

CLAIMS

What is claimed is:

1. A threshold determining method, comprising:

obtaining predetermined target values respectively corresponding to multiple
5 identification models for identity verification, wherein the predetermined target values
are used to indicate expected target identification capabilities of the identification
models for identity verification; and

determining user service variable values and identity verification thresholds
10 respectively corresponding to the multiple identification models for identity
verification based on the predetermined target values, wherein the user service
variable values are used for classification of active users and inactive users, and the
identity verification thresholds are used by the identification models for identity
verification to exclude users who need strong verification from the inactive users;

wherein the determining user service variable values and identity verification
15 thresholds respectively corresponding to the multiple identification models for
identity verification based on the predetermined target values comprises:

determining the user service variable values and the identity verification
20 thresholds corresponding to the identification models for identity verification by
using an optimization algorithm, in order to minimize differences between the
identity verification thresholds and the predetermined target values corresponding
to the identification models for identity verification, and to maximize a range of
inactive users identified based on the user service variable values.

~~2. The threshold determining method according to claim 1, wherein the
25 determining user service variable values and identity verification thresholds
respectively corresponding to the multiple identification models for identity
verification based on the predetermined target values comprises:~~

~~determining the user service variable values and the identity verification
30 thresholds corresponding to the identification models for identity verification by using
an optimization algorithm, in order to minimize differences between the identity
verification thresholds and the predetermined target values corresponding to the
identification models for identity verification, and to maximize a range of inactive
users identified based on the user service variable values.~~

32. The threshold determining method according to claim 21, wherein the determining the user service variable values and the identity verification thresholds corresponding to the identification models for identity verification by using an optimization algorithm, in order to minimize differences between the identity verification thresholds and the predetermined target values corresponding to the identification models for identity verification, and to maximize a range of inactive users identified based on the user service variable values comprises:

constructing a solution vector by using the user service variable values and the identity verification thresholds respectively corresponding to the multiple identification models for identity verification; and

solving the solution vector based on using maximizing the range of inactive users identified based on the user service variable values as a condition of the optimization algorithm and by using an objective function, of the optimization algorithm, that the identity verification thresholds corresponding to the multiple identification models for identity verification are less than the predetermined target values corresponding to the multiple identification models for identity verification.

43. The threshold determining method according to ~~any one of claims 1 to or 32~~, wherein the identification models for identity verification comprise a misappropriation risk identification model, a sense of security identification model, and/or a password modification motivation abnormality identification model, the misappropriation risk identification model is used to identify the possibility of account misappropriation, the sense of security identification model is used to identify a user demand for the degree of account security, and the password modification motivation abnormality identification model is used to identify the possibility of behavior abnormality of the user when modifying a password.

54. An identity verification method, comprising:

determining, based on user service variable values in response to an identity verification request, whether a user to be verified is an inactive user;

determining an identification result of at least one of multiple identification models for identity verification for the user to be verified when the user to be verified is an inactive user;

determining an identity verification method of the user to be verified based on the identification result of the identification model for identity verification and an identity verification threshold corresponding to the identification model for identity

verification, wherein the identity verification method comprises a weak identity verification method and a strong identity verification method, and the user service variable values and the identity verification threshold are obtained by using the method according to ~~any one of~~ claims 1 ~~to or~~ 23; and

5 performing identity verification on the user to be verified by using the identity verification method.

65. The identity verification method according to claim 54, wherein the identification models for identity verification comprise a misappropriation risk identification model, a sense of security identification model, and/or a password modification motivation abnormality identification model, the misappropriation risk identification model is used to identify the possibility of account misappropriation, the
10 sense of security identification model is used to identify a user demand for the degree of account security, and the password modification motivation abnormality identification model is used to identify the possibility of behavior abnormality of the
15 user when modifying a password.

76. The identity verification method according to claim 65, wherein the determining an identity verification method of the user to be verified based on the identification result of the identification model for identity verification and an identity verification threshold corresponding to the identification model for identity
20 verification comprises:

determining a first identity verification method of the user to be verified based on a first identification result and an identity verification threshold corresponding to the misappropriation risk identification model, determining a second identity verification method of the user to be verified based on a second identification result
25 and an identity verification threshold corresponding to the sense of security identification model, and determining a third identity verification method of the user to be verified based on a third identification result and an identity verification threshold corresponding to the password modification motivation abnormality identification model, wherein the first identification result, the second identification
30 result, and the third identification result are respectively identification results of the misappropriation risk identification model, the sense of security identification model, and the password modification motivation abnormality identification model for the user to be verified; and

determining that the identity verification method of the user to be verified is the

weak identity verification method when each of the first identity verification method, the second identity verification method, and the third identity verification method is the weak identity verification method.

5 ~~87.~~ The identity verification method according to claim ~~76~~, wherein the determining an identity verification method of the user to be verified based on the identification result and a corresponding identity verification threshold further comprises:

10 determining that the identity verification method of the user to be verified is the strong identity verification method when at least one of the first identity verification method, the second identity verification method, and the third identity verification method is the strong identity verification method.

