[0014]** FIG. 4 is a diagram of a hardware structure of a computing system according to an embodiment of this specification;

**[0015]** FIG. 5 is a flowchart of a risky merchant identification method according to an embodiment of this specification;

**[0016]** FIG. 6 is a flowchart of determining whether a target merchant is a risky merchant according to an embodiment of this specification; and

**[0017]** FIG. 7 is a schematic diagram of determining whether a target merchant is a risky merchant according to an embodiment of this specification.

## DESCRIPTION OF EMBODIMENTS

**[0018]** 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

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 that of the claims.

**[0019]** The terms used herein are merely intended to describe specific example embodiments, and impose no limitation. For example, unless otherwise explicitly stated in the context, the singular forms "one", "an", and "the" used herein can include plural forms. When being used in this specification, the terms "include", "comprise", and/or "have" 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.

**[0020]** 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.

**[0021]** The flowchart used in this specification shows operations implemented by a system according to some embodiments of this specification. It should be clearly understood that the operations in the flowchart 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.

**[0022]** For ease of description, the terms that appear below in this specification are first explained.

**[0023]** Term 1 is illegal web address embedding. In this specification, illegal web address embedding can also be referred to as illegal merchant embedding, or can be referred to as merchant shelling. Illegal web address embedding means that when an illegal merchant generates an illegal transaction, a transaction generated on a website of the illegal merchant is redirected to a website of a compliant merchant through page redirection, so that the transaction looks like a transaction generated on the website of the compliant merchant. The above manner implements shelling for

the illegal merchant, and is a means for avoiding risk control scanning by the illegal merchant.

**[0024]** Term 2 is web address tracking point. The web address tracking point technology (Web Analytics Tagging) is a method for collecting and analyzing behavior data of users on websites. By embedding code snippets (usually referred to as "tracking points") at specific locations on a web page, behavior of users on the web page can be obtained.

**[0025]** Term 3 is source address (referer url). The source address is also referred to as a hypertext transfer protocol (HTTP) source address, is a field in an HTTP header, is used to indicate an address of a web page on which a user stays before accessing a current web page, and uses a format of a uniform resource locator (URL).

**[0026]** An application scenario of this specification is described below.

**[0027]** The technical solutions provided in this specification are applicable to a payment scenario, that is, used in the payment scenario to identify a risky merchant. With reference to FIG. 1, a system architecture of the payment scenario is described below by using an example.

**[0028]** FIG. 1 is a schematic diagram of a payment scenario according to an embodiment of this specification. With reference to FIG. 1, the scenario can include a target user 11, a merchant system 12 of a target merchant, a wallet system 13, and an acquiring system 14. The target merchant provides a merchant or a service to the target user 11. The merchant system 12 is a system used by the target merchant to manage a transaction. The wallet system 13 can be a system that provides a service such as fund storage, payment, and transfer to the target user 11. For example, the target user 11 can select a required product or service from the merchant system 12, and specify use of the wallet system 13 to pay for the product or service. The acquiring system 14 is a system that provides an acquiring service and a settlement service to the merchant system 12. The acquiring system 14 can be connected to the wallet system 13 and the merchant system 12. The target merchant resides in the acquiring system 14. After the target user 11 places an order in the merchant system 12 and initiates a payment operation, the acquiring system 14 can receive a payment request from the merchant system 12, and forward the payment request to the wallet system 13, so that the wallet system 13 completes a payment of the transaction.

**[0029]** In the payment scenario shown in FIG. 1, some illegal merchants may conduct services by using an illegal web address embedding technology. FIG. 2 is a schematic diagram of conducting a service through illegal web address embedding in a payment scenario according to an embodiment of this specification. As shown in FIG. 2, the payment scenario includes a target

user 11, a merchant system 12 of a compliant merchant (for example, a website of the compliant merchant), a merchant system 15 of an illegal merchant (for example, a website of the illegal merchant), a wallet system 13, and an acquiring system 14. The compliant merchant is a legal registered merchant (resident merchant) of the acquiring system 14. The illegal merchant is not registered with the acquiring system 14, and is not a legal registered merchant (resident merchant) of the acquiring system 14. The merchant system 15 of the illegal merchant can be linked to the merchant system 15 of the compliant merchant through illegal web address embedding. The target user 11 can access the merchant system 15 of the illegal merchant and initiate a transaction in the merchant system 15 of the illegal merchant. When the target user 11 needs to pay the transaction, the merchant system 15 of the illegal merchant redirects to the merchant system 12 of the compliant merchant, so that the merchant system 12 of the compliant merchant initiates a payment request to the acquiring system 14. In the view of the acquiring system 14, the transaction to be paid is a transaction between the target user 11 and the compliant merchant.

