CHARGEBACK REQUEST PROCESSING METHOD, APPARATUS, DEVICE, MEDIUM AND PROGRAM PRODUCT

RELATED APPLICATION

[0001] This application claims the priority to Chinese Patent Application No. 2024114871904 filed on October 23, 2024 and entitled "METHOD AND APPARATUS FOR PROCESSING CHARGEBACK REQUEST, DEVICE, MEDIUM, AND PROGRAM PRODUCT", which is incorporated herein in its entirety by reference.

FIELD OF THE TECHNOLOGY

[0002] This application belongs to the technical field of computers, and particularly relates to a method and an apparatus for processing a chargeback request, a device, a medium, and a program product.

BACKGROUND OF THE DISCLOSURE

[0003] In the current digital age, the electronic payment system has become indispensable to commercial transactions, greatly boosting the convenience and efficiency of global economic activities. Payment behavior, as the core link of the transaction procedure, involves the process of transferring funds from the account of the payer to the account of the payee through channels such as bank cards and third-party payment platforms in most cases. With the technology development, the payment system requires high security and stability, and also requires the flexibility to quickly respond to market changes and needs of users.

[0004] However, in the actual application, the payment process is not always smooth. When a transaction dispute occurs, for example, when the payer suspects a payment or transaction is fraudulent or erroneous, the payee may face a chargeback request from the payer. The chargeback request means that the payer requests cancellation of the completed payment transaction from the payee through the bank or the payment institution. This mechanism aims to protect rights and interests of the customers, but also brings potential financial risks and operational challenges to merchants, especially when the chargeback requests are frequent and lack rational bases.

[0005] During the processing of the chargeback request, the evidence plays a vital role in verifying whether a transaction is filed by the payer or is a fraudulent or erroneous transaction. As a result, how to obtain more rational evidences for accurately verifying the transaction subject to the chargeback request filed by the payer has become a critical issue.

SUMMARY

[0006] An objective of embodiments of this application is to provide a method and an apparatus for processing a chargeback request, a device, a medium, and a program product that can obtain a more rational evidence for more accurately verifying a chargeback request transaction filed by a payer. To achieve the objective, the technical solution according to the embodiments of this application is as follows:

[0007] In a first aspect, a method for processing a chargeback request is provided. The method is performed by a payment verification device and includes:

[0008] receiving a request for provision of a payment evidence regarding a completed payment transmitted by a device for processing a chargeback request, a payment identifier of the completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

[0009] obtaining a second biometric feature corresponding to the completed payment based on the payment identifier, the second biometric feature being a biometric feature of a second part of the payer collected in the payment process of the completed payment; and

[0010] transmitting payment evidence information including the second biometric feature to the device for processing a chargeback request, and making the device for processing a chargeback request process the chargeback request based on a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester.

[0011] In a second aspect, a method for processing a chargeback request is provided. The method is performed by a device for processing a chargeback request and includes:

[0012] transmitting a request for provision of a payment evidence to a payment verification device, a payment identifier corresponding to a completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

[0013] receiving payment evidence information including a second biometric feature transmitted by the payment verification device, the second biometric feature being obtained by the payment verification device based on the payment identifier, and the second biometric feature being a biometric feature of a second part collected in the payment process of the completed payment;

[0014] determining a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester, and processing the chargeback request based on the matching degree.

[0015] In a third aspect, an apparatus for processing a chargeback request is provided. The apparatus is arranged in a payment verification device and includes:

[0016] a module for receiving a request for provision of a payment evidence configured to receive the request for provision of a payment evidence regarding a completed payment transmitted by a device for processing a chargeback request, a payment identifier of the completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

[0017] an obtaining module configured to obtain a second biometric feature corresponding to the completed payment based on the payment identifier, the second biometric feature being a biometric feature of a second part of the payer collected in the payment process of the completed payment; and

[0018] a payment evidence information transmitting module configured to transmit payment evidence information including the second biometric feature to the device for processing a chargeback request, and make the device for processing a chargeback request process the chargeback request based on a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester.

[0019] In a fourth aspect, an apparatus for processing a chargeback request is provided. The apparatus is arranged in a device for processing a chargeback request and includes:

[0020] a module for transmitting a request for provision of a payment evidence configured to transmit the request for provision of a payment evidence to a payment verification device, a payment identifier corresponding to a completed payment being carried in the request for provision

of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

[0021] a payment evidence information receiving module configured to receive payment evidence information including a second biometric feature transmitted by the payment verification device, the second biometric feature being obtained by the payment verification device based on the payment identifier, and the second biometric feature being a biometric feature of a second part collected in the payment process of the completed payment;

[0022] a matching degree determining module configured to determine a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester; and

[0023] a chargeback request processing module configured to process the chargeback request based on the matching degree.

[0024] In a fifth aspect, the embodiments of this application further provide a payment verification device. The payment verification device includes a memory and a processor, the memory having a computer program stored therein, and the processor, when running the computer program, implementing the method for processing a chargeback request according to any possible implementation in the first aspect.

[0025] In a sixth aspect, the embodiments of this application further provide a device for processing a chargeback request. The device for processing a chargeback request includes a memory and a processor, the memory having a computer program stored therein, and the processor, when executing the computer program, implementing the method for processing a chargeback request according to any possible implementation in the second aspect.

[0026] In a seventh aspect, the embodiments of this application further provide a computer-readable storage medium. The computer-readable storage medium has a computer program stored therein, the computer program, when executed by a processor, implementing the method for processing a chargeback request according to any possible implementation in the first aspect or the second aspect.

[0027] In an eighth aspect, the embodiments of this application further provide a computer program product. The computer program product includes a computer program, the computer

program, when executed by a processor, implementing the method for processing a chargeback request according to any possible implementation in the first aspect or the second aspect.

[0028] Details of one or more embodiments of this application are set forth in the following accompanying drawings and descriptions. Other features, objectives, and advantages of this application will become apparent from the description, the accompanying drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] To describe technical solutions in the embodiments of this application more clearly, accompanying drawings required by the embodiments will be briefly described below. Apparently, the accompanying drawings in the following description merely show the embodiments of this application, and those of ordinary skill in the art can still derive other accompanying drawings from the disclosed accompanying drawings without creative efforts.

[0030] FIG. 1 is a schematic diagram of a system for processing a chargeback request in an embodiment of this application.

[0031] FIG. 2 is an exemplary diagram of a system for processing a chargeback request in an embodiment of this application.

[0032] FIG. 3a is a flowchart of a method for processing a chargeback request in an embodiment of this application.

[0033] FIG. 3b is an exemplary diagram of a method for processing a chargeback request in an embodiment of this application.

[0034] FIG. 4 is a flowchart of collecting a biometric feature by a payment feature collecting device in an embodiment of this application.

[0035] FIG. 5 is a more specific flowchart of collecting a biometric feature by a payment feature collecting device in an embodiment of this application.

[0036] FIG. 6 is a flowchart of another method for processing a chargeback request in an embodiment of this application.

[0037] FIG. 7 is a schematic structural diagram of an apparatus for processing a chargeback request in an embodiment of this application.

[0038] FIG. 8 is a schematic structural diagram of another apparatus for processing a chargeback request in an embodiment of this application.

[0039] FIG. 9 is a schematic structural diagram of an electronic device in an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

[0040] Technical solutions in embodiments of this application will be described clearly and completely below in conjunction with accompanying drawings in the embodiments of this application. Apparently, the embodiments described are merely some embodiments rather than all embodiments of this application. All other embodiments derived by those of ordinary skill in the art from the embodiments of this application without creative efforts are to fall within the protection scope of this application.

[0041] Those of ordinary skill in the art can understand that singular forms "a/an", "one", "said", and "the" used herein may also include plural forms unless expressly stated. Further, the terms "comprise" and "include" used in the embodiments of this application mean that corresponding features can be implemented as presented features, information, data, steps, operations, elements and/or components, without excluding implementation as other features, information, data, steps, operations, elements, components and/or their combinations supported by the technical field. When one element is referred to as "connected" or "coupled" to another element, the element can be directly connected or coupled to another element, or one element and the other element can establish a connection relationship through an intermediate element. In addition, "connected" or "coupled" used herein may include wireless connection or wireless coupling. The term "and/or" used herein indicates that at least one of the items defined by the term. For example, "A and/or B" can be implemented as "A", "B" or "A and B". When a plurality of (two or more) items are described, if the relationship among the plurality of items is not clearly defined, the plurality of items can refer to one, more than one, or all of the plurality of items. For example, the description of "parameter A includes A1, A2, and A3" can be implemented as parameter A including A1 or A2 or A3, and can be implemented as parameter A including at least two of parameters A1, A2, and A3.

[0042] In the related art, when a payer pays offline by swiping a credit card or other electronic payment methods, an identity of the payer may be verified to complete a payment in a method as follows.

[0043] 1. A cardholder signs after swiping the credit card at an offline merchant. By checking whether the signature is consistent with the signature on the back of the card or in a bank record, an identity of the cardholder is confirmed and verified, to avoid fraudulent action.

[0044] 2. User three-domain (3D) Secure is used. A user verifies the identity by entering a short message service verification code of card application or confirms the account through a mobile banking application of an issuer.

[0045] The signature verification and dispute handling process adopting the method in 1 is as follows.

[0046] Signature collection: when the cardholder conducts a card swiping transaction, the signature is recorded on a transaction receipt. The merchant has the responsibility to check whether the signature of the cardholder is consistent with the signature on the back of the credit card, to preliminarily verify the identity of the cardholder.

[0047] Signature filing: the merchant keeps the signed receipt properly, usually for a period of time (such as several months to several years) for future verification.

[0048] Dispute processing: if there is a dispute in the transaction (for example, the cardholder denies making a transaction), the cardholder can file a dispute with the issuer. In this case, the issuer requires the merchant to provide the signed receipt as the evidence.

[0049] Signature check: after the signed receipt provided by the merchant is received, the issuer check the signature with the signature of the cardholder registered in the bank, to confirm authenticity of the transaction. If the signatures are inconsistent, the bank may determine the transaction is fraudulent and take corresponding measures.

[0050] However, the method may have the following disadvantages:

[0051] 1. Vulnerability to forgery: the signature of the user may be easily forged, especially in the absence of strict verification, namely, the accuracy of the same verification is low.

[0052] 2. Inconsistency: the signatures of the user may vary at different times or situations, leading to difficulty in verification and low accuracy of verification.

[0053] 3. Poor user experience: the requirement for the signature by the user may increase payment time and affect the user experience, especially during peak hours. Thus, some merchants omit verification.

[0054] For the method in 2, the transaction is verified by the 3DS, and the issuer is responsible for fraudulent chargeback. If the dispute cannot be resolved between the issuer and the cardholder, the card organization network may intervene in arbitration and make a final decision based on the evidences provided by both parties with details as below:

[0055] 1. The user confirms the payment, and the merchant places an order to initiate the transaction.

[0056] 2. The issuer requires the user to complete verification via the short message service verification code or authorize verification on the webpage or application (APP) of the issuer.

[0057] 3. After successful verification, funds are deducted to complete the payment.

[0058] 4. Dispute processing method (if the payer thinks that there is a dispute over the above payment, namely, when a chargeback request is filed, the specific processing method): if there is the dispute in the transaction (for example, the cardholder denies making a transaction), the cardholder can file the dispute with the issuer. In this case, the issuer requires the merchant to provide the signed receipt as the evidence.

[0059] However, the method (3DS) may have the following disadvantages:

[0060] 1. User experience: 3DS often requires the user to input additional authentication information (such as a password or one-time verification code), which may lead to a complicated payment process and affect the user experience.

[0061] 2. Vulnerability to forgery: a malicious user may give the verification information to another person to be entered and verified.

[0062] 3. High abandonment rate: due to additional authentication operations, some users may abandon the transaction, resulting in a decrease in conversion rate.

[0063] Before the embodiments of this application are further described in detail, the nouns and terms involved in the embodiments of this application are described. The nouns and terms involved in the embodiments of this application are constructed as follows:

[0064] Chargeback: also referred to as bill refund, indicating that the cardholder can apply for chargeback on a transaction on the bill to the bank within a period (generally 120 days, extendable up to 540 days for some chargeback reasons) after payment. The chargeback is actually a right given to the cardholder by the credit card company.