~~98.~~ A threshold determining apparatus, comprising:

15 an acquisition module, configured to obtain predetermined target values respectively corresponding to multiple identification models for identity verification, wherein the predetermined target values are used to indicate expected target identification capabilities of the identification models for identity verification; and

20 a first determining module, configured to determine user service variable values and identity verification thresholds respectively corresponding to the multiple identification models for identity verification based on the predetermined target values, wherein the user service variable values are used for classification of active users and inactive users, and the identity verification thresholds are used by the identification models for identity verification to exclude users who need strong verification from the inactive users~~2~~.

~~wherein the first determining module comprises:~~

25 ~~an optimization submodule, configured to determine the user service variable values and the identity verification thresholds corresponding to the identification models for identity verification by using an optimization algorithm, in order to minimize differences between the identity verification thresholds and the predetermined target values corresponding to the identification models for identity verification, and to maximize a range of inactive users identified based on the user service variable values.~~

30

~~10. The threshold determining apparatus according to claim 9, wherein the first determining module comprises:~~

~~an optimization submodule, configured to determine the user service variable~~

~~values and the identity verification thresholds corresponding to the identification models for identity verification by using an optimization algorithm, in order to minimize differences between the identity verification thresholds and the predetermined target values corresponding to the identification models for identity verification, and to maximize a range of inactive users identified based on the user service variable values.~~

~~119.~~ The threshold determining apparatus according to claim ~~108~~, wherein the optimization submodule comprises:

a construction submodule, configured to construct a solution vector by using the user service variable values and the identity verification thresholds respectively corresponding to the multiple identification models for identity verification; and

a solution submodule, configured to solve the solution vector based on using maximizing the range of inactive users identified based on the user service variable values as a condition of the optimization algorithm and by using an objective function, of the optimization algorithm, that the identity verification thresholds corresponding to the multiple identification models for identity verification are less than the predetermined target values corresponding to the multiple identification models for identity verification.

~~1210.~~ The threshold determining apparatus according to ~~any one of~~ claims ~~9-8 to~~ ~~or 119~~, wherein the identification models for identity verification comprise a misappropriation risk identification model, a sense of security identification model, and/or a password modification motivation abnormality identification model, the misappropriation risk identification model is used to identify the possibility of account misappropriation, the sense of security identification model is used to identify a user demand for the degree of account security, and the password modification motivation abnormality identification model is used to identify the possibility of behavior abnormality of the user when modifying a password.

~~1311.~~ An identity verification apparatus, comprising:

a second determining module, configured to determine, based on user service variable values in response to an identity verification request, whether a user to be verified is an inactive user;

a third determining module, configured to determine an identification result of at least one of multiple identification models for identity verification for the user to be verified when the user to be verified is an inactive user;

a fourth determining module, configured to determine an identity verification method of the user to be verified based on the identification result of the identification model for identity verification and an identity verification threshold corresponding to the identification model for identity verification, wherein the identity verification method comprises a weak identity verification method and a strong identity verification method, and the user service variable values and the identity verification threshold are obtained by using the apparatus according to ~~any one of~~ claims ~~9-8 to or~~ 1412; and

an identity verification module, configured to perform identity verification on the user to be verified by using the identity verification method.

1412. The identity verification apparatus according to claim ~~13~~11, wherein the identification models for identity verification comprise a misappropriation risk identification model, a sense of security identification model, and/or a password modification motivation abnormality identification model, the misappropriation risk identification model is used to identify the possibility of account misappropriation, the sense of security identification model is used to identify a user demand for the degree of account security, and the password modification motivation abnormality identification model is used to identify the possibility of behavior abnormality of the user when modifying a password.

~~15~~13. The identity verification apparatus according to claim 1412, wherein the fourth determining module comprises:

a first determining submodule, configured to determine a first identity verification method of the user to be verified based on a first identification result and an identity verification threshold corresponding to the misappropriation risk identification model, determine a second identity verification method of the user to be verified based on a second identification result and an identity verification threshold corresponding to the sense of security identification model, and determine a third identity verification method of the user to be verified based on a third identification result and an identity verification threshold corresponding to the password modification motivation abnormality identification model, wherein the first identification result, the second identification result, and the third identification result are respectively identification results of the misappropriation risk identification model, the sense of security identification model, and the password modification motivation abnormality identification model for the user to be verified; and

a second determining submodule, configured to determine that the identity verification method of the user to be verified is the weak identity verification method when each of the first identity verification method, the second identity verification method, and the third identity verification method is the weak identity verification method.

~~46~~14. The identity verification apparatus according to claim ~~45~~13, wherein the fourth determining module further comprises:

a third determining submodule, configured to determine that the identity verification method of the user to be verified is the strong identity verification method when at least one of the first identity verification method, the second identity verification method, and the third identity verification method is the strong identity verification method.

~~47~~15. An electronic device, comprising a memory and a processor, wherein the memory is configured to store one or more computer instructions, and the one or more computer instructions are executed by the processor to implement the steps of the method according to any one of claims 1 to ~~8~~7.

~~48~~16. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer instruction, and the computer instruction is executed by a processor to implement the steps of the method according to any one of claims 1 to ~~8~~7.