**[0030]** It can be learned from FIG. 2 that shelling is usually implemented for illegal merchants through illegal web address embedding, which is equivalent to putting shells of compliant merchants on the illegal merchants, to avoid risk control scanning by the acquiring system 14. When performing risk scanning on merchants, the acquiring system 14 can obtain only the compliant merchants through scanning, and cannot obtain, through scanning, the illegal merchants embedded into the compliant merchants, which brings some difficulties to identification of the illegal merchants. In addition, the acquiring system 14 cannot obtain important information such as profile information of users, transaction behavior habits, and used devices. Therefore, a risky merchant cannot be identified by using data on a user side. This further increases a difficulty of identifying the risky merchant.

**[0031]** This specification provides a risky merchant identification method, applied to an acquiring system, to effectively identify a merchant with a shell service conduction risk. Specifically, the acquiring system can integrate a checkout counter into a first merchant page of a target merchant. If a target transaction is generated between a target user and the target merchant, in a payment process of the target transaction, the acquiring system can collect a page web address of a previous hop of page of the first merchant page through the checkout counter, and then identify, based on the page web address of the previous hop of page, whether the target merchant is a merchant with a shell service conduction risk.

**[0032]** FIG. 3 is a schematic diagram of a principle of identifying a risky merchant according to an embodiment of this specification. As shown in FIG. 3, an acquiring system 14 can include a checkout counter, a risk control module, and a payment processing module. The checkout counter can be deployed on a terminal device or a page accessed by a terminal device, and the risk control module and the payment processing module can be deployed on a server. The checkout counter can also be referred to as a client of the acquiring system 14, and the risk control module and the payment processing module can serve as serving ends of the acquiring system 14.

**[0033]** With reference to FIG. 3, the checkout counter can be integrated into a merchant system 12 of a target merchant to provide an acquiring service to the merchant system 12. In this specification, a page integrated with the checkout counter in the merchant system 12 is referred to as a first merchant page 121. In a shell service conduction scenario, a target user 11 can first access a second merchant page 151. The second merchant page 151 is a page of an illegal merchant embedded into the merchant system 12 (for example, the second merchant page 151 is a page in a merchant system 15 of an illegal merchant in FIG. 2). The target user 11 generates a target transaction on the second merchant page 151. In a payment process of the target transaction, there is redirection from the second merchant page 151 to the first merchant page 121 integrated with the checkout counter. The target user 11 can initiate a payment operation of the target transaction through the checkout counter. In response to the payment operation of the target transaction, the checkout counter generates a payment request of the target transaction. Because the checkout counter is integrated into the first merchant page 121, the checkout counter considers, by default, the target transaction as a transaction generated on the first merchant page 121, that is, merchant information in the payment request generated by the checkout counter is merchant information of a legal merchant associated with the first merchant page 121. That is, by using the above page redirection process, a transaction actually occurring on the second merchant page 151 is packaged as a transaction occurring on the first merchant page 121.

**[0034]** In the above payment process, after detecting that there is redirection from the second merchant page 151 to the first merchant page 121, the checkout counter can collect a page web address of the second merchant page 151. Further, when generating the payment request, the checkout counter can carry the page web address of the second merchant page 151 in the payment request.

**[0035]** Still with reference to FIG. 3, the risk control module can obtain the web address of the

second merchant page 151 based on the payment request of the target transaction, and determine, based on at least the web address of the second merchant page 151, whether the target merchant is a risky merchant (that is, whether the target merchant is a merchant with a shell service conduction risk). If the target merchant is a risky merchant, the risk control module can intercept the payment request of the target transaction and terminate the target transaction. If the target merchant is not a risky merchant, the risk control module in the acquiring system 14 can tell the payment processing module to continue to advance a subsequent payment procedure.

**[0036]** The acquiring system 14 can be a computing system with a specific computing capability. The acquiring system 14 can include one or more computing systems, and each computing system can be configured to perform a different function, for example, the checkout counter, the risk control module, and the payment processing module.

**[0037]** The risky merchant identification method provided in this specification can be performed by the acquiring system 14. The acquiring system 14 can store data or instructions for performing the risky merchant identification method described in this specification, and can execute or be configured to execute the data or the instructions. In some embodiments, the acquiring system 14 can include a hardware device with a data information processing function and a program required to drive the hardware device to work. The steps performed by using the acquiring system 14 mentioned in this specification can be performed by using modules such as the checkout counter, the risk control module, or the payment processing module based on content involved in the steps.

**[0038]** It should be understood that the acquiring system 14 can run on a separate server, or can run on a server group, a distributed server, a cloud server, or another device in a distributed manner.

**[0039]** It should be noted that there can be a plurality of types of illegal transaction activities conducted through shell service conduction. The gambling transaction provided above is merely a possible example. The risky merchant identification method provided in this specification can not only be applied to the gambling transaction scenario, but also be applied to other transaction activity scenarios involving the shell service conduction risk, for example, a fraudulent transaction scenario and a transaction scenario involving a prohibited item. A person skilled in the art should understand that when the risky merchant identification method provided in this specification is applied to other use scenarios, implementations and technical effects thereof are similar.