[0065] 3D Secure (3DS): the identity of the cardholder in the transaction is authenticated, or the identity is verified by providing a password and the short message service verification code, and the account is confirmed through the mobile banking application of the issuer. Implementation is usually the responsibility of the issuer.

[0066] To solve the technical problems, the embodiments of this application provide a method for processing a chargeback request. The method may be applied to a system for processing

a chargeback request. As shown in FIG. 1, the system for processing a chargeback request may include a chargeback requester device, a payment feature collecting device, a payment verification device, and a device for processing a chargeback request. The chargeback requester device performs information interaction with the device for processing a chargeback request. The device for processing a chargeback request performs information interaction with the payment verification device. The payment verification device performs information interaction with the payment feature collecting device.

[0067] In a possible implementation, as shown in FIG. 2, the device for processing a chargeback request may be an issuer device (namely, the issuer device through which the payment is made). The payment system may also include an acquirer device, a merchant device (a payment receiving side device), etc. In this case, the chargeback requester device performs information interaction with the issuer device, the issuer device performs information interaction with the acquirer device, and the acquirer device performs information interaction with the merchant device. The merchant device performs information interaction with the payment verification device, and the payment verification device performs information interaction with the payment feature collecting device.

[0068] The payment verification device is a device that is specially responsible for receiving a request for provision of a payment evidence transmitted by the device for processing a chargeback request in a chargeback request processing procedure. According to a payment identifier carried in the request, the payment verification device obtains a second biometric feature corresponding to a completed payment from a corresponding storage. The second biometric feature is a biometric feature of a second part of a payer in a payment process. Then, the payment verification device transmits payment evidence information including the second biometric feature to the device for processing a chargeback request, to assist the device for processing a chargeback request in accurately processing the chargeback request. Implementation of a function of the payment verification device is conducive to an improvement in rationality and accuracy of payment transaction verification.

[0069] The device for processing a chargeback request plays a core role in an overall system for processing a chargeback request. When the device for processing a chargeback request receives the chargeback request carrying the payment identifier filed by the payer, the device for processing a chargeback request quickly generates a request for provision of a payment evidence and transmits the request for provision of a payment evidence to the payment verification device. After the payment evidence information fed back by the payment verification device is received, the device

may compute matching between the biometric feature in the payment evidence information and the biometric feature of the chargeback requester, and obtain a matching degree. Based on the matching degree, the device for processing a chargeback request makes a corresponding decision, such as rejecting or accepting the chargeback request. Thus, the chargeback request is processed, and fairness and security of the payment transaction are guaranteed.

[0070] The payment feature collecting device is a collection source of biometric feature data in the payment process. After the payment procedure is started, the payment feature collecting device responds to the payment request, and uses a collection function to obtain a biometric feature collecting video stream including the first biometric feature and the second biometric feature of the payer. When payment success information is received, the collected first biometric feature and second biometric feature of the payer may be stored in the payment evidence storing device. Thus, key evidence data is provided for a subsequent possible chargeback request, and traceability of the payment transaction is guaranteed.

[0071] The payment evidence storing device is a device specially configured to store payment-related biometric feature data. The payment evidence storing device associatively stores the payment identifier of each payment and the biometric feature of the second part of the payer, and also stores the first biometric feature of the payer. These stored data is stored in an encrypted and associated way, and is managed using a specific storage key, to ensure security and integrity of the data. When the payment verification device needs to obtain the biometric feature of the completed payment, the payment evidence storing device provides accurate data according to the corresponding key and identifier, providing strong data support for processing the chargeback request.

[0072] Based on the payment system, as shown in FIG. 3a, a method for processing a chargeback request is provided by the embodiments of this application. The method is performed by a payment verification device, the payment verification device may be the payment verification device in FIG. 1 or FIG. 2. The method may include:

[0073] Operation S301: Receive a request for provision of a payment evidence regarding a completed payment transmitted by a device for processing a chargeback request, a payment identifier of the completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully,

and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment.

[0074] The payment identifier corresponding to a completed payment is carried in the request for provision of a payment evidence. The request for provision of a payment evidence is transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier. In the embodiments of this application, if a subject finds that a payment corresponding to the account has some problem, or a transaction is not made by the subject, the subject may file the chargeback request. The chargeback request carries a payment identifier, and the payment identifier may include a serial number corresponding to the payment (completed payment). Further, in addition to the payment identifier, the chargeback request may further carry an identity identifier of the chargeback requester.

[0075] The completed payment refers to a payment transaction that is verified based on the first biometric feature of the first part of the payer and successfully completes transfer of funds. In a payment process, a payment system collects the biometric feature (such as a palmprint feature) of the first part of the payer for identity verification, and completes the payment operation after verification. In addition, the biometric feature (such as a facial feature) of the second part of the payer may be further collected during the payment process. The biometric feature serves as an important evidence for processing the subsequent possible chargeback request.

[0076] The chargeback request is a request for cancellation of the payment transaction made by the payer to a payee through a bank or payment institution if the payer suspects the completed payment transaction has some problem, such as a fraudulent or erroneous transaction. The request carries the payment identifier that may uniquely identify the completed payment, and may also include relevant information such as the identity identifier of the chargeback requester, which is a key trigger to start a chargeback processing procedure.

[0077] Further, the completed payment subject to the chargeback request filed by the chargeback requester is a payment made based on the first biometric feature and made successfully. The first biometric feature is the biometric feature of the first part of each payer collected in the payment process of the completed payment. In the embodiments of this application, the first part may be a palm, namely, the first biometric feature is the palmprint feature of the payer collected in the payment process. To be specific, the completed payment subject to the chargeback request filed by the chargeback requester passes palmprint feature verification, and is made successfully.

[0078] For the embodiments of this application, when the device for processing a chargeback request receives the chargeback request filed by the chargeback requester, a request for

provision of a payment evidence regarding to the completed payment is generated, and is transmitted to the payment verification device.

[0079] Specifically, in the system shown in FIG. 2, the device for processing a chargeback request may be the issuer device through which the payment is made. When the issuer device receives the chargeback request filed by the chargeback requester, the request for provision of a payment evidence is generated, and the request for provision of a payment evidence is transmitted to the payment verification device through the acquirer device and the merchant device corresponding to the completed payment. Further, in this procedure, if the merchant device receives the request for provision of a payment evidence, the merchant may know the chargeback request of the chargeback requester according to the request for provision of a payment evidence. If the chargeback request is accepted, the request for provision of a payment evidence does not need to be transmitted to the payment verification device, but a chargeback accepting message is transmitted to the acquirer device, and the acquirer device may notify the issuer device that the merchant accepts the chargeback request of the chargeback requester. The issuer device returns an amount deducted in the completed payment with details shown in FIG. 3b.

[0080] The acquirer device is an intermediate link device in the payment transaction procedure, receives the request for provision of a payment evidence transmitted by the device for processing a chargeback request (such as the issuer device), and forwards the request for provision of a payment evidence to the merchant device. In addition, the acquirer device checks the matching degree between the biometric features in the payment evidence information according to a specific matching algorithm, then transmits a check result to the device for processing a chargeback request, and plays the role of information transmission and preliminary verification in the overall chargeback request processing procedure.

[0081] The merchant device is directly related to the payment transaction, and is responsible for receiving the payment request and processing a payment service in the payment process. In a chargeback request processing procedure, the merchant device receives the request for provision of a payment evidence forwarded by the acquirer device, and the merchant may know the chargeback request of the chargeback requester according to the request. If the merchant accepts the chargeback request, the merchant transmits a chargeback accepting message to the acquirer device. If the merchant rejects the chargeback request, the merchant continues to forward the request for provision of a payment evidence to the payment verification device.

[0082] Operation S302: Obtain a second biometric feature corresponding to the completed payment based on the payment identifier, the second biometric feature being a biometric feature of a second part of the payer collected in the payment process of the completed payment.

[0083] The second biometric feature is the biometric feature of the second part of the payer collected in the payment process of the completed payment. In the embodiment of this application, the biometric features of the second part of the payer may be a facial feature of the payer, an iris feature, etc., which is not limited in the embodiment of this application.

[0084] In the embodiments of this application, the biometric feature of the second part of the payer being the facial feature of the payer is taken as an example for introduction. To be specific, the payment verification device obtains the facial feature of the completed payment collected by the payment feature collecting device in the payment process after receiving the request for provision of a payment evidence carrying the payment identifier (serial number).

[0085] Operation S303: Transmit payment evidence information including the second biometric feature to the device for processing a chargeback request, and make the device for processing a chargeback request process the chargeback request based on a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester.

[0086] Further, after obtaining the facial feature of the completed payment collected by the payment feature collecting device in the payment process, the payment verification device transmits payment evidence information including the facial feature to the device for processing a chargeback request. After receiving the payment evidence information including the facial feature, the device for processing a chargeback request matches the received payment evidence information including the facial feature with the biometric feature of the chargeback requester, and processes the chargeback request based on a matching degree. In the embodiments of this application, the chargeback request is processed at least according to the matching degree between the facial feature carried in the payment evidence information and the second biometric feature (namely, the facial feature of the chargeback requester) provided by the chargeback requester.

[0087] The matching degree is a quantitative index to measure the similarity between the biometric feature in the payment evidence information and the biometric feature of the chargeback requester. The matching degree comprehensively considers the matching condition between the second biometric feature (the biometric feature of the second part of the payer in the payment process) and the fifth biometric feature of the second part of the chargeback requester, and the matching condition between the third biometric feature (the biometric feature of the first part

registered by the subject corresponding to the payer identifier) and the fourth biometric feature of the first part of the chargeback requester. The device for processing a chargeback request determines the rationality of the chargeback request according to the matching degree, and then makes a corresponding processing decision.

[0088] Specifically, in the embodiments of this application, the second biometric feature (facial feature of the chargeback requester) of the chargeback requester may be collected or obtained by the device for processing a chargeback request. The second biometric feature of the chargeback requester may be further obtained from the chargeback request. In this case, the chargeback request may carry the second biometric feature of the chargeback requester.

[0089] Specifically, in the system shown in FIG. 2, if the merchant does not accept the chargeback request, the payment evidence information needs to be obtained from the payment verification device, and the payment evidence information is transmitted to the acquirer device through the merchant device. The acquirer device checks the matching degree between the biometric features (such as the facial features and the palmprint features collected in the payment process) in payment evidence information according to a specific matching algorithm. For example, for the facial features, a scale-invariant feature transform (SIFT) algorithm is used to extract feature points, and a Euclidean distance between the feature points is computed to determine the matching degree. For the palmprint features, the matching condition is measured by combining the comprehensive scores of multi-index evaluation such as clarity, integrity, distance, and brightness.

[0090] The acquirer device transmits a check result to the issuer device, and the issuer device makes a chargeback decision based on the result. There are two main cases of chargeback decisions. One decision is to reject the chargeback request. To be specific, it is determined that the completed payment is not fraudulent or erroneous and maintains a payment state. The second decision is to accept the chargeback request and return the successfully paid amount to an account of the chargeback requester.

[0091] The issuer device transmits the processing result (namely, the chargeback decision) of the chargeback request to the chargeback requester device, and the chargeback requester decides to accept or reject the chargeback decision. If the chargeback requester accepts the chargeback decision, for example, accepts rejection of the chargeback request, and accepts that the payment is filed by the chargeback requester. Alternatively, the chargeback requester accepts the chargeback request, accepts refund, and then closes the chargeback procedure. On the other hand, if the chargeback requester rejects the chargeback decision, for example, thinks that rejection of the chargeback request by the issuer is irrational and insists that there is a problem with the payment.

The chargeback request may be solved through other procedures. Other procedures may include further providing supplementary evidence and applying for arbitration, and the specific methods are not limited, as shown in FIG. 3b.

[0092] Further, in some cases, the device for processing a chargeback request may be the issuer device, or may be a combination of the issuer device and the acquirer device. When the acquirer device is included, the acquirer device is used as a transparent transmission device, and is responsible for transmitting the request for provision of a payment evidence and the payment evidence. The operations of biometric feature matching and processing the chargeback request according to the matching result are performed by the issuer device, and the specific situation is not limited. Further, the chargeback request may be processed based on the matching degree between the biometric features in the payment evidence information and the biometric features of the chargeback requester, or may be manually checked by the issuer or the acquirer.

