

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

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

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

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

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

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

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

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