**[0040]** FIG. 4 is a diagram of a hardware structure of a computing system 200 according to an embodiment of this specification. The computing system 200 can serve as the acquiring system 14 shown in FIG. 1 to FIG. 3 to perform the risky merchant identification method described in this specification.

**[0041]** As shown in FIG. 4, the computing system 200 can include at least one storage medium 230 and at least one processor 220. In some embodiments, the computing system 200 can further include a communication port 250 and an internal communication bus 210. The computing system 200 can further include an I/O component 260.

**[0042]** The internal communication bus 210 can be connected to different system components. For example, the internal communication bus 210 can be connected to the storage medium 230, the processor 220, the communication port 250, the I/O component 260, and the like.

**[0043]** The I/O component 260 supports input/output between the computing system 200 and another component.

**[0044]** The communication port 250 is used for data communication between the computing system 200 and the outside. For example, the communication port 250 can be used for data communication between the computing system 200 and a network. The communication port 250 can be a wired communication port, or can be a wireless communication port.

**[0045]** The storage medium 230 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 232, a read-only storage medium (ROM) 234, or a random access storage medium (RAM) 236. The storage medium 230 further includes at least one instruction set stored in the data storage apparatus. The instruction set can include computer program code. The computer program code can include a program, a routine, an object, a component, a data structure, a process, a module, and the like.

**[0046]** The at least one processor 220 can be communicatively connected to the at least one storage medium 230. When the computing system 200 runs, the at least one processor 220 reads the at least one instruction set, and performs, based on an indication of the at least one instruction set, the risky merchant identification method provided in this specification. The processor 220 can perform the steps included in the risky merchant identification method. The processor 220 can be in a form of one or more processors. In some embodiments, the processor 220 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.

**[0047]** To merely describe a problem, only one processor 220 is shown in the computing system 200 in the accompanying drawings. However, it should be noted that, the computing system 200 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 220 in the computing system 200 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 220 (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 step A and step B).

**[0048]** FIG. 5 is a flowchart of a risky merchant identification method according to an embodiment of this specification. As described above, the acquiring system 14 can perform the risky merchant identification method in this specification.

**[0049]** As shown in FIG. 5, the risky merchant identification method can include the following steps.

**[0050]** S310: Receive a payment request corresponding to a target transaction, where the target transaction is a transaction between a target user and a target merchant, and the payment request is a request triggered by a payment operation performed by the target user on a first merchant page integrated with a checkout counter by using a terminal device.

**[0051]** With reference to FIG. 5, after the terminal device redirects from a second merchant page to the first merchant page, the target user can perform a payment operation on the checkout counter integrated on the first merchant page. For example, the target user can select, on the checkout counter, an electronic wallet to be used for a payment, and provide payment authorization information (for example, a payment password, a verification code, face information, and fingerprint information) of the electronic wallet. In response to the payment operation performed by the target user, the checkout counter generates the payment request corresponding to the target

transaction. The payment request can include an identifier of the target user, an identifier of the target merchant, transaction information of the target transaction, and the like. Further, the checkout counter can send the payment request to the risk control module in the acquiring system. Therefore, the acquiring system (or the risk control module in the acquiring system) can perform S310 to S330.

**[0052]** In this specification, the checkout counter can be integrated into the target merchant in a plurality of forms. In some embodiments, the checkout counter can be integrated into the target merchant in a form of a web page (WEB). When a payment for the target transaction is triggered, the terminal device invokes a checkout counter page on the first merchant page, so that the target user performs a payment operation on the checkout counter page. In some embodiments, the checkout counter can be integrated into a program of the target merchant in a form of a software development kit (SDK). When a payment for the target transaction is triggered, the program of the target merchant renders a checkout counter page on the first merchant page by invoking the SDK, so that the target user performs a payment operation on the checkout counter page.

**[0053]** S320: Obtain a page web address of the second merchant page from the payment request, where the second merchant page is a previous hop of page of the first merchant page.

**[0054]** In some implementations, the page web address of the second merchant page is collected by the checkout counter when it is detected that the terminal device redirects from the second merchant page to the first merchant page.

**[0055]** In some implementations, the checkout counter in the acquiring system can collect the page web address of the second merchant page by using a web address tracking point technology. For example, the acquiring system can preconfigure a tracking point plug-in on the checkout counter, and the tracking point plug-in is configured to obtain source information of the first merchant page from page code of the first merchant page. For a page, source information is located in an HTTP request header. When the target user redirects from the second merchant page to the first merchant page, a page browser includes the source information in the HTTP request header. The source information can be a referer field, and the referer field usually includes a referer url. Because the referer url represents an address of a page on which the user stays before accessing a current page (that is, a previous hop of page of the current page), the referer url in the source information of the first merchant page is the page web address of the second merchant page. In this specification, the referer url is also referred to as a tracking point web address.