[0093] The embodiments of this application provide the method for processing a chargeback request. In the method, when a device for processing a chargeback request receives a chargeback request carrying a payment identifier, and a completed payment corresponding to the payment identifier is a payment made based on a first biometric feature and made successfully. The device for processing a chargeback request transmits a request for provision of a payment evidence regarding the completed payment to a payment verification device. The payment verification device obtains, based on the payment identifier, a biometric feature of a second part of a payer collected in a payment process of the completed payment, transmits payment evidence information including the biometric feature of the second part of the payer to the device, and makes the device for processing a chargeback request process the chargeback request based on a matching degree between the biometric feature in the payment evidence information and a biometric feature of the chargeback requester. To be specific, the payment evidence information regarding the completed payment obtained by the device for processing a chargeback request carries the biometric feature of the second part of the payer. The device for processing a chargeback request matches the biometric feature of the second part of the payer with the biometric feature of the chargeback requester and determines whether the payer of the completed payment is consistent with the chargeback requester. If so, the completed payment is the payment of the chargeback requester; otherwise, the completed payment may not be the payment of the chargeback requester. To be specific, the provided evidence is a biometric feature of another part of the payer in the payment process. The provided evidence is more rational for verifying whether the transaction subject to the chargeback request filed by the payer is made by the payer, such that the transaction subject to the chargeback request filed by the payer can be accurately verified.

[0094] Further, after the payment verification device obtains the payment identifier of the completed payment through the request for provision of a payment evidence, the payment verification device obtains the second biometric feature corresponding to the completed payment based on the payment identifier. Specifically, in the embodiment of this application, operation S302 of obtaining a second biometric feature corresponding to the completed payment based on the payment identifier may specifically include: transmit a request for obtainment of the biometric feature to a payment evidence storing device; and receive the second biometric feature corresponding to the completed payment transmitted by the payment evidence storing device.

[0095] The request for obtainment of the biometric feature includes the payment identifier, and the payment evidence storing device stores the biometric feature of the second part of the payer corresponding to the payment identifier of each payment.

[0096] According to the embodiments, the biometric feature of the second part may be a facial feature, namely, the payment evidence storing device stores the facial feature of the payer corresponding to the payment identifier of each payment. The facial feature of the payer corresponding to the payment identifier of each payment is the facial feature of the payer collected by the payment feature collecting device in the payment process of the payment. To be specific, in the payment process of one payment, the payment feature collecting device collects a palmprint feature of the payer, and further collects the facial features of the payer. The palmprint feature of the payer is collected to find the payer identifier and deduct a corresponding amount from the corresponding account. The facial feature of the payer is collected in the payment process to provide the evidence for the chargeback request, to verify whether the chargeback requester and the payer are consistent, and know whether the completed payment corresponding to the chargeback request is fraudulent or erroneous.

[0097] Further, for the one payment process, the corresponding payment evidence information is collected by the payment feature collecting device. For the completed payment, corresponding payment evidence information is also collected by the payment feature collecting device. In the embodiments of this application, the payment evidence information corresponding to the completed payment is collected by the payment feature collecting device by a method as follows (operation Sa and operation Sb), and is stored in the payment evidence storing device. In the embodiments of this application, the payment evidence storing device may be a cloud storage device, other storage devices, or storage devices in the payment verification device, Specifically, as shown in FIG. 4,

[0098] Operation Sa: Receive a payment request regarding the completed payment.

[0099] For the embodiments of this application, a cashier device (for example, a cashier point of sale (POS) terminal) initiates the payment, and transmits the payment identifier (serial number) carrying the completed payment to the payment feature collecting device. The payment feature collecting device receives the payment request regarding the completed payment.

[00100] Operation Sb: Obtain a biometric feature collecting video stream in response to the payment request, and store the first biometric feature and the second biometric feature of the payer in the payment evidence storing device when payment success information is received.

[00101] The biometric feature collecting video stream includes at least the first biometric feature and the second biometric feature of the payer.

[00102] Specifically, operation Sb of obtaining a biometric feature collecting video stream, and storing the second biometric feature in the payment evidence storing device when payment success information is received may specifically include operation Sb1, operation Sb2, operation Sb3, operation Sb4, and operation Sb5. Operation Sb1 to operation Sb5 are not shown in the figure with details as follows.

[00103] Operation Sb1: Collect a first video frame.

[00104] The first video frame including the second biometric feature corresponding to the payer.

[00105] For the embodiments of this application, after receiving the payment request from the cashier device, the payment feature collecting device starts capture and collects the first video frame including the second biometric feature corresponding to the payer, namely, collects the facial feature of the payer before the palmprint feature is captured.

[00106] Operation Sb2: Output first prompt information.

[00107] The first prompt information being configured for prompting the payer to provide the first biometric feature. In the embodiments of this application, after the payment feature collecting device obtains the first video frame, the prompt information configured for prompting the payer to provide the first biometric feature is outputted. To be specific, when the first video frame including the facial feature of the payer is collected, the payer is reminded to extend a palm such that the corresponding palmprint feature is collected.

[00108] Operation Sb3: Collect a second video frame including the first biometric feature. To be specific, the biometric feature collecting device collects the second video frame including the payer palmprint feature.

[00109] Specifically, to improve the accuracy of palmprint verification and reduce a storage space for storing the payer palmprint feature, when the biometric feature collecting device collects the second video frame including the palmprint feature, a preferred frame may be extracted as the second video frame from the video stream including the payer palmprint features. The preferred frame is a video frame to which clear and complete palmprints belong, and may further include a proper distance between the palm and the biometric feature collecting device, and proper brightness of the collected video frame.

[00110] The method of multi-index evaluation is used to extract the preferred frame from the video stream including the palmprint feature of the payer. Specifically, operations may be as follows:

[00111] Evaluate sharpness: compute the Laplacian variance for each frame of image in the video stream. The greater the Laplacian variance is, the sharper the image is. The formula is $V_{laplace} = Var(\nabla^2 I)$, in the formula, $V_{laplace}$ denotes the Laplacian variance, $\nabla^2 I$ denotes Laplacian transform on the image I, and Var denotes a computing variance.

[00112] Evaluate integrity: use an edge detection algorithm (such as the Canny algorithm) to detect an edge of palmprint and compute a perimeter and an area of the edge. If the perimeter and area are within a preset rational range, the palmprint is considered to be complete.

[00113] Evaluate a distance: evaluate the distance between the palm and the biometric feature collecting device through a depth sensor, and give a high score if the distance is within a preset proper range.

[00114] Evaluate a brightness: compute an average brightness of the image. If the average brightness is within the preset proper range, the brightness is considered proper. The scores of the evaluation indexes are weighted and summed to get a comprehensive score of each image frame. The weight of each evaluation index is determined by a method as follows: collect a particular number of sample video frames including palmprint features, and marking a preferred frame manually; and train a linear regression model by using the sample data, with the comprehensive score as a target variable and the scores of various evaluation indexes as independent variables. After the training is completed, a coefficient of a model is the weight of each evaluation index. The formula is $S_{total} = w_1 \times S_{clarity} + w_2 \times S_{integrity} + w_3 \times S_{distance} + w_4 \times S_{brightness}$. In the formula, S_{total} denotes the comprehensive score, w_1, w_2, w_3, and w_4 denote the weights of the evaluation indexes of the clarity, the integrity, the distance, and the brightness respectively, and $w_1 + w_2 + w_3 + w_4 = 1$, $S_{clarity}$ denotes a clarity score, $S_{integrity}$ denotes an integrity score,

$S_{distance}$ denotes a distance score, and $S_{brightness}$ denotes a brightness score. The frame having a highest comprehensive score is selected as the preferred frame, the second video frame.

[00115] Operation Sb4: Collect a third video frame including the second biometric feature of the payer if the payment success information is received and the first part of the payer is detected to leave a field of view.

[00116] For the embodiments of this application, after obtaining the preferred frame, the payment feature collecting device may transmit the preferred frame to the payment verification device for matching verification. To be specific, the payment verification device determines the matching payer from the first biometric features corresponding to the payers, to complete the payment. In this case, the payment verification device transmits a payment success message to the payment feature collecting device, and when the payment feature collecting device receives the payment success message, a second prompt message may be outputted. The second prompt information is configured for notifying the payer that the payment verification is successful based on the first biometric feature, and the palm of the payer may leave the field of view. When the palm of the payer is detected to leave the field of view, the third video frame including the second biometric feature (facial feature) of the payer is collected.

[00117] In the embodiments of this application, the first video frame, the second video frame, and the third video frame may be frame sequences, namely, multi-frame images, or single-frame images, which is not limited in the embodiments of this application. Further, in the embodiments of this application, the collection of the biometric feature of the first part and the biometric feature of the second part of the payer in the payment process is authorized and accepted by the payer.

[00118] Operation Sb5: Transmit the first video frame, the third video frame, and the corresponding payment identifier to the payment evidence storing device, and make the payment evidence storing device associatively store the second biometric feature included in the first video frame, the second biometric feature included in the third video frame, and the payment identifier.

[00119] Further, the payment evidence storing device may further associatively store the second biometric feature included in the first video frame, the first biometric feature included in the second video frame, the second biometric feature included in the third video frame, and the payment identifier.

[00120] Specifically, after the payment feature collecting device collects the first video frame, the second video frame, and the third video frame, the payment feature collecting device may extract the corresponding biometric features from the video frames. To be specific, the

payment feature collecting device obtains the second biometric feature from the first video frame, the first biometric feature from the second video frame, and the second biometric feature from the third video frame, and store these biometric features and the payment identifier in the payment evidence storing device. In another possible implementation, the payment evidence storing device or other devices may also extract the corresponding biometric features from the video frames, and store these biometric features and the payment identifier in the payment evidence storing device.

[00121] Further, the video frames may be further stored in the payment evidence storing device directly. To be specific, the first video frame, the third video frame, and the payment identifier may be further associatively stored in the payment evidence storing device directly. Specifically, the second video frame may be further associatively stored. To be specific, the first video frame, the second video frame, the third video frame, and the payment identifier may be further associatively stored in the payment evidence storing device. In the embodiments of this application, if the first video frame, the third video frame, and the payment identifier are at least associatively stored in the payment evidence storing device, the payment verification device, when receiving the request for provision of a payment evidence, obtains the first video frame and the third video frame (or the second video frame may be included) from the payment evidence storing device, and transmits the first video frame and the third video frame (or the second video frame may be included) to the device for processing a chargeback request based on the payment identifier carried in the request for provision of a payment evidence.

[00122] A specific method for the device for processing a chargeback request to analyze the corresponding second biometric features from the first video frame and the third video frame is as follows: for the first video frame and the third video frame, perform image preprocessing including graying processing, convert a color image into a gray image, to reduce a data amount and computational complexity; perform histogram equalization, enhance a contrast of the image, to make a feature in the image more prominent; use a face detection algorithm (such as a Haar cascade classifier or a deep learning-based face detection algorithm) to detect a face region in a preprocessed image; after the face region is detected, use a feature extraction algorithm (such as principal component analysis (PCA), linear discriminant analysis (LDA), or a deep learning-based feature extraction network) to extract the second biometric feature (such as a facial feature vector) from the face region; and obtain the second biometric features corresponding to the first video frame and the third video frame.

[00123] For a specific example of operation Sb1 to operation Sb5, as shown in FIG. 5,

[00124] 1. The cashier POS initiates a payment and transmits a serial number to a palm-scanning terminal (payment feature collecting device).

[00125] 2. The palm-scanning terminal captures an image, and then prompts the user to extend a palm. The image captured in this operation is an initial frame of the voucher, namely, the first video frame shown above.

[00126] 3. The palm-scanning terminal always captures the palmprint and detects the palmprint. If the palmprint is not detected by the palm-scanning terminal in the operation, operation 2 is performed.

[00127] 4. A preferred image is selected from the video stream captured in operation 3, and the preferred image is transmitted to a backend server (payment verification device) as a voucher intermediate frame for being recognized. If the palm-scanning terminal does not obtain the preferred frame, operation 3 is performed to repeatedly capture the palmprint feature.

[00128] 5. If the backend server carries out recognition successful, the palm-scanning terminal indicates success.

