

What is claimed is:

1. A method for resetting a payment password, comprising:

training, by one or more processors, a prediction model with sample data, wherein the sample data comprises user data of one of the following users:

(a) first users having historical payment behaviors indicating a frequency of using payment passwords greater than a threshold and having payment failure due to an incorrect or a locked payment password; and

(b) second users having historical payment behaviors indicating a frequency of using payment passwords greater than the threshold, who do not reset their respective payment passwords within a preset time period, and who made a successful payment with their respective payment passwords;

obtaining, by the one or more processors, user information of a user as an input feature to the trained prediction model;

predicting, by the one or more processors using the trained prediction model according to a set determination condition, whether the user has forgotten a payment password associated with a payment application; and

in response to predicting that the user has forgotten the payment password associated with the payment application and detecting the user logging in the payment application with a login password different from the payment password associated with the payment application, displaying, by the one or more processors, a user interface for directing the user to a payment password resetting interface for resetting the payment password associated with the payment application.

2. The method according to claim 1, wherein the user information comprises one or more pieces of the following:

identity information, asset information, behavior information of using the payment password associated with the payment application, or management information on the payment password associated with the payment application.

3. The method according to claim 1, wherein the user has historical payment behaviors satisfying an activeness condition.

4. The method according to claim 1, wherein the set of the determination conditions comprises any one of the following:

a payment failure because of inputting an incorrect payment password or a locked payment password, and the payment password associated with the payment application having not been reset since the payment failure;

that the user has not used the payment password associated with the payment application in a first preset time period; or

that the user has not logged in the payment application in a second preset time period.

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

in response to the user selecting an option to reset the payment password associated with the payment application at the user interface, displaying, by the one or more processors, the payment password resetting interface for resetting the payment password associated with the payment application.

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

predicting, by the one or more processors, that the user has not forgotten the payment password associated with the payment application when the user uses a biometric feature to authorize payments.

7. An electronic device, comprising:

a processor; and

a memory configured to store instructions executable by the processor,

wherein the processor is configured to perform operations comprising:

training a prediction model with sample data, wherein the sample data comprises user data of one of the following users:

(a) first users having historical payment behaviors indicating a frequency of using payment passwords greater than a threshold and having payment failure due to an incorrect or a locked payment password; and

(b) second users having historical payment behaviors indicating a frequency of using payment passwords greater than the threshold, who do not reset their respective payment passwords within a preset time period, and who made a successful payment with their respective payment passwords;

obtaining user information of a user as an input feature to the trained prediction model;

predicting, using the trained prediction model according to a set of determination conditions, whether the user has forgotten a payment password associated with a payment application; and

in response to predicting that the user has forgotten the payment password associated with the payment application and detecting the user logging in the payment application with a login password different from the payment password associated with the payment application, displaying a user interface for directing the user to a payment password resetting interface for resetting the payment password associated with the payment application.

8. The electronic device according to claim 7, wherein the user information comprises one or more pieces of:

identity information, asset information, behavior information of using the payment password associated with the payment application, or management information on the payment password associated with the payment application.

9. The electronic device according to claim 7, wherein the user has historical payment behaviors that satisfy an activeness condition.

10. The electronic device according to claim 7, wherein the set of the determination conditions comprises one of the following:

a payment failure because of inputting an incorrect payment password or a locked payment password, and the payment password associated with the payment application having not been reset since the payment failure;

that the user has not used the payment password associated with the payment application in a first preset time period; or

that the user has not logged in the payment application in a second preset time period.

11. The electronic device according to claim 7, wherein the operations further comprise:

in response to the user selecting an option to reset the payment password associated with the payment application at the user interface, displaying the payment password resetting interface for resetting the payment password associated with the payment application.

12. The electronic device according to claim 7, wherein the operations further comprise:

predicting, by the one or more processors, that the user has not forgotten the payment password associated with the payment application when the user uses a biometric feature to authorize payments.

13. One or more non-transitory computer-readable storage media configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising:

training a prediction model with sample data, wherein the sample data comprises user data of one of the following users:

(a) first users having historical payment behaviors indicating a frequency of using payment passwords greater than a threshold and having payment failure due to an incorrect or a locked payment password; and

(b) second users having historical payment behaviors indicating a frequency of using payment passwords greater than the threshold, who do not reset their respective payment passwords within a preset time period, and who made a successful payment with their respective payment passwords;

obtaining user information of a user as an input feature to the trained prediction model;
predicting, using the trained prediction model according to a set of determination conditions, whether the user has forgotten a payment password associated with a payment application; and
in response to predicting that the user has forgotten the payment password associated with the payment application and detecting the user logging in the payment application with a login password different from the payment password associated with the payment application, displaying a user interface for directing the user to a payment password resetting interface for resetting the payment password associated with the payment application.

14. The one or more non-transitory computer-readable storage media according to claim 13, wherein the user information comprises one or more pieces of:

identity information, asset information, behavior information of using the payment password associated with the payment application, or management information on the payment password associated with the payment application.

15. The one or more non-transitory computer-readable storage media according to claim 13, wherein the user has historical payment behaviors that satisfy an activeness condition.

16. The one or more non-transitory computer-readable storage media according to claim 13, wherein the set of the determination conditions comprises one of the following:

a payment failure because of inputting an incorrect payment password or a locked payment password, and the payment password associated with the payment application having not been reset since the payment failure;

that the user has not used the payment password associated with the payment application in a first preset time period; or

that the user has not logged in the payment application in a second preset time period.

17. The one or more non-transitory computer-readable storage media according to claim 13, wherein the operations further comprise:

in response to the user selecting an option to reset the payment password associated with the payment application at the user interface, displaying the payment password resetting interface for resetting the payment password associated with the payment application.

18. The one or more non-transitory computer-readable storage media according to claim 13, wherein the operations further comprise:

predicting, by the one or more processors, that the user has not forgotten the payment password associated with the payment application when the user uses a biometric feature to authorize payments.