**[0056]** In some implementations, when the checkout counter integrated into the first merchant page generates the payment request in response to the payment operation, the acquiring system can obtain the source information of the first merchant page by using the tracking point plug-in. Then, the checkout counter can integrate the source information of the first merchant page into the payment request, and transmit the payment request to the risk control module in the acquiring system, to perform risk control processing on the payment request.

**[0057]** In this embodiment, the acquiring system obtains the source information of the first merchant page through the checkout counter, and then collects the page web address of the second merchant page, to more accurately track a source of the payment request, provide data support for identifying whether the target merchant is a risky merchant, and increase a success rate of identifying the risky merchant.

**[0058]** S330: Determine, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant.

**[0059]** FIG. 6 is a flowchart of determining whether a target merchant is a risky merchant according to an embodiment of this specification.

**[0060]** In some implementations, with reference to FIG. 6, when determining whether the target merchant is a risky merchant, the acquiring system can first obtain a service conduction web address reported by the target merchant; then compare the page web address of the second merchant page with the service conduction web address, to obtain a comparison result; and if the comparison result is "consistent", determine that the target merchant is not a risky merchant. If the comparison result is "inconsistent", the acquiring system can obtain page data of the second merchant page based on the page web address of the second merchant page, and determine, based on the page data, whether the target merchant is a risky merchant.

**[0061]** In some implementations, the risky merchant can be a merchant with a shell service conduction risk. In an example, a transaction conducted through shell service conduction can include a gambling transaction, a fraudulent transaction, a prohibited product transaction, or the like.

**[0062]** The service conduction web address is a web address provided by the target merchant during registration with the acquiring system. When the page web address of the second merchant page is consistent with the service conduction web address, it indicates that the target merchant does not have a shell case, and it can be considered that the target merchant is not a risky merchant.

When the page web address of the second merchant page is inconsistent with the service conduction web address, it indicates that the target merchant may have a shell case, and further verification needs to be performed.

**[0063]** The page web address of the second merchant page is compared with the service conduction web address, and only when the comparison result is "inconsistent", it is determined, based on the page web address of the second merchant page, whether the target merchant is a risky merchant. This can rule out a risk-free merchant and improve detection accuracy; and can further decrease a quantity of times of analyzing the page web address of the second merchant page, save computing power, and improve detection efficiency.

**[0064]** In some implementations, the acquiring system can obtain the page data of the second merchant page based on the page web address of the second merchant page, and determine, based on the page data, whether the target merchant is a risky merchant.

**[0065]** For example, when the page data meets a target condition, the acquiring system can determine that the target merchant is a risky merchant. The target condition includes at least one of the following: There is a preset keyword in text content in the page data; there is a preset object or a preset keyword in image content in the page data; and there are at least some links configured to redirect to a preset risk page in link content in the page data.

**[0066]** Herein, an example in which shell service conduction is performed to execute a gambling transaction is used to further describe determining, by the acquiring system based on the page data of the second merchant page, of whether the target merchant is a risky merchant. In this case, the risky merchant is a merchant executing a gambling transaction through shell service conduction.

**[0067]** In some implementations, for the merchant executing a gambling transaction through shell service conduction, the page data of the second merchant page usually includes gambling-related information. For example, the page data of the second merchant page may include gambling-related text or image content or a link for redirecting to another gambling web page. In this case, the preset keyword can be a gambling-related geographical location, a gambling-related term, or the like. The preset object can be a gambling-related device, scenario, character, or the like.

**[0068]** The acquiring system can compare the text in the page data of the second merchant page with the preset keyword, and if it is determined that there is the preset keyword in the text

content in the page data, determine that the target merchant is a risky merchant.

**[0069]** The acquiring system can further perform content recognition on the image content in the page data of the second merchant page by using an image recognition algorithm, and if a recognition result includes the preset keyword or the preset object, determine that the target merchant is a risky merchant.

**[0070]** The acquiring system can further detect links existing in the page data of the second merchant page. For example, the acquiring system can compare these links with a link of the preset risk page, and if there is a link that matches the link of the preset risk page, determine that the target merchant is a risky merchant. Alternatively, the acquiring system can detect pages corresponding to these links, and if there is a page that meets the target condition in the pages corresponding to these links, determine that the target merchant is a risky merchant.

**[0071]** The acquiring system detects the page data of the second merchant page of the target merchant, and determines, by using the preset keyword, the preset object, and the link of the preset risk page, whether the target merchant is a risky merchant.

**[0072]** In the above solution, whether the target merchant is a risky merchant can be determined without using profile information and transaction behavior information on a user side and without depending on specific details of the transaction between the target user and the target merchant, to accurately identify a merchant with a shell service conduction risk.