[00129] 6. In this case, the palm-scanning terminal needs to implement retrieval again, captures a frame when the palm leaves, and takes the frame captured when the palm leaves as a tail frame.

[00130] 7. The palm-scanning terminal transmits the initial frame, the preferred frame, the tail frame, and the serial number of the voucher to a cloud device for being associatively stored. The palm-scanning terminal and the cloud storage device are encrypted through transport layer security (TLS).

[00131] Further, in each payment process, the biometric feature collected by the payment feature collecting device is stored in the payment evidence storing device. To be specific, the biometric feature of the second part of each payer and the storage key are encrypted and associatively stored in the payment evidence storing device. The biometric feature of the second part of each payer is encrypted and stored by an encryption algorithm, such as the SM4 encryption algorithm. To further improve the storage security, the storage key is also computed with the payment identifier (such as the serial number), the payer identifier (payer ID), a device number (the device identifier of the payment feature collecting device), and the initial key through a specific algorithm (such as sha64 algorithm). The initial key is stored in the secure element (SE) of the payment feature collecting device. Further, the biometric features of the video frames (the first

video frame, the second video frame, and the third video frame) of each payer and the storage key may be encrypted and associatively stored in the payment feature collecting device.

[00132] Further, the second biometric feature corresponding to each payer is stored in the payment evidence storing device by the encryption method. Then, operation S302 of obtaining a second biometric feature corresponding to the completed payment based on the payment identifier may specifically include: determine the payer identifier corresponding to the completed payment based on the payment identifier; obtain the device identifier and the initial key from the payment feature collecting device corresponding to the completed payment; encrypt the payment identifier, the payer identifier, the device identifier, and the initial key, and obtain a biometric feature storage encryption key; and obtain the second biometric feature corresponding to the completed payment from the payment evidence storing device based on the biometric feature storage encryption key.

[00133] The sha64 algorithm may be used to encrypt the payment identifier, the payer identifier, the device identifier, and the initial key, to obtain the biometric feature storage encryption key. The specific operations are as follows: concatenate the payment identifier, the payer identifier, the device identifier, and the initial key to form a new string; input the string into the sha64 algorithm for hash computation, and obtain a 64-bit hash value, the hash value being the biometric feature storage encryption key. The formula is $K = sha64\big(concat(PID, UID, DID, IK)\big)$. In the formula, K denotes the biometric feature storage encryption key, PID denotes the payment identifier, UIDdenotes the payer identifier, DID denotes the device identifier, IK denotes the initial key, and $concat$ denotes the string concatenating operation.

[00134] In the embodiments of this application, the encrypted and stored second biometric feature (the second biometric feature corresponding to the completed payment) is obtained from the payment evidence storing device based on the biometric feature storage encryption key. The payment evidence storing device may not directly store the second biometric feature corresponding to each payer clearly, but store the video frames (the first video frame, the second video frame, and the third video frame) corresponding to each payer. Based on the embodiment, specifically, operation S303 that the payment verification device transmits payment evidence information including the second biometric feature to the device for processing a chargeback request may specifically include: the payment verification device transmits the payment evidence information including the first video frame and the third video frame to the device for processing a chargeback request.

[00135] The payment verification device transmits the payment evidence information including the first video frame and the third video frame to the device for processing a chargeback

request. The first video frame and the third video frame included in the payment evidence information are encrypted. In this case, the device for processing a chargeback request also needs to decrypt the first video frame and the third video frame, to obtain the decrypted first video frame and third video frame. Alternatively, after obtaining the encrypted first video frame and third video frame in the payment evidence information, the payment verification information decrypts the first video frame and the third video frame before transmitting the first video frame and the third video frame to the device for processing a chargeback request. The payment evidence information that may be further transmitted by the payment verification device to the device for processing a chargeback request may further include the second video frame associated with the payment evidence information, or may not include the second video frame associated with the payment evidence information, which is not limited in this embodiment of this application. Further, from the above embodiments, for one payment (the completed payment), the device for processing a chargeback request may at least obtain the second biometric feature corresponding to the first video frame and the second biometric feature corresponding to the third video frame. Under a condition that the second biometric feature included in the first video frame matches the second biometric feature included in the third video frame (namely, when the same facial features exist in the facial features included in the first video frame and the third video frame), the device for processing a chargeback request processes the chargeback request by a method (operation S1 and operation S2) as follows. Specifically, operation S1 and operation S2 are not shown in the figure. The features of the chargeback requester shown above include the fifth biometric feature of the second part of the chargeback requester. For example, the fifth biometric feature of the second part of the chargeback requester refers to the facial feature of the chargeback requester.

[00136] Operation S1: Reject the chargeback request and transmit a first notification message to the chargeback requester if the fifth biometric feature of the second part of the chargeback requester matches the designated second biometric feature.

[00137] The designated second biometric feature is the second biometric feature included in the first video frame or the third video frame. In the embodiments of this application, if the fifth biometric feature of the second part of the chargeback requester matches the designated second biometric feature, the facial feature collected during the actual payment of the completed payment is consistent with the facial feature of the chargeback requester, namely, a probability that the completed payment is fraudulent or erroneous is low. In this case, the device for processing a chargeback request rejects the chargeback request and transmits a first notification message to the chargeback requester. The first notification message carries the matching result of the second

biometric feature, and is configured for notifying the chargeback requester that the device for processing a chargeback request rejects the chargeback request.

[00138] Operation S2: Accept the chargeback request and return a successfully paid amount to an account of the chargeback requester if the fifth biometric feature of the second part of the chargeback requester fails to match the designated second biometric feature.

[00139] In the embodiments of this application, if the fifth biometric feature of the second part of the chargeback requester fails to match the designated second biometric feature, the facial feature collected during the actual payment of the completed payment is inconsistent with the facial feature of the chargeback requester, namely, a probability that the completed payment is fraudulent or erroneous is high. In this case, the device for processing a chargeback request accepts the chargeback request and returns the successfully paid amount to the account of the chargeback requester. To improve security and accuracy clearly, other errors may also be used for rechecking in this case, and then a corresponding chargeback decision (decision based on chargeback request) is made.

[00140] Further, under a condition that the second biometric feature included in the first video frame matches the second biometric feature included in the third video frame, if the fifth biometric feature of the second part of the chargeback requester fails to match the designated second biometric feature, the facial feature collected in the actual payment process of the completed payment is inconsistent with the facial feature of the chargeback requester, namely, a probability that the completed payment is fraudulent or erroneous is high. Operation S3, operation S4, and operation S5 (not shown in the figure) are performed by the device for processing a chargeback request, and there is no strict sequential performing order for operation S3 to operation S5 and for operation S1 to operation S2 with details as follows.

[00141] Operation S3: Match the designated second biometric feature with second biometric features corresponding to associated subjects of the chargeback requester.

[00142] For the embodiments of this application, besides the first biometric feature (namely the palmprint feature) of the first part of the chargeback requester, the account of the chargeback requester (the account of the completed payment) may be further bound to the palmprint feature of other associated subjects of the chargeback requester, for example, the palmprint features of relatives. To be specific, in this case, the completed payment may alternatively be made by the associated subject of the chargeback requester through palmprint scanning. Then, the facial feature of the chargeback requester is inconsistent with the facial feature collected in the payment process (facial features in the first video frame and the third video frame). In this case, the facial feature of

the associated subject of the chargeback requester is obtained (this obtaining function is accepted by the chargeback requester or provided by the chargeback requester), and then the facial features in the first video frame and the third video frame are matched with the facial features of the associated subject of the chargeback requester.

[00143] For example, the associated subjects of the chargeback requester may include subject 1 and subject 2. To be specific, the facial feature of subject 1 and the facial feature of subject 2 are matched with the facial features in the first video frame and the third video frame.

[00144] Operation S4: Transmit, if an associated matching subject having the matching second biometric feature exists in the associated subjects, a second notification message carrying the second biometric feature of the associated matching subject to the chargeback requester.

[00145] For example, if the facial feature of the subject 1 matches the facial features in the first video frame and the third video frame, the second notification message carrying the facial feature of the subject 1 is transmitted to the chargeback requester.

[00146] The second notification message is configured for notifying the chargeback requester that the completed payment is completed by the associated matching subject.

[00147] Operation S5: Receive reply information regarding the second notification message from the chargeback requester, and process the chargeback request based on the reply information.

[00148] For the embodiments of this application, after the second notification message is received, if the chargeback requester accepts the completed payment, the chargeback requester transmits the reply message regarding the second notification message to the device for processing a chargeback request, the reply message indicates that the chargeback requester accepts the completed payment (or accept withdrawal of the chargeback request), and the process may end in this case. If the reply message indicates that the chargeback request is not accepted, the device for processing a chargeback request may further reject the chargeback request, transmit the chargeback request to the device of other institutions for being processed, or process the chargeback request by other methods without limitation.

[00149] Further, under a condition that the second biometric feature included in the first video frame fails to match the second biometric feature included in the third video frame, namely, the facial features of the payer in the video frame before and after the payment collected by the payment feature collecting device fail to match. To be specific, the facial features collected in the first video frame and the facial feature collected in the third video frame are not the facial features of the same person. To rationally process the biometric feature submitted and accurately process the

chargeback request, the chargeback request is processed by the device for processing a chargeback request through operation S6 and operation S7 (not shown in the figure). There is no strict sequential performing order for operation S6 to operation S7 and for operation S1 to operation S5 with details as follows.

[00150] Operation S6: Obtain a seventh biometric feature corresponding to a first completed payer according to payment time corresponding to the completed payment if the second biometric feature included in the first video frame matches the second biometric feature of the chargeback requester, match the seventh biometric feature with the second biometric feature included in the third video frame, and process the chargeback request based on a matching result.

[00151] For the embodiments of this application, the second biometric feature included in the first video frame matches the second biometric feature of the chargeback requester. To be specific, the payment feature collecting device may collects the facial feature of the payer before the payer makes the payment (the second video frame), but fail to collect the facial feature of the payer after the payer makes the payment. In this case, the device for processing a chargeback request obtains the facial feature corresponding to the first completed payer from the payment verification device, to match the facial feature with the facial feature included in the third video frame.

[00152] The first completed payer is a payer completing the payment after the completed payment. The seventh biometric feature is the biometric feature of the second part corresponding to the first completed payer.

[00153] Further, if the device for processing a chargeback request obtains the facial feature corresponding to the first completed payer from the payment verification device, matches the facial feature with the facial feature included in the third video frame, and the matching is successful, there is no erroneous condition. Then the chargeback request of the chargeback requester is rejected, or other measures are taken to process the chargeback request, which is not limited in the embodiments of this application.

[00154] Operation S7: Obtain an eighth biometric feature corresponding to a second completed payer according to the payment time corresponding to the completed payment if the second biometric feature included in the third video frame matches the second biometric feature of the chargeback requester, match the eighth biometric feature with the second biometric feature included in the first video frame, and process the chargeback request based on a matching result.

[00155] For the embodiments of this application, the second biometric feature included in the third video frame matches the second biometric feature of the chargeback requester. To be specific,

the payment feature collecting device may collects the facial feature of the payer after the payer makes the payment (the second video frame), but fail to collect the facial feature of the payer before the payer makes the payment. In this case, the device for processing a chargeback request obtains the facial feature corresponding to the second completed payer from the payment verification device, to match the facial feature with the facial feature included in the first video frame.

[00156] The second completed payer is a payer completing the payment before the completed payment. The eighth biometric feature is the biometric feature of the second part corresponding to the second completed payer.

[00157] Further, if the device for processing a chargeback request obtains the facial feature corresponding to the second completed payer from the payment verification device, matches the facial feature with the facial feature included in the first video frame, and the matching is successful, there is no erroneous condition. Then the chargeback request of the chargeback requester is rejected, or other measures are taken to process the chargeback request, which is not limited in the embodiments of this application.

