CLAIMS

1. A payment risk control method applied to an application side, the method comprising:

after receiving trigger of a station entering and exiting payment operation, generating a payment graphic code generation request carrying preset risk control features, wherein the risk control features comprise at least: a payment account feature, a current location feature, and a station entering and exiting feature;

sending the payment graphic code generation request to a risk control side, so that the risk control side obtains pre-stored historical risk control features of an account according to the payment account feature in the request, detects whether there is a transaction risk on the application side by comparing the obtained historical risk control features with the risk control features carried in the request, and returns a risk control detection result to the application side, wherein a method for detecting the transaction risk includes: deciding whether a payment graphic code generated this time is used for station entering or station exiting according to the station entering and exiting feature; if it is for station entering, deciding whether a frequency of the payment graphic code generation request is higher than a preset threshold, and if so, determining that there is a transaction risk; and if it is for station exiting, deciding whether the current location feature and a corresponding station entering location feature in the historical risk control features meet a preset location relation condition, and if not, determining that there is a transaction risk; and

after receiving a result of no transaction risk returned by the risk control side, generating and displaying, by the application side, a payment graphic code,

wherein the risk control side comprises:

a cloud risk control side and a local risk control side,

wherein the cloud risk control side is deployed on a cloud server and connected with the application side through a wireless network, and the local risk control side is deployed on a local

mobile terminal where the application side is located and connected with the application side through a wired link in the terminal, and

wherein sending the request to the risk control side comprises:

deciding, by the application side, whether a current network signal of the mobile terminal reaches a preset strength; if so, sending the payment graphic code generation request to the cloud risk control side, and if not, sending the payment graphic code generation request to the local risk control side.

2. The method according to claim 1, after the risk control side receives the payment graphic code generation request sent by the application side, further comprising:

updating the historical risk control features of a corresponding payment account with the risk control features carried in the payment graphic code generation request, so that the transaction risk detection is performed subsequently according to the updated historical risk control features.

3. The method according to claim 1, wherein the method for detecting the transaction risk further comprises:

obtaining a pre-stored blacklist; and

determining whether objects with transaction risks recorded in the blacklist comprise an object corresponding to the request according to the risk control features in the payment graphic code generation request,

wherein the object comprises at least: a payment account, user information bound to the payment account, and/or device information of a mobile terminal where the application side is located.

4. A payment risk control method applied to a risk control side, the method comprising:

after receiving a payment graphic code generation request sent by an application side after receiving trigger of a station entering and exiting payment operation, wherein the payment graphic code generation request carries preset risk control features, wherein the risk control features comprise: a payment account feature, a current location feature, and a station entering and exiting feature, obtaining pre-stored historical risk control features of the account according to the payment account feature in the request; and

detecting whether there is a transaction risk on the application side by comparing the obtained historical risk control features with risk control features carried in the request, and returning a risk control detection result to the application side,

wherein a method for detecting the transaction risk includes: deciding whether a payment graphic code generated this time is used for station entering or station exiting according to a station entering and exiting feature; if it is for station entering, deciding whether a frequency of the payment graphic code generation request is higher than a preset threshold, and if so, determining that there is a transaction risk; and if it is for station exiting, deciding whether a current location feature and a corresponding station entering location feature in the historical risk control features meet a preset location relation condition, and if not, determining that there is a transaction risk,

wherein the risk control side comprises:

a cloud risk control side and a local risk control side,

wherein the cloud risk control side is deployed on a cloud server and connected with the application side through a wireless network, and the local risk control side is deployed on a local mobile terminal where the application side is located and connected with the application side through a wired link in the terminal, and

wherein the request being sent by an application side comprises:

deciding, by the application side, whether a current network signal of the mobile terminal reaches a preset strength; if so, sending the payment graphic code generation request to the cloud risk control side, and if not, sending the payment graphic code generation request to the local risk control side.

5. The method according to claim 4, after the risk control side receives the payment graphic code generation request sent by the application side, further comprising:

updating the historical risk control features of a corresponding payment account with the risk control features carried in the payment graphic code generation request, so that the transaction risk detection is performed subsequently according to the updated historical risk control features.

6. The method according to claim 4, wherein the risk control side detects the transaction risk specifically further by:

obtaining a pre-stored blacklist; and

determining whether objects with transaction risks recorded in the blacklist comprise an object corresponding to the request according to the risk control features in the payment graphic code generation request,

wherein the object comprises at least: a payment account, user information bound to the payment account, and/or device information of a mobile terminal where the application side is located.

7. A payment risk control apparatus applied to an application side device, the apparatus comprising: a memory, a processor, and a computer program stored on the memory and

executable on the processor, wherein the processor implements the method according to any one of claims 1 to 3 when executing the program.

8. A payment risk control apparatus applied to a risk control side device, comprising a memory, a processor, and a computer program stored on the memory and executable on the processor, wherein the processor implements the method according to any one of claims 4 to 6 when executing the program.