**[0073]** In some implementations, due to a technical limitation, the page web address of the second merchant page possibly cannot be obtained, or whether the target merchant is a risky merchant cannot be accurately determined by using the second merchant page alone. In this case, the acquiring system can add a determining dimension of the risky merchant. That is, it is determined, based on the page web address of the second merchant page and historical transaction data of the target merchant, whether the target merchant is a risky merchant.

**[0074]** In some implementations, the acquiring system can determine a first intermediate risk identification result of the target merchant based on the page web address of the second merchant page; then, determine a second intermediate risk identification result of the target merchant based on the historical transaction data of the target merchant; and finally, determine, based on the first intermediate risk identification result and the second intermediate risk identification result, whether the target merchant is a risky merchant.

**[0075]** In some implementations, a manner in which the acquiring system determines the first

intermediate risk identification result of the target merchant based on the page web address of the second merchant page is similar to the above manner of determining, based on the page data of the second merchant page, whether the target merchant is a risky merchant. When the acquiring system determines that the target merchant is a risky merchant, it indicates that the first intermediate risk identification result represents that the target merchant is risky. When the acquiring system determines that the target merchant is not a risky merchant, it indicates that the first intermediate risk identification result indicates that the target merchant is not risky.

**[0076]** In some implementations, that the acquiring system determines a second intermediate risk identification result of the target merchant based on the historical transaction data of the target merchant includes: The acquiring system determines an abnormal transaction feature corresponding to the target merchant based on the historical transaction data, where the abnormal transaction feature represents a statistical feature of an abnormal transaction associated with the target merchant, and the abnormal transaction is a transaction that meets a preset condition in terms of at least one dimension in a transaction amount, a transaction frequency, and a transaction time period; determines a risky user aggregation feature corresponding to the target merchant based on the historical transaction data, where the risky user aggregation feature represents a statistical feature of a risky user having a transaction relationship with the target merchant; and determines the second intermediate risk identification result based on the abnormal transaction feature and the risky user aggregation feature.

**[0077]** Herein, an example in which shell service conduction is performed to execute a gambling transaction is still used to further describe determining of the second intermediate risk identification result of the target merchant by the acquiring system based on the historical transaction data of the target merchant. In this case, the risky merchant is a merchant executing a gambling transaction through shell service conduction.

**[0078]** In an example, a transaction conducted by a gambling risk merchant usually has a specific transaction statistical feature, and the transaction statistical feature can be used as an abnormal transaction feature for the acquiring system to identify the gambling risk merchant. For example, in a specific time period, the gambling risk merchant may have features such as a sudden increase in a quantity of transactions, a percentage of transactions of hundreds being greater than a first preset threshold, and a percentage of nighttime transactions being greater than a second preset threshold. When the target merchant meets any one of the above features, the acquiring

system can determine that the target merchant has an abnormal transaction feature.

**[0079]** In an example, a transaction counterpart (target user) of the gambling risk merchant has a specific aggregation feature. For example, in a specific time period, the gambling risk merchant may execute transactions with a specific quantity or a specific percentage of risky users. The risky user is a user whose gambling transaction has been confirmed by the acquiring system in a historical risk control process. When a quantity of risky users conducting transactions with the target merchant is greater than a third threshold, or a percentage of risky users in users conducting transactions with the target merchant is greater than a fourth threshold, the acquiring system can determine that the target merchant has a risk aggregation feature.

**[0080]** The acquiring system separately uses the page web address of the second merchant page and the historical transaction data of the target merchant as a determining dimension to collaboratively determine whether the target merchant is a risky merchant. When the page web address of the second merchant page cannot be obtained or an accurate determining result cannot be provided, more reference information is provided to assist in identifying the risky merchant, thereby increasing the rate of identifying the risky merchant.

**[0081]** FIG. 7 is a schematic diagram of determining whether a target merchant is a risky merchant according to an embodiment of this specification.

**[0082]** In some implementations, with reference to FIG. 7, that the acquiring system determines, based on the first intermediate risk identification result and the second intermediate risk identification result, whether the target merchant is a risky merchant includes any one of the following: when both the first intermediate risk identification result and the second intermediate risk identification result represent that the target merchant is not risky, determining that the target merchant is not a risky merchant; when both the first intermediate risk identification result and the second intermediate risk identification result represent that the target merchant is risky, determining that the target merchant is a risky merchant; and when one of the first intermediate risk identification result and the second intermediate risk identification result represents that the target merchant is risky, sending a manual analysis task to an operator, and determining, based on an analysis result of the operator, whether the target merchant is a risky merchant.

**[0083]** In some implementations, when both the first intermediate risk identification result and the second intermediate risk identification result represent that the target merchant is not risky, it indicates that the second merchant page of the target merchant is not risky, and there is no abnormal

transaction feature or risk aggregation feature for the historical transaction data, and the acquiring system can determine that the target merchant is not a risky merchant. In this case, the acquiring system can release the payment request, and continue to advance a subsequent payment procedure of the target transaction.