[00158] Further, in some cases, the chargeback requester mistakenly binds the biometric feature (palmprint) of the first part to an account, for example, the biometric feature of the first part of other people is bound. To improve the accuracy of the chargeback request processing, after the payment identifier of the completed payment is obtained, the method may also include: determine the payer identifier corresponding to the completed payment based on the payment identifier; and determine a third biometric feature to which the payer identifier is bound. Based on the payment identifier, the payment verification device determines the payer identifier corresponding to the completed payment by querying a pre-built association table of the payment identifier and the payer identifier in a local database. A building process of the association table is as follows: when each payment is completed, the payment verification device receives the payment identifier (such as the serial number) and the payer identifier (such as the payment subject identifier) transmitted by the payment feature collecting device, and stores a correspondence relationship between the payment identifier and the payer identifier in the association table of the local database. The association table uses the payment identifier as an index for the convenience of quick query. If the relevant information is not found in the local database, a query request is transmitted to the cloud storage device, and the cloud storage device retrieves the massive transaction data stored according to the payment identifier. During retrieval, the cloud storage device manages the stored data by partition, and divides the data according to dimensions such as payment time and payment amounts, to

improve retrieval efficiency. After the corresponding payer identifier is found, the payer identifier is fed back to the payment verification device.

[00159] In the embodiments of this application, after the payment identifier of the completed payment is obtained from the request for provision of a payment evidence, the payer identifier corresponding to the completed payment is determined based on the payment identifier. To be specific, a mapping relationship between the payment identifier and the payer identifier may be stored in the payment verification device, or the mapping relationship between the payment identifier and the payer identifier may be obtained from other devices (such as the cloud storage device).

[00160] Further, in another possible implementation, the request for provision of a payment evidence received by the payment verification device carries the payer identifier. In the embodiments of this application, the payer identifier carried in the request for provision of a payment evidence may be carried in the chargeback request triggered by the chargeback requester, or may be determined by the device for processing a chargeback request based on the payment identifier carried in the chargeback request after the chargeback request is received, and carried in the request for provision of a payment evidence.

[00161] For example, the payment identifier is the serial number of the completed payment, and the payer identifier is the ID of an actual payer of the completed payment.

[00162] Further, the payment verification device determines the third biometric feature to which the payer identifier is bound after obtaining the payer identifier corresponding to the completed payment (the ID of the actual payer of the completed payment). The third biometric feature is the biometric feature of the first part registered by a subject corresponding to the payer identifier. According to the embodiment, the biometric feature of the first part may be a palmprint feature, namely, the third biometric feature is a palmprint feature registered by the subject corresponding to the payer identifier (or may be referred to as a payment-associated palmprint feature). To be specific, if the palmprint feature collected by the payment feature collecting device matches the payment-associated palmprint feature per payment each time, verification passes, and an amount corresponding to the payment may be deducted from the account corresponding to the payer identifier. For example, if the payer 1 buys apples for 10 yuan, and the payer 1 matches the payment-associated palmprint feature through palm scanning, 10 yuan is deducted to the account of the merchant from the account bound to the payment-associated palmprint feature. The payment-associated palmprint feature is the palmprint feature registered by the subject corresponding to the payer identifier. Every time the payment is made, the payment feature

collecting device matches the collected palmprint feature with the payment-associated palmprint feature. If the matching is successful, the verification passes, and the amount corresponding to the payment may be deducted from the account corresponding to the payer identifier, which is one of the important bases for payment verification.

[00163] To improve the rationality of the provided evidence, and further and more accurately verify the transaction subject to the chargeback request filed by the payer, the payment evidence provided by the payment verification device to the device for processing a chargeback request may further include the third biometric feature, namely, the biometric feature of the first part registered by the subject corresponding to the payer identifier. From the embodiments, the biometric feature of the first part may be a palmprint feature, the third biometric feature is the palmprint feature (payment-associated palmprint feature) bound by the actual payer of the completed payment to an electronic account (electronic account 1). To be specific, in the process of payment, if the payment verification device matches the biometric feature with the corresponding palmprint feature, the verification passes, and the corresponding amount may be deducted from the electronic account 1 in this case.

[00164] Further, the biometric feature of the chargeback requester includes a fourth biometric feature of the first part and a fifth biometric feature of the second part of the chargeback requester, and the matching degree includes a matching degree between the second biometric feature and the fifth biometric feature and a matching degree between the third biometric feature and the fourth biometric feature. To be specific, in the embodiment, when the chargeback request is processed according to the matching degree between the biometric feature in the payment evidence information and the biometric feature of the chargeback requester, the fifth biometric features (facial feature) of the chargeback requester is matched with the second biometric features (facial feature collected in the payment process), and the fourth biometric feature (palmprint) of the first part of the chargeback requester further needs to be matched with the fifth biometric feature (palmprint feature bound to the account) bound to the account. If the two matching results are higher than a preset matching degree, the chargeback requester in the chargeback request and the payer collected in the actual payment process are the same person, namely, there is no fraudulent, or erroneous case (a subsequent payer makes an erroneous transaction, or a previous payer makes an erroneous transaction), and the chargeback request is rejected. For details of other cases, reference can be made to the embodiment, which is not repeated herein.

[00165] The embodiments of this application further provides another method for processing a chargeback request. The method is performed by a device for processing a chargeback request. As shown in FIG. 6, the method may include:

[00166] Operation S601: Transmit a request for provision of a payment evidence to a payment verification device, a payment identifier corresponding to a completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment.

[00167] The payment identifier corresponding to the completed payment is carried in the request for provision of a payment evidence. The request for provision of a payment evidence is transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier. The completed payment is the payment made based on the first biometric feature and made successfully. The first biometric feature is the biometric feature of the first part of each payer collected in the payment process of the completed payment.

[00168] Operation S602: Receive payment evidence information including a second biometric feature transmitted by the payment verification device, the second biometric feature being obtained by the payment verification device based on the payment identifier, and the second biometric feature being a biometric feature of a second part collected in the payment process of the completed payment.

[00169] The second biometric feature is obtained by the payment verification device based on the payment identifier. The second biometric feature is the biometric feature of the second part collected in the payment process of the completed payment.

[00170] Operation S603: Determine a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester, and process the chargeback request based on the matching degree.

[00171] Specifically, the second biometric feature includes second biometric feature information corresponding to two video frames. One video frame is a video frame collected by the payment feature collecting device before the payment feature collecting device collects the first biometric feature of the payer, and the other video frame is a video frame collected by the payment

feature collecting device when the payment feature collecting device detects the first biometric feature of the payer to leave a field of view.

[00172] Operation S603 of determining a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester, and processing the chargeback request based on the matching degree may specifically include: obtain a fifth biometric feature of the second part of the chargeback requester; determine the matching degree between the biometric feature in the payment evidence information and the biometric feature of the chargeback requester based on the second biometric feature information corresponding to the two video frames respectively and the fifth biometric feature; and process the chargeback request based on the matching degree.

[00173] A feature point matching algorithm may be used to determine the matching degree. Firstly, feature extraction is performed on the second biometric feature information corresponding to the two video frames and the fifth biometric feature, and respective feature point sets are obtained. Then, a scale-invariant feature transform (SIFT) algorithm is used to find matching feature point pairs from these feature point sets. The matching feature point pairs are corresponding feature point combinations found from respective feature point sets when the two pieces of biometric feature information is matched using a feature point matching algorithm (such as the SIFT algorithm). By computing a Euclidean distance between feature vectors of these matching feature point pairs, and averaging the Euclidean distances of all matching feature point pairs, an average Euclidean distance is obtained. Then, a reciprocal of the average Euclidean distance is used as the matching degree to determine similarity between the biometric features.

[00174] For each matching feature point pair, the Euclidean distance between the feature vectors is computed. The Euclidean distances of all matching feature point pairs are summed and averaged to obtain the average Euclidean distance. Finally, the reciprocal of the average Euclidean distance is taken as the matching degree. The formula is $M = \frac{1}{\frac{1}{n}\sum_{i=1}^{n} d_i}$. In the formula, M denotes the matching degree, n denotes the number of matching feature point pairs, and d_i denotes the Euclidean distance of an i^{th} matching feature point pair.

[00175] The procedure performed by the device for processing a chargeback request in the embodiments of this application is detailed in the embodiment, which is not repeated herein.

[00176] To better understand and explain the practical value of the solution provided by the embodiments of this application, optional embodiments of this application will be described in conjunction with specific scenario embodiments.

[00177] I. Payment procedure:

[00178] 1. The cashier POS transmits the payment request to the palm-scanning terminal. The payment request carries the serial number of a bill currently paid, and this payment is hereinafter referred to as payment 1.

[00179] 2. The palm-scanning terminal is activated for image capturing, and several frames are obtained before palm scanning, to capture the facial feature of the payment subject that is subject to palm scanning as the initial frame.

[00180] 3. The payer subject is prompted to extend the palm for palmprint scanning.

[00181] 4. After the palm-scanning terminal detects the payment palm, the palmprint is captured. When the palm-scanning terminal detects the payment palmprint, the palmprint for a preset time period may be captured, and then the payment subject is reminded to move the palm. Alternatively, the payment subject may be reminded to move the palm when the clear and complete palmprint is detected to be captured. The clear and complete palmprint is taken as the preferred frame.

[00182] 5. The palm-scanning terminal transmits the selected frame (preferred frame) to the backend server for being recognized, and the identity of the payment subject is determined. The identity is transmitted to the issuer, such that the issuer may deduct the payment from the corresponding account.

[00183] 6. When the backend server recognizes the matching palmprint, the backend server transmits indication information of successful matching to the palm-scanning terminal.

[00184] 7. The palm-scanning terminal outputs prompt information, to prompt the payment subject to move the palm.

[00185] 8. When the palm-scanning terminal detects that the payment subject moves away the palm, the palm-scanning terminal performs recapturing, to capture the facial feature of the payment subject that performs palm scanning as a tail frame.

[00186] 9. The palm-scanning terminal encrypts all frames (the initial frame, the preferred frame, and the tail frame) using the storage key and adopting the SM4 method. The storage key is obtained by encrypting the serial number, the successfully recognized user ID (payment subject identifier), the device number, and the initial key and using sha64. The initial key is stored in a secure element (SE) of the palm-scanning terminal.

[00187] II. When the chargeback request is detected, the procedure of providing evidence to make a decision on the chargeback request is as follows:

[00188] 1. When the issuer device detects the chargeback request regarding payment 1 transmitted by the chargeback requester, the issuer device generates a request for provision of a payment evidence and transmits the request for provision of a payment evidence to the acquirer device. The request for provision of a payment evidence is configured for requesting the payment evidence corresponding to payment 1, to make a decision on the chargeback request.

[00189] 2. The acquirer bank device transmits the request for provision of a payment evidence to a corresponding merchant device. If the merchant device accepts the chargeback, the acquirer device may transmit the message that the merchant accepts the chargeback to the issuer device, and the issuer device may return the amount paid by the payment 1 to the account of the chargeback requester.

[00190] 3. If the merchant rejects the chargeback, the merchant device transmits the request for provision of a payment evidence carrying the serial number to the backend server (payment verification device). Further, the request for provision of a payment evidence further carries the identity of the chargeback requester, the device identity of the palm-scanning terminal, and the initial key (obtained from the SE of the palm-scanning terminal).

[00191] 4. The backend server obtains the storage key based on the identity identifier of the chargeback requester, the device identifier of the palm-scanning terminal, the initial key, and the serial number, and obtains the payment evidence corresponding to payment 1 from the cloud storage based on the storage key. The payment evidence may at least include the initial frame and the tail frame.

[00192] 5. The backend server may transmit the payment evidence to the issuer device through the acquirer device.

[00193] 6. The issuer device may obtain the facial feature of the chargeback requester. If the facial feature of the chargeback requester matches the facial feature included in the initial frame and the facial feature included in the tail frame, the chargeback request is rejected. If the facial feature of the chargeback requester fails to match the facial features included in the initial frame and the tail frame, the issuer device returns the amount paid by the payment 1 to the account of the chargeback requester, and notify the corresponding merchant device of such a result. Alternatively, if the facial feature of the chargeback requester fails to match the facial features included in the initial frame and

the tail frame, the evidence and verification results are transmitted to the corresponding institutions for being processed.

[00194] If the facial feature of the chargeback requester matches the facial feature included in the initial frame, but fails to match the facial feature included in the tail frame, or if the facial feature of the chargeback requester matches the facial feature included in the tail frame, but fails to match the facial feature included in the initial frame, other measures may be taken or the condition is transmitted to relevant institutions for being further processed.