**[0084]** In some implementations, when both the first intermediate risk identification result and the second intermediate risk identification result represent that the target merchant is risky, it indicates that the second merchant page of the target merchant is risky, and there is an abnormal transaction feature or a risk aggregation feature for the historical transaction data, and the acquiring system can determine that the target merchant is a risky merchant.

**[0085]** In some implementations, after determining that the target merchant is a risky merchant, the acquiring system can reject the payment request corresponding to the target transaction.

**[0086]** In some implementations, after rejecting the payment request corresponding to the target transaction, the acquiring system can further update a risk control policy corresponding to the target merchant. For example, the acquiring system can limit a quantity of transactions of the target merchant or a transaction amount, or suspend a transaction function of the target merchant.

**[0087]** After determining that the target merchant is a risky merchant, the acquiring system controls the risky merchant by rejecting the payment request corresponding to the target transaction or updating the risk control policy corresponding to the target merchant, to effectively reduce a loss of the target user and provide a more secure payment environment.

**[0088]** In some implementations, when one of the first intermediate risk identification result and the second intermediate risk identification result represents that the target merchant is risky, it indicates that the target merchant may be a risky merchant, but evidence is insufficient. In this case, the acquiring system can generate a manual analysis task, and determine, based on the analysis result fed back by the operator, whether the target merchant is a risky merchant.

**[0089]** In an example, when the first intermediate risk identification result represents that the target merchant is risky, and the second intermediate risk identification result represents that the target merchant is not risky, the manual analysis task can be manually reviewing the second merchant page of the target merchant to determine whether the second merchant page of the target merchant is risky. After determining whether the second merchant page of the target merchant is risky, the operator feeds back the analysis result to the acquiring system. If the analysis result indicates that the target merchant is not risky, the acquiring system determines that the target

merchant is not a risky merchant. In this case, the acquiring system can release the payment request, and continue to advance the subsequent payment procedure of the target transaction. If the analysis result indicates that the target merchant is risky, the acquiring system determines that the target merchant is a risky merchant. In this case, the acquiring system can reject the payment request of the target transaction, and can further update the risk control policy corresponding to the target merchant.

**[0090]** In an example, when the first intermediate risk identification result represents that the target merchant is not risky, or the first intermediate risk identification result is not obtained, and the second intermediate risk identification result represents that the target merchant is risky, the manual analysis task can be manually reviewing a historical transaction of the target merchant to determine whether the target merchant is risky. When the operator feeds back the analysis result to the acquiring system, if the analysis result indicates that the target merchant is not risky, the acquiring system determines that the target merchant is not a risky merchant. In this case, the acquiring system can release the payment request, and continue to advance the subsequent payment procedure of the target transaction. If the analysis result indicates that the target merchant is risky, the acquiring system determines that the target merchant is a risky merchant. In this case, the acquiring system can reject the payment request of the target transaction, and can further update the risk control policy corresponding to the target merchant.

**[0091]** When one of the first intermediate risk identification result and the second intermediate risk identification result represents that the target merchant is risky, the acquiring system generates the manual analysis task, and determines, based on the analysis result fed back by the operator, whether the target merchant is a risky merchant. In the case of insufficient evidence, the acquiring system can identify the risky merchant based on a manual intervention result, to further increase the rate of identifying the risky merchant, and increase the application scenario of the risky merchant identification method.

**[0092]** In conclusion, in the risky merchant identification method provided in this specification, the acquiring system integrates the checkout counter into the first merchant page of the target merchant. If the target transaction is generated between the target user and the target merchant, when receiving the payment request corresponding to the target transaction, the acquiring system can obtain the page web address of the second merchant page from the payment request, where the second merchant page is a previous hop of page of the first merchant page. Further, the

acquiring system determines, based on at least the page web address of the second merchant page, whether the target merchant is a merchant with a shell service conduction risk. It can be learned that in the above solution, in a transaction process, it can be accurately identified whether the target merchant has the shell service conduction risk, to help effectively prevent and control the merchant with the shell service conduction risk. In addition, in the above solution, in a process of identifying the risky merchant, user profile data and user transaction behavior data on a user side do not need to be used. Therefore, the solution can be applicable to deployment and implementation in the acquiring system, to improve an effect of preventing and controlling the risky merchant by the acquiring system.

**[0093]** It should be noted that user data obtained in this specification is authorized by the user, and does not relate to user privacy.

**[0094]** According to another aspect of this specification, a computer-readable non-transitory storage medium is provided and stores at least one instruction set for performing image recognition. When the at least one instruction set is executed by a processor, the at least one instruction set instructs the processor to implement the steps in the risky merchant identification method 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 computing system 200, the program code is used to enable the computing system 200 to perform the steps in the risky merchant identification method described in this specification. The program product used to implement the above-mentioned method can be a portable compact disk read-only memory (CD-ROM) including program code, and can run on the computing system 200. However, the program product in this specification is not limited thereto. In this specification, a 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, and includes but is 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 computing system 200, partially executed on the computing system 200, executed as an independent software package, partially executed on the computing system 200 and partially executed on a remote computing device, or completely executed on a remote computing device.

**[0095]** Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, 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.

**[0096]** 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.

**[0097]** 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 references to "embodiments", "one embodiment", or "alternative embodiments" in various parts of this specification do not necessarily refer to a same embodiment. In addition, specific features, structures, or characteristics can be properly combined in one or more embodiments of this specification.

**[0098]** It should be understood that in the above 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. Content of each secondary embodiment is also true when a quantity of features is less than a quantity of all features in one of the above disclosed embodiments.

**[0099]** 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.

**[0100]** Finally, it should be understood that the principles of the implementation solutions of this specification are described in the implementation solutions of the application disclosed in this specification. Other modified embodiments also fall within the scope of this specification. Therefore, the embodiments disclosed in this specification are merely examples and not limitations.

A person skilled in the art can use an alternative configuration according to the embodiments of this specification to implement the application in this specification. Therefore, the embodiments of this specification are not limited to the embodiments accurately described in the application.

## CLAIMS

What is claimed is:

1. A risky merchant identification method, applied to an acquiring system, wherein the acquiring system provides an acquiring service to a target merchant through a checkout counter, and the method comprises:

receiving a payment request corresponding to a target transaction, wherein the target transaction is a transaction between a target user and the target merchant, and the payment request is a request triggered by a payment operation performed by the target user on a first merchant page integrated with the checkout counter by using a terminal device;

obtaining a page web address of a second merchant page from the payment request, wherein the second merchant page is a previous hop of page of the first merchant page; and

determining, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant.

2. The method according to claim 1, wherein the page web address of the second merchant page is collected by the checkout counter when it is detected that the terminal device redirects from the second merchant page to the first merchant page.

3. The method according to claim 1, wherein the determining, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant comprises:

obtaining page data of the second merchant page based on the page web address of the second merchant page, and determining, based on the page data, whether the target merchant is a risky merchant.

4. The method according to claim 3, wherein the determining, based on the page data, whether the target merchant is a risky merchant comprises:

when the page data meets a target condition, determining that the target merchant is a risky merchant, wherein the target condition comprises at least one of the following:

there is a preset keyword in text content in the page data;

there is a preset object or a preset keyword in image content in the page data; and

there are at least some links configured to redirect to a preset risk page in link content in the page data.

5. The method according to claim 3, wherein the obtaining page data of the second merchant

page based on the page web address of the second merchant page, and determining, based on the page data, whether the target merchant is a risky merchant comprises:

obtaining a service conduction web address reported by the target merchant;

comparing the page web address of the second merchant page with the service conduction web address, to obtain a comparison result; and

if the comparison result is "inconsistent", obtaining the page data of the second merchant page based on the page web address of the second merchant page, and determining, based on the page data, whether the target merchant is a risky merchant.

6. The method according to claim 1, wherein the determining, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant comprises:

determining, based on the page web address of the second merchant page and historical transaction data of the target merchant, whether the target merchant is a risky merchant.

7. The method according to claim 6, wherein the determining, based on the page web address of the second merchant page and historical transaction data of the target merchant, whether the target merchant is a risky merchant comprises:

determining a first intermediate risk identification result of the target merchant based on the page web address of the second merchant page;

determining a second intermediate risk identification result of the target merchant based on the historical transaction data of the target merchant; and

determining, based on the first intermediate risk identification result and the second intermediate risk identification result, whether the target merchant is a risky merchant.

8. The method according to claim 7, wherein the determining a second intermediate risk identification result of the target merchant based on the historical transaction data of the target merchant comprises:

determining an abnormal transaction feature corresponding to the target merchant based on the historical transaction data, wherein the abnormal transaction feature represents a statistical feature of an abnormal transaction associated with the target merchant, and the abnormal transaction is a transaction that meets a preset condition in terms of at least one dimension in a transaction amount, a transaction frequency, and a transaction time period;

determining a risky user aggregation feature corresponding to the target merchant based on the historical transaction data, wherein the risky user aggregation feature represents a statistical

feature of a risky user having a transaction relationship with the target merchant; and

determining the second intermediate risk identification result based on the abnormal transaction feature and the risky user aggregation feature.

9. The method according to claim 7, wherein the determining, based on the first intermediate risk identification result and the second intermediate risk identification result, whether the target merchant is a risky merchant comprises any one of the following:

when both the first intermediate risk identification result and the second intermediate risk identification result represent that the target merchant is not risky, determining that the target merchant is not a risky merchant;

when both the first intermediate risk identification result and the second intermediate risk identification result represent that the target merchant is risky, determining that the target merchant is a risky merchant; and

when one of the first intermediate risk identification result and the second intermediate risk identification result represents that the target merchant is risky, sending a manual analysis task to an operator, and determining, based on an analysis result of the operator, whether the target merchant is a risky merchant.