[00195] Further, in addition to the IOT terminal measure, to improve the security of the payment:

[00196] Risk control measures: a risk control model based on machine learning is added. The model uses a random forest algorithm to analyze transaction data in real time. The specific operations are as follows: first, collect the transaction data including a transaction amount, transaction time, a trading place, a transaction frequency and other features, and divide the transaction data into a training set and a test set; use the training set to train the random forest model; in a training process, optimize a performance of the model by adjusting parameters of the model; for the number of trees, try from a small value (such as 10 trees), gradually increase the number of trees, observe changes in the accuracy and recall of the model on the test set, and determine the appropriate number of trees when these indicators are no longer significantly improved; for the maximum depth, use a gradual trial method, start from a small depth (such as three layers), gradually increase a depth, and avoid over-fitting; adjust other parameters, such as the minimum number of samples for splitting, and the minimum number of sample leaves; and in a real-time analysis stage, input new transaction data into a trained model, and the model computes a risk probability of the transaction according to the feature. For example, if the same account initiates several large transactions in different regions within a short time, and the risk probability computed by the model exceeds a preset threshold (such as 0.8), it is determined that a risk may exists. When the model recognizes a possible risk, additional verification methods are added. For example, users are required to enter an additional short message service verification code, and perform face recognition or fingerprint recognition, to reduce the possibility of fraudulence.

[00197] Limit measures: 3DS verification is added when the transaction exceeds the limit, to ensure liability transfer for high-risk transactions. The specific method to set different transaction limits according to historical trading data and credit ratings of the user is as follows: analyze the historical trading data of the user including a distribution of trading amount, the trading frequency, trading stability, and other features. Credit rating information of the user is obtained, the credit

rating may be obtained from a professional credit rating agency, or self-evaluated according to a credit record of the user in the bank. Then, a linear regression model is used to compute a single transaction limit and a daily cumulative transaction limit. The formulas are $L_{single} = \alpha_1 \times A_{avg} + \alpha_2 \times C + \beta_1$ and $L_{daily} = \gamma_1 \times A_{total} + \gamma_2 \times C + \beta_2$. In the formulas, L_{single} denotes the single transaction limit, L_{daily} denotes the daily cumulative transaction limit, A_{avg} denotes an average amount of the historical transactions of the user, A_{total} denotes daily cumulative average amount of the historical transactions of the user, C denotes the credit rating score of the users, α_1, α_2, γ_1 and γ_2 are coefficients of the model, and β_1 and β_2 are constant items. These coefficients and constant terms may be obtained by training a large number of user data. When the transaction amount exceeds a set limit, 3D secure (3DS) verification is added. A specific procedure is as follows: when the transaction triggers the limit, the issuer transmits the verification code to the registered mobile phone of the user, and the user needs to enter the verification code on the payment page for verification. In addition, the user may also need to confirm the authorization on the mobile banking APP or the webpage of the issuer, and the transaction may be completed merely after the verification is successful, to ensure that the liability transfer for high-risk transactions.

[00198] Device and data security: the device is arranged at the merchant side. The device needs to be guaranteed extremely secure and is prevented from being breached or tampered with.

[00199] Reliable algorithm: the algorithm has an extremely low false recognition rate, authoritative authentication, etc., and establishes reliable expectations in the industry.

[00200] Further, based on the solution introduced in the embodiment, the embodiments of this application can improve the security. The palmprint recognition is a biometric feature technology, has the features of uniqueness and difficulty in forgery, can improve the security of the payment, and can further improve the user experience. Compared with traditional 3DS authentication (such as entering a password or a one-time verification code), the palmprint recognition can provide smoother payment experience, and reduce the possibility of users giving up the transactions. Through the instant verification, the biometric technology can quickly verify the identity of the user and reduce the risk of chargeback due to input errors.

[00201] Based on the same principle as the method for processing a chargeback request provided by the embodiments of this application, the embodiments of this application further provides an apparatus for processing a chargeback request. As shown in FIG. 7, the apparatus 70 may be arranged in a payment verification device, the apparatus 70 may include:

[00202] a module 71 for receiving a request for provision of a payment evidence configured to receive the request for provision of a payment evidence regarding a completed payment transmitted by a device for processing a chargeback request, a payment identifier of the completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

[00203] an obtaining module 72 configured to obtain a second biometric feature corresponding to the completed payment based on the payment identifier, the second biometric feature being a biometric feature of a second part of the payer collected in the payment process of the completed payment; and

[00204] a payment evidence information transmitting module 73 configured to transmit payment evidence information including the second biometric feature to the device for processing a chargeback request, and make the device for processing a chargeback request process the chargeback request based on a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester.

[00205] In a possible implementation of the embodiments of this application, the apparatus 70 further includes a first determining module and a second determining module.

[00206] The first determining module is configured to determine the payer identifier corresponding to the completed payment based on the payment identifier.

[00207] The second determining module is configured to determine a third biometric feature to which the payer identifier is bound, the third biometric feature being the biometric feature of the first part registered by a subject corresponding to the payer identifier;

[00208] the payment evidence information further including the third biometric feature, the biometric feature of the chargeback requester including a fourth biometric feature of the first part and a fifth biometric feature of the second part of the chargeback requester, and the matching degree including a matching degree between the second biometric feature and the fifth biometric feature and a matching degree between the third biometric feature and the fourth biometric feature.

[00209] In a possible implementation of the embodiments of this application, the obtaining module 72 is specifically configured to obtain the second biometric feature corresponding to the completed payment based on the payment identifier as follows:

[00210] transmit a request for obtainment of the biometric feature to a payment evidence storing device, the request for obtainment of the biometric feature including the payment identifier, and the payment evidence storing device storing the biometric feature of the second part of the payer corresponding to the payment identifier of each payment; and

[00211] receive the second biometric feature corresponding to the completed payment transmitted by the payment evidence storing device.

[00212] In another possible implementation of the embodiments of this application, the payment evidence information is collected by a payment feature collecting device and is stored in the payment evidence storing device as follows:

[00213] receive a payment request regarding the completed payment; and

[00214] obtain a biometric feature collecting video stream in response to the payment request, and store the first biometric feature and the second biometric feature of the payer in the payment evidence storing device when payment success information is received, the biometric feature collecting video stream including at least the first biometric feature and the second biometric feature of the payer.

[00215] In another possible implementation of the embodiments of this application, the operations of obtaining a biometric feature collecting video stream, and storing the second biometric feature in the payment evidence storing device when payment success information is received include:

[00216] collect a first video frame, the first video frame including the second biometric feature corresponding to the payer;

[00217] output first prompt information, the first prompt information being configured for prompting the payer to provide the first biometric feature;

[00218] collect a second video frame including the first biometric feature;

[00219] collect a third video frame including the second biometric feature of the payer if the payment success information is received and the first part of the payer is detected to leave a field of view; and

[00220] transmit the first video frame, the third video frame, and the corresponding payment identifier to the payment evidence storing device, and make the payment evidence storing device associatively store the second biometric feature included in the first video frame, the second biometric feature included in the third video frame, and the payment identifier.

[00221] In another possible implementation of the embodiments of this application, the second biometric feature included in the first video frame matches the second biometric feature included in the third video frame; and

[00222] the payment evidence information transmitting module 73 is specifically configured to transmit the payment evidence information including the second biometric feature to the device for processing a chargeback request as follows:

[00223] transmit the payment evidence information including the first video frame and the third video frame to the device for processing a chargeback request, and make the device for processing a chargeback request process the chargeback request by a method as follows:

[00224] reject the chargeback request and transmit a first notification message to the chargeback requester if the fifth biometric feature of the second part of the chargeback requester matches the designated second biometric feature, the designated second biometric feature being the second biometric feature included in the first video frame or the third video frame, and the first notification message carrying a matching result of the second biometric feature, and being configured for notifying the chargeback requester that the device for processing a chargeback request rejects the chargeback request.

[00225] In another possible implementation of the embodiments of this application, the device for processing a chargeback request processes the chargeback request by a method as follows:

[00226] match the designated second biometric feature with second biometric features corresponding to associated subjects of the chargeback requester if the fifth biometric feature of the second part of the chargeback requester fails to match the designated second biometric feature;

[00227] transmit, if an associated matching subject having the matching second biometric feature exists in the associated subjects, a second notification message carrying the second biometric feature of the associated matching subject to the chargeback requester; the second notification message being configured for notifying the chargeback requester that the completed payment is completed by the associated matching subject; and

[00228] receive reply information regarding the second notification message from the chargeback requester, and process the chargeback request based on the reply information.

[00229] In another possible implementation of the embodiments of this application, the device for processing a chargeback request processes the chargeback request by any method as follows:

[00230] accept the chargeback request and return a successfully paid amount to an account of the chargeback requester if the fifth biometric feature of the second part of the chargeback requester fails to match the designated second biometric feature.

[00231] In another possible implementation of the embodiments of this application, the second biometric feature included in the first video frame fails to match the second biometric feature included in the third video frame; and

[00232] the payment evidence information transmitting module 73 is specifically configured to transmit the payment evidence information including the second biometric feature to the device for processing a chargeback request as follows:

[00233] transmit the payment evidence information including the first video frame and the third video frame to the device for processing a chargeback request, and make the device for processing a chargeback request process the chargeback request by a method as follows:

[00234] obtain a seventh biometric feature corresponding to a first completed payer according to payment time corresponding to the completed payment if the second biometric feature included in the first video frame matches the second biometric feature of the chargeback requester, match the seventh biometric feature with the second biometric feature included in the third video frame, and process the chargeback request based on a matching result, the first completed payer being a payer completing the payment after the completed payment, and the seventh biometric feature being the biometric feature of the second part corresponding to the first completed payer; and

[00235] obtain an eighth biometric feature corresponding to a second completed payer according to the payment time corresponding to the completed payment if the second biometric feature included in the third video frame matches the second biometric feature of the chargeback requester, match the eighth biometric feature with the second biometric feature included in the first video frame, and process the chargeback request based on a matching result, the second completed payer being a payer completing the payment before the completed payment, and the eighth

biometric feature being the biometric feature of the second part corresponding to the second completed payer.

[00236] In another possible implementation of the embodiments of this application, the biometric feature of the second part of each payer and a storage key are stored associatively in the payment evidence storing device, the storage key of each payer is obtained by encrypting the payment identifier, the payer identifier, an initial key, and a device identifier of the corresponding payment feature collecting device, and the initial key is stored in the payment feature collecting device.

[00237] The obtaining module 72 is specifically configured to obtain the second biometric feature corresponding to the completed payment based on the payment identifier as follows:

[00238] determine the payer identifier corresponding to the completed payment based on the payment identifier;

[00239] obtain the device identifier and the initial key from the payment feature collecting device corresponding to the completed payment;

[00240] encrypt the payment identifier, the payer identifier, the device identifier, and the initial key, and obtain a biometric feature storage encryption key; and

[00241] obtain the second biometric feature corresponding to the completed payment from the payment evidence storing device based on the biometric feature storage encryption key.

[00242] The embodiments of this application further provide another apparatus for processing a chargeback request. As shown in FIG. 8, the apparatus 80 is arranged in a device for processing a chargeback request, and the apparatus 80 may include:

[00243] a module 81 for transmitting a request for provision of a payment evidence configured to transmit the request for provision of a payment evidence to a payment verification device, a payment identifier corresponding to a completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

[00244] a payment evidence information receiving module 82 configured to receive payment evidence information including a second biometric feature transmitted by the payment verification device, the second biometric feature being obtained by the payment verification device based on the

payment identifier, and the second biometric feature being a biometric feature of a second part collected in the payment process of the completed payment;

[00245] a matching degree determining module 83 configured to determine a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester; and

[00246] a chargeback request processing module 84 configured to process the chargeback request based on the matching degree.

[00247] In a possible implementation of the embodiments of this application, the second biometric feature includes second biometric feature information corresponding to two video frames. One video frame is a video frame collected by the payment feature collecting device before the payment feature collecting device collects the first biometric feature of the payer, and the other video frame is a video frame collected by the payment feature collecting device when the payment feature collecting device detects the first biometric feature of the payer to leave a field of view.

[00248] The matching degree determining module 83 is specifically configured to determine the matching degree between the biometric feature in the payment evidence information and the biometric feature of the chargeback requester as follows:

[00249] obtain a fifth biometric feature of the second part of the chargeback requester; and

[00250] determine the matching degree between the biometric feature in the payment evidence information and the biometric feature of the chargeback requester based on the second biometric feature information corresponding to the two video frames and the fifth biometric feature.

[00251] The embodiments of this application provide the apparatus for processing a chargeback request. In the embodiments of this application, when the device for processing a chargeback request receives a chargeback request carrying a payment identifier, and a completed payment corresponding to the payment identifier is a payment made based on a first biometric feature and made successfully. The device for processing a chargeback request transmits a request for provision of a payment evidence regarding the completed payment to a payment verification device. The payment verification device obtains, based on the payment identifier, a biometric feature of a second part of a payer collected in a payment process of the completed payment, transmits payment evidence information including the biometric feature of the second part of the payer to the device, and makes the device for processing a chargeback request process the chargeback request based on a matching degree between the biometric feature in the payment evidence information and a biometric feature of the chargeback requester. To be specific, the

payment evidence information regarding the completed payment obtained by the device for processing a chargeback request carries the biometric feature of the second part of the payer. The device for processing a chargeback request matches the biometric feature of the second part of the payer with the biometric feature of the chargeback requester and determines whether the payer of the completed payment is consistent with the chargeback requester. If so, the completed payment is the payment of the chargeback requester; otherwise, the completed payment may not be the payment of the chargeback requester. To be specific, the provided evidence is a biometric feature of another part of the payer in the payment process. The provided evidence is more rational for verifying whether the transaction subject to the chargeback request filed by the payer is made by the payer, such that the transaction subject to the chargeback request filed by the payer can be accurately verified.

[00252] FIG. 9 shows a schematic structural diagram of an electronic device applied according to the embodiment of the present disclosure. As shown in FIG. 9, the electronic device may be the payment verification device, the device for processing a chargeback request, the payment feature collecting device, etc. If the electronic device is the payment verification device shown above, the electronic device may be configured to perform the method according to any embodiment performed by the payment verification device. If the electronic device is the device for processing a chargeback request shown above, the electronic device may be configured to perform the method according to any embodiment performed by the device for processing a chargeback request above. If the electronic device is the payment feature collecting device shown above, the electronic device may be configured to perform the method according to any embodiment performed by the payment feature collecting device above.

[00253] As shown in FIG. 9, the electronic device 2000 may mainly include at least one processor 2001 (one is shown in FIG. 9), a memory 2002, a communication module 2003, an input/output interface 2004, and other components. In some embodiments, the components may be connected and communicate through a bus 2005. The structure of the electronic device 2000 shown in FIG. 9 is merely exemplary, and does not constitute limitation to the electronic device applied to the method according to the embodiments of this application.

[00254] The memory 2002 may be configured to store an operating system, an application, etc. The application programs may include a computer program that implements the method shown in the embodiments of the present disclosure when invoked by the processor 2001, and may further include a program that implements other functions or services. The memory 2002 may be a read only memory (ROM) or other types of static storage devices that may store static information and

instructions, a random access memory (RAM) or other types of dynamic storage devices that may store information and computer programs, or may be an electrically erasable programmable read only memory (EEPROM), a compact disc read only memory (CD-ROM), or other optical disc storages, an optical disk storage (including a compact optical disk, a laser disc, an optical disk, a digital versatile disk, a Blu-ray disc, etc.), a magnetic disc storage medium or other magnetic storage devices, or any other medium that may be configured to carry or store expected program code in the form of instructions or data structures and may be accessed by a computer, which is not limited.

[00255] The processor 2001 is connected to the memory 2002 through the bus 2005, and corresponding functions are implemented by invoking the application stored in the memory 2002. The processor 2001 may be a central processing unit (CPU), a general processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic devices, a transistor logic device, a hardware component, or their any combination, and may implement or perform various exemplary logic blocks, modules, and circuits described in connection with the present disclosure. The processor 2001 may alternatively be a combination implementing a computation function, and may include, for example, one or a combination of two or more microprocessors, and a combination of a DSP and a microprocessor.

[00256] The electronic device 2000 may be connected to the network through the communication module 2003 (including but not limited to components such as the network interface), to communicate with other devices (such as a user terminal or a server) through the network and implement data interaction, for example, transmitting data to or receiving data from other devices. The communication module 2003 may include a wired network interface and/or a wireless network interface, etc. To be specific, the communication module may include at least one of a wired communication module or a wireless communication module.

[00257] The electronic device 2000 may be connected to a required input/output device, such as a keyboard and a display device, through the input/output interface 2004. The electronic device 2000 may have a display device, and may be further externally connected to other display devices through the interface 2004. In some embodiments, a storage apparatus, such as a hard disk, may be connected through the interface 2004, such that data in the electronic device 2000 may be stored in the storage device, or data in the storage device may be read, and data in the storage device may be further stored in the memory 2002. The input/output interface 2004 may be a wired interface or a wireless interface. According to varying actual application scenarios, the device connected to the

input/output interface 2004 may be a component of the electronic device 2000 or an external device connected to the electronic device 2000 when necessary.

[00258] The bus 2005 configured to connect various components may include a path to transfer information between the above components. The bus 2005 may be a peripheral component interconnect (PCI) bus or an extended industry standard architecture (EISA) bus. According to different functions, the bus 2005 may be divided into an address bus, a data bus, and a control bus.

[00259] In some embodiments, for the solution provided by the embodiment of the present disclosure, the memory 2002 may be configured to store a computer program configured to perform the solution of the present disclosure and run by the processor 2001, and the processor 2001, when running the computer program, implements the actions of the method or the apparatus according to the embodiments of the present disclosure.

[00260] Based on the same principle as the method according to the embodiments of this application, the embodiments of this application provide a computer-readable storage medium. The computer-readable storage medium has a computer program stored therein, and the computer program, when executed by a processor, may implement corresponding contents of the method embodiment described above.

[00261] The embodiments of this application further provide a computer program product. The product includes a computer program. The computer program, when executed by a processor, may implement corresponding contents of the method embodiment described above.

[00262] To sum up, this application provides the method and the apparatus for processing a chargeback request, the device, the computer-readable storage medium, and the computer program product. The payment verification device receives the request for provision of a payment evidence carrying the payment identifier of the completed payment transmitted by the device for processing a chargeback request, the request is transmitted when the device for processing a chargeback request receives the chargeback request carrying the same payment identifier, and the completed payment is successfully made based on the first biometric feature of the first part of the payer collected in the payment process. Then, the payment verification device obtains the second biometric feature of the second part of the payer corresponding to the completed payment based on the payment identifier, transmits the payment evidence information including the second biometric feature to the device for processing a chargeback request, and makes the device for processing a chargeback request process the chargeback request based on the matching degree between the biometric feature in the payment evidence information and the biometric feature of the chargeback requester. By introducing the biometric feature of the second part as the payment evidence, dimension of biometric feature

verification is increased. Compared with single biometric feature verification, the method can reflect the identity feature of the payer more comprehensively, thus improving the verification accuracy of the transaction subject to the chargeback request filed by the payer. The biometric features of different parts have different feature information. Combined use can reduce a probability of erroneous determination caused by susceptibility of the single biometric feature to fraudulence or errors, reliability of payment verification can be improved, and the security of payment transactions can be guaranteed.

[00263] Further, after receiving the request for provision of a payment evidence, the payment verification device further determines the payer identifier corresponding to the completed payment based on the payment identifier, and determines the third biometric feature to which the payer identifier is bound, namely, the biometric feature of the first part registered by the subject corresponding to the payer identifier. In addition to the second biometric feature, the payment evidence information further includes the third biometric feature. The biometric feature of the chargeback requester includes the fourth biometric feature of the first part and the fifth biometric feature of the second part. The matching degree comprehensively considers the matching condition between the second biometric feature and the fifth biometric feature, and the matching condition between the third biometric feature and the fourth biometric feature. This multi-dimensional biometric feature matching method verifies the identities of the payer and the chargeback requester from different angles, reducing a verification error caused by individual differences in biometric feature or environmental factors. The comprehensive verification of a plurality of biometric features improves the accuracy and reliability of the identity identification, makes the processing of the chargeback request more scientific and rational, and reduces a possibility of erroneous determination and missed determination.

[00264] Further, when the payment verification device obtains the second biometric feature corresponding to the completed payment based on the payment identifier, the payment verification device transmits the request for obtainment of the biometric feature including the payment identifier to the payment evidence storing device. The payment evidence storing device stores the biometric feature of the second part of the payer corresponding to the payment identifier of each payment, and the payment verification device receives the second biometric feature corresponding to the completed payment transmitted by the storing device. The centralized storage of the biometric feature through the special payment evidence storing device implements unified management of biometric feature data. This centralized storage method facilitates data classification, indexing and retrieval, and improves efficiency of data query. In addition, the centralized storage is also conducive to the security protection of data. By adopting unified security policies and technical

means, the integrity and confidentiality of biometric feature data are guaranteed, data leakage and tampering are prevented, and a reliable data basis is provided for subsequent accurate processing of the chargeback request.

[00265] Further, the payment evidence information is collected by the payment feature collecting device and is stored in the payment evidence storing device. The payment feature collecting device receives the payment request regarding the completed payment, obtains a biometric feature collecting video stream including at least the first biometric feature and the second biometric feature of the payer in response to the request, and stores the first biometric feature and the second biometric feature of the payer to the payment evidence storing device when payment success information is received. In the payment process, the biometric feature is collected synchronously, ensuring timeliness and accuracy of data. The collected biometric feature is obtained in real time when the payment behavior occurs, reflects real identity information of the payer at that time, and avoids possible information discrepancy or fraudulence due to ex-post collection. In addition, the biometric feature is stored in the payment evidence storing device in time. Thus, relevant data is rapidly obtained conveniently for subsequently processing the chargeback request, and efficiency of the processing procedure is improved.

[00266] Further, the process for the payment feature collecting device to obtain the biometric feature collecting video stream and store the second biometric feature includes: collect the first video frame including the second biometric feature of the payer, output first prompt information prompting the payer to provide the first biometric feature, collect the second video frame including the first biometric feature, collect the third video frame including the second biometric feature of the payer if the payment success message is received and the first part of the payer is detected to leave the field of view, transmit the first video frame, the third video frame, and a corresponding payment identifier to the payment evidence storing device, and make the storing device store the information. Different video frames are collected in stages, and changes in biometric feature of the payer in the payment process are comprehensively recorded. The first video frame is collected before the payment, and reflects the biometric feature of the payer at an initial state. The second video frame collects the first biometric feature configured for payment identity verification. The third video frame is collected after the payment, to verify continuity of the identity of the payer. These video frames and the payment identifier are associatively stored, such that relevant biometric feature information is quickly and accurately obtained conveniently according to the payment identifier when the chargeback request is processed, the efficiency of evidence collection and management is improved, and the accuracy and reliability of the processing of the chargeback request are improved.

[00267] Further, when the second biometric feature included in the first video frame matches the second biometric feature included in the third video frame, the payment verification device transmits the payment evidence information including the first video frame and the third video frame to the device for processing a chargeback request. If the fifth biometric feature of the second part of the chargeback requester matches the designated second biometric feature included in the first video frame or the third video frame, the device for processing a chargeback request rejects the chargeback request, and transmits the first notification message carrying the matching result of the second biometric feature to the chargeback requester. The determination method based on matching of the biometric features of multi-video frames increases the dimension and reliability of verification. The biometric features in the multi-video frames verify each other, improving the accuracy of identity verification of the payer. When the matching is successful, it can be determined that the payment is made by the payer with greater confidence, and the situation of erroneous determination of the chargeback request can be reduced. The matching result notification is transmitted to the chargeback requester in time. The transparency of the processing procedure is improved, the chargeback requester can know the processing result in time, and the trust of the user in the payment system is improved.