10. The method according to claim 1, wherein after determining that the target merchant is a risky merchant, the method further comprises at least one of the following:

rejecting the payment request corresponding to the target transaction; and

updating a risk control policy corresponding to the target merchant.

11. An acquiring system, wherein the acquiring system provides an acquiring service to a target merchant through a checkout counter, and the acquiring system comprises:

at least one storage medium that stores at least one instruction set for identifying a risky merchant; and

at least one processor that is communicatively connected to the at least one storage medium, wherein when the acquiring system runs, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set:

receiving a payment request corresponding to a target transaction, wherein the target transaction is a transaction between a target user and the target merchant, and the payment request is a request triggered by a payment operation performed by the target user on a first merchant page integrated with the checkout counter by using a terminal device;

obtaining a page web address of a second merchant page from the payment request, wherein the second merchant page is a previous hop of page of the first merchant page; and

determining, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant.

12. The acquiring system according to claim 11, wherein the page web address of the second merchant page is collected by the checkout counter when it is detected that the terminal device redirects from the second merchant page to the first merchant page.

13. The acquiring system according to claim 11, wherein to determine, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant, the at least one processor performs the following operation:

obtaining page data of the second merchant page based on the page web address of the second merchant page, and determining, based on the page data, whether the target merchant is a risky merchant.

14. The acquiring system according to claim 13, wherein to determine, based on the page data, whether the target merchant is a risky merchant, the at least one processor performs the following operation:

when the page data meets a target condition, determining that the target merchant is a risky merchant, wherein the target condition comprises at least one of the following:

there is a preset keyword in text content in the page data;

there is a preset object or a preset keyword in image content in the page data; and

there are at least some links configured to redirect to a preset risk page in link content in the page data.

15. The acquiring system according to claim 13, wherein to obtain the page data of the second merchant page based on the page web address of the second merchant page, and determine, based on the page data, whether the target merchant is a risky merchant, the at least one processor performs the following operations:

obtaining a service conduction web address reported by the target merchant;

comparing the page web address of the second merchant page with the service conduction web address, to obtain a comparison result; and

if the comparison result is "inconsistent", obtaining the page data of the second merchant page based on the page web address of the second merchant page, and determining, based on the page

data, whether the target merchant is a risky merchant.

16. The acquiring system according to claim 11, wherein to determine, based on at least the page web address of the second merchant page, whether the target merchant is a risky merchant, the at least one processor performs the following operation:

determining, based on the page web address of the second merchant page and historical transaction data of the target merchant, whether the target merchant is a risky merchant.

17. The acquiring system according to claim 16, wherein to determine, based on the page web address of the second merchant page and the historical transaction data of the target merchant, whether the target merchant is a risky merchant, the at least one processor performs the following operations:

determining a first intermediate risk identification result of the target merchant based on the page web address of the second merchant page;

determining a second intermediate risk identification result of the target merchant based on the historical transaction data of the target merchant; and

determining, based on the first intermediate risk identification result and the second intermediate risk identification result, whether the target merchant is a risky merchant.

18. The acquiring system according to claim 17, wherein to determine the second intermediate risk identification result of the target merchant based on the historical transaction data of the target merchant, the at least one processor performs the following operations:

determining an abnormal transaction feature corresponding to the target merchant based on the historical transaction data, wherein the abnormal transaction feature represents a statistical feature of an abnormal transaction associated with the target merchant, and the abnormal transaction is a transaction that meets a preset condition in terms of at least one dimension in a transaction amount, a transaction frequency, and a transaction time period;

determining a risky user aggregation feature corresponding to the target merchant based on the historical transaction data, wherein the risky user aggregation feature represents a statistical feature of a risky user having a transaction relationship with the target merchant; and

determining the second intermediate risk identification result based on the abnormal transaction feature and the risky user aggregation feature.

19. The acquiring system according to claim 17, wherein to determine, based on the first intermediate risk identification result and the second intermediate risk identification result,

whether the target merchant is a risky merchant, the at least one processor implements any one of the following:

when both the first intermediate risk identification result and the second intermediate risk identification result represent that the target merchant is not risky, determining that the target merchant is not a risky merchant;

when both the first intermediate risk identification result and the second intermediate risk identification result represent that the target merchant is risky, determining that the target merchant is a risky merchant; and

when one of the first intermediate risk identification result and the second intermediate risk identification result represents that the target merchant is risky, sending a manual analysis task to an operator, and determining, based on an analysis result of the operator, whether the target merchant is a risky merchant.

20. A computer-readable nonvolatile storage medium, wherein the computer-readable nonvolatile 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 10 is implemented.