[00268] Further, if the fifth biometric feature of the second part of the chargeback requester fails to match the designated second biometric feature, the device for processing a chargeback request has two processing methods. Firstly, the designated second biometric feature is matched with the second biometric feature corresponding to the associated subject of the chargeback requester. If a matching associated matching subject exists, a second notification message carrying the second biometric feature of the associated matching subject is transmitted to the chargeback requester, the chargeback requester is notified that the completed payment is completed by the associated matching subject, reply information regarding the notification message is received from the chargeback request policy, and the chargeback request is processed based on the reply information. Secondly, the chargeback request is directly accepted and a successfully paid amount is returned to an account of the chargeback requester. These two processing methods consider various possible situations. Thus, the flexibility and accuracy of the processing of the chargeback request are improved. When the chargeback requester fails to match the payment biometric feature, the associated subject matching is used for further investigation, to avoid erroneous determination caused by the fact that the payer may entrust others to pay. If no rational association may be found, the chargeback request is processed in time. Thus, rights and interests of the chargeback requester are guaranteed, and fairness and user experience of the payment system are improved.

[00269] Further, the biometric feature of the second part of each payer and a storage key are stored associatively in the payment evidence storing device, the storage key of each payer is obtained by encrypting the payment identifier, the payer identifier, an initial key, and a device identifier of the corresponding payment feature collecting device, and the initial key is stored in the payment feature collecting device. When the payment verification device obtains the second biometric feature corresponding to the completed payment based on the payment identifier, the payment verification device first determines the payer identifier, obtains the device identifier and the initial key from the payment feature collecting device, encrypts the information to obtain the biometric feature storage encryption key, and then obtains the second biometric feature from the payment evidence storing device based on the key. The security of biometric feature data is improved by using encrypted storage and obtaining the biometric feature. An encryption algorithm encrypts the biometric feature data, and converts the data into ciphertext. Original data can be obtained merely through decryption by using a correct storage key. Even if the data is intercepted in a transmission or storage process, an attacker cannot obtain effective information, and privacy of the payer and the security of the payment transaction are guaranteed. In addition, the storage key generated based on a plurality of factors is used, increasing complexity and randomness of the key, and further improving reliability of encryption.

[00270] Further, when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the device for processing a chargeback request transmits a request for provision of a payment evidence carrying the same payment identifier to the payment verification device, receives the payment evidence information including the second biometric feature transmitted by the payment verification device, determines the matching degree between the biometric feature in the payment evidence information and the biometric feature of the chargeback requester, and processes the chargeback request based on the matching degree. The device for processing a chargeback request plays a core coordinating and decision-making role throughout an overall procedure, and through information interaction with the payment verification device, effective use of biometric feature data is implemented. By accurately determining the matching degree between the biometric features, rationality of the chargeback request can be scientifically and rationally determined, and normal order of the payment transaction can be guaranteed. In addition, the decision-making is made based on the matching degree, interference of human factors is reduced, subjectivity and accuracy of a processing result are improved, and the stability and reliability of the payment system are improved.

[00271] The terms "first", "second", "third", "fourth", "1", "2", etc. (if any) in the description of this application, the claims, and the accompanying drawings are used to distinguish similar

objects, but are not necessarily used to describe specific sequence or sequential order. Data used in this way is interchangeable under appropriate circumstances, such that the embodiments of this application described herein can be implemented in a sequence other than those illustrated or described in text.

[00272] In the embodiments of this application, the term "module" or "unit" refers to a computer program or a part of the computer program having a predetermined function, works with other related parts to achieve a predetermined target, and may be implemented in whole or in part by using software, hardware (such as a processing circuit or a memory) or their combinations. Similarly, a processor (or a plurality of processors or memories) may be configured to implement one or more modules or units. Further, each module or unit may be a part of an entire module or unit that includes a function of the module or unit.

[00273] Although various operation steps are indicated by arrows in the flowchart of the embodiments of this application, the implementation order of these steps is not limited to the order indicated by arrows. Unless explicitly stated herein, in some implementation scenarios of the embodiments of this application, the implementation steps in each flowchart may be executed in other orders as required. In addition, some or all steps in each flowchart may include a plurality of sub-steps or a plurality of stages based on actual implementation scenarios. Some or all of these sub-steps or stages may be performed simultaneously, and the sub-steps or stages may alternatively be performed at different moments. The performing sequence of these sub-steps or stages may be flexibly configured according to the requirements under different performing moments, which is not limited by the embodiments of this application.

[00274] The technical features of the embodiments described above can be combined in different manners to form other embodiments. The combinations of these technical features are to fall within the scope in the description as long as no conflict exists. For those of ordinary skill in the art, several variations and improvements can also be made without departing from the concept of this application, and are to fall within the protection scope of this application. Hence, the protection scope of the patent for this application is to be subject to the appended claims.

CLAIMS

1. A method for processing a chargeback request, performed by a payment verification device, comprising:

receiving a request for provision of a payment evidence regarding a completed payment transmitted by a device for processing a chargeback request, a payment identifier of the completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

obtaining a second biometric feature corresponding to the completed payment based on the payment identifier, the second biometric feature being a biometric feature of a second part of the payer collected in the payment process of the completed payment; and

transmitting payment evidence information comprising the second biometric feature to the device for processing a chargeback request, and making the device for processing a chargeback request process the chargeback request based on a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester.

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

determining a payer identifier corresponding to the completed payment based on the payment identifier; and

determining a third biometric feature to which the payer identifier is bound, the third biometric feature being the biometric feature of the first part registered by a subject corresponding to the payer identifier;

the payment evidence information further comprising the third biometric feature, the biometric feature of the chargeback requester comprising a fourth biometric feature of the first part and a fifth biometric feature of the second part of the chargeback requester, and the matching degree comprising a matching degree between the second biometric feature and the fifth biometric feature and a matching degree between the third biometric feature and the fourth biometric feature.

3. The method according to claim 1 or 2, wherein the obtaining a second biometric feature corresponding to the completed payment based on the payment identifier comprises:

transmitting a request for obtainment of the biometric feature to a payment evidence storing device, the request for obtainment of the biometric feature comprising the payment identifier, and the payment evidence storing device storing the biometric feature of the second part of the payer corresponding to the payment identifier of each payment; and

receiving the second biometric feature corresponding to the completed payment transmitted by the payment evidence storing device.

4. The method according to claim 3, wherein the payment evidence information is collected by a payment feature collecting device and is stored in the payment evidence storing device as follows:

receiving a payment request regarding the completed payment; and

obtaining a biometric feature collecting video stream in response to the payment request, and storing the first biometric feature and the second biometric feature of the payer in the payment evidence storing device when payment success information is received, the biometric feature collecting video stream comprising at least the first biometric feature and the second biometric feature of the payer.

5. The method according to claim 4, wherein the obtaining a biometric feature collecting video stream, and storing the second biometric feature in the payment evidence storing device when payment success information is received comprise:

collecting a first video frame, the first video frame comprising the second biometric feature corresponding to the payer;

outputting first prompt information, the first prompt information being configured for prompting the payer to provide the first biometric feature;

collecting a second video frame comprising the first biometric feature;

collecting a third video frame comprising the second biometric feature of the payer if the payment success information is received and the first part of the payer is detected to leave a field of view; and

transmitting the first video frame, the third video frame, and the corresponding payment identifier to the payment evidence storing device, and making the payment evidence storing device associatively store the second biometric feature comprised in the first video frame, the second biometric feature comprised in the third video frame, and the payment identifier.

6. The method according to claim 5, wherein the second biometric feature comprised in the first video frame matches the second biometric feature comprised in the third video frame; and

the transmitting payment evidence information comprising the second biometric feature to the device for processing a chargeback request comprises:

transmitting the payment evidence information comprising the first video frame and the third video frame to the device for processing a chargeback request, and making the device for processing a chargeback request process the chargeback request by a method as follows:

rejecting the chargeback request and transmitting a first notification message to the chargeback requester if the fifth biometric feature of the second part of the chargeback requester matches the designated second biometric feature, the designated second biometric feature being the second biometric feature comprised in the first video frame or the third video frame, and the first notification message carrying a matching result of the second biometric feature, and being configured for notifying the chargeback requester that the device for processing a chargeback request rejects the chargeback request.

7. The method according to claim 6, wherein the device for processing a chargeback request processes the chargeback request by any method as follows:

matching the designated second biometric feature with second biometric features corresponding to associated subjects of the chargeback requester if the fifth biometric feature of the second part of the chargeback requester fails to match the designated second biometric feature; transmitting, if an associated matching subject having the matching second biometric feature exists in the associated subjects, a second notification message carrying the second biometric feature of the associated matching subject to the chargeback requester; and receiving reply information regarding the second notification message from the chargeback requester, and processing the chargeback request based on the reply information, the second notification message being configured for notifying the chargeback requester that the completed payment is completed by the associated matching subject; and

accepting the chargeback request and returning a successfully paid amount to an account of the chargeback requester if the fifth biometric feature of the second part of the chargeback requester fails to match the designated second biometric feature.

8. The method according to any one of claims 3 to 7, wherein the biometric feature of the second part of each payer and a storage key are stored associatively in the payment evidence storing device, the storage key of each payer is obtained by encrypting the payment identifier, the payer identifier, an initial key, and a device identifier of the corresponding payment feature collecting device, and the initial key is stored in the payment feature collecting device; and

the obtaining a second biometric feature corresponding to the completed payment based on the payment identifier comprises:

determining the payer identifier corresponding to the completed payment based on the payment identifier;

obtaining the device identifier and the initial key from the payment feature collecting device corresponding to the completed payment;

encrypting the payment identifier, the payer identifier, the device identifier, and the initial key, and obtaining a biometric feature storage encryption key; and

obtaining the second biometric feature corresponding to the completed payment from the payment evidence storing device based on the biometric feature storage encryption key.

9. A method for processing a chargeback request, performed by a device for processing a chargeback request, comprising:

transmitting a request for provision of a payment evidence to a payment verification device, a payment identifier corresponding to a completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

receiving payment evidence information comprising a second biometric feature transmitted by the payment verification device, the second biometric feature being obtained by the payment verification device based on the payment identifier, and the second biometric feature being a biometric feature of a second part collected in the payment process of the completed payment; and

determining a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester, and processing the chargeback request based on the matching degree.

10. An apparatus for processing a chargeback request, arranged in a payment verification device, comprising:

a module for receiving a request for provision of a payment evidence configured to receive the request for provision of a payment evidence regarding a completed payment transmitted by a device for processing a chargeback request, a payment identifier of the completed payment being carried in

the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

an obtaining module configured to obtain a second biometric feature corresponding to the completed payment based on the payment identifier, the second biometric feature being a biometric feature of a second part of the payer collected in the payment process of the completed payment; and

a payment evidence information transmitting module configured to transmit payment evidence information comprising the second biometric feature to the device for processing a chargeback request, and making the device for processing a chargeback request process the chargeback request based on a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester.

11. An apparatus for processing a chargeback request, arranged in a device for processing a chargeback request, comprising:

a module for transmitting a request for provision of a payment evidence configured to transmit the request for provision of a payment evidence to a payment verification device, a payment identifier corresponding to a completed payment being carried in the request for provision of a payment evidence, the request for provision of a payment evidence being transmitted when the device for processing a chargeback request receives the chargeback request carrying the payment identifier, the completed payment being a payment made based on a first biometric feature and made successfully, and the first biometric feature being a biometric feature of a first part of each payer collected in a payment process of the completed payment;

a payment evidence information receiving module configured to receive payment evidence information comprising a second biometric feature transmitted by the payment verification device, the second biometric feature being obtained by the payment verification device based on the payment identifier, and the second biometric feature being a biometric feature of a second part collected in the payment process of the completed payment;

a matching degree determining module configured to determine a matching degree between the biometric feature in the payment evidence information and a biometric feature of a chargeback requester; and

a chargeback request processing module configured to process the chargeback request based on the matching degree.

12. A payment verification device, comprising a memory and a processor, the memory having a computer program stored therein, and the processor, when running the computer program, performing the method for processing a chargeback request according to any one of claims 1 to 8.

13. A device for processing a chargeback request, comprising a memory and a processor, the memory having a computer program stored therein, and the processor, when running the computer program, performing the method for processing a chargeback request according to claim 9.

14. A computer-readable storage medium, having a computer program stored therein, the computer program, when executed by a processor, implementing the method for processing a chargeback request according to any one of claims 1 to 9.

15. A computer program product, comprising a computer program, the computer program, when executed by a processor, implementing the method for processing a chargeback request according to any one of claims 1 to 9.