DEFENSE FILE GENERATION METHOD AND SYSTEM, AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to a defense file generation method and system, and a storage medium.

BACKGROUND

[0002] Transaction payment refusal means that, within a certain period of time after a transaction occurs, a cardholder can apply to an issuing bank to refuse to pay for the transaction for reasons such as unauthorized card usage or a fraudulent transaction. In a payment scenario, after the cardholder trades with a merchant using a bank card, the cardholder may initiate a transaction payment refusal against the transaction.

[0003] After the cardholder initiates a transaction payment refusal, the merchant can initiate a defense to the issuing bank to prove that the transaction that the cardholder refuses to pay for is not an unauthorized transaction or a fraudulent transaction. To perform defense, the merchant needs to generate a defense file against the refused transaction and provide the defense file for the issuing bank. If the issuing bank accepts the defense and acknowledges that the transaction is not an unauthorized transaction or a fraudulent transaction, the issuing bank refunds, to the merchant, funds that the cardholder refuses to pay.

[0004] Currently, the defense file is generated based on a common template, and a data filling rate is low, making it difficult to provide targeted evidence for different transaction scenarios. Consequently, the persuasiveness of the defense file is insufficient, leading to a low success rate for defense.

[0005] Content in the background is merely information known to the inventor, and neither means that the information has entered the public domain before the application date of this disclosure, nor means that the information can become the existing technology of this disclosure.

SUMMARY

[0006] This specification provides a defense file generation method and system, and a storage medium. After a payment refusal notification corresponding to a target transaction is refused, a target defense template applicable to defense of the target transaction is determined from a defense template set based on a transaction feature of the target transaction, and a defense file corresponding to the target transaction is generated based on the target defense template. The defense file generated in this way can provide targeted evidence for different transaction scenarios, increase the persuasiveness of the defense file, and improve a defense success rate.

[0007] According to a first aspect, this specification provides a defense file generation method, including: receiving a payment refusal notification corresponding to a target transaction, where the payment refusal notification indicates that a target user initiates a payment refusal behavior for the target transaction; determining a target defense template applicable to defense of the target transaction from a defense template set based on a transaction feature of the target transaction, where different defense templates in the defense template set respectively correspond to different transaction features; and generating a defense file corresponding to the target transaction based on the target defense template.

[0008] According to a second aspect, this specification further provides a defense file generation system, including: at least one storage medium storing at least one instruction set and used to generate a defense file; and at least one processor that is communicatively connected to the at least one storage medium, where when the defense file generation system runs, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set: receiving a payment refusal notification corresponding to a target transaction, where the payment refusal notification indicates that a target user initiates a payment refusal behavior for the target transaction; determining a target defense template applicable to defense of the target transaction from a defense template set based on a transaction feature of the target transaction, where different defense templates in the defense template set respectively correspond to different transaction features; and generating a defense file corresponding to the target transaction based on the target defense template.

[0009] According to a third aspect, this specification further provides a computer-readable nonvolatile storage medium. The computer-readable nonvolatile storage medium stores at least

one instruction set, and the at least one instruction set is executed by at least one processor to implement the method according to the first aspect.

[0010] Other functions of the defense file generation method provided in this specification are listed in the following descriptions. The creative aspects of the defense file generation method provided in this specification can be fully explained by practice or by using the method, apparatus, and combination described in the following detailed example.

BRIEF DESCRIPTION OF DRAWINGS

[0011] To describe the technical solutions in embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following description are merely some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0012] FIG. 1 is a schematic diagram of a scenario for defending against a transaction payment refusal behavior according to an embodiment of this specification;

[0013] FIG. 2 is a diagram of a hardware structure of a computing system 200 according to an embodiment of this specification;

[0014] FIG. 3 is a flowchart of a defense file generation method according to an embodiment of this specification;

[0015] FIG. 4 is a flowchart of determining a target defense template based on a transaction feature of a target transaction according to an embodiment of this specification;

[0016] FIG. 5 is a schematic diagram of a basic template subset according to an embodiment of this specification;

[0017] FIG. 6 is a schematic diagram of an enhanced template subset according to an embodiment of this specification;

[0018] FIG. 7 is a schematic diagram of generating a defense file based on a target defense template of a transfer type according to an embodiment of this specification; and

[0019] FIG. 8 is a schematic diagram of generating a defense file based on a target defense template of a direct debit type according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0020] Specific application scenarios and requirements of this specification are provided in the following descriptions, so that a person skilled in the art can manufacture and use content of this specification. For the person skilled in the art, various local modifications to the disclosed embodiments are apparent, and the general principles defined herein can be applied to other embodiments and applications without departing from the spirit and scope of this specification. Therefore, this specification is not limited to the shown embodiments, but has a widest scope consistent with that of the claims.

[0021] The terms used herein are only intended to describe a particular example embodiment, but do not impose a limitation. For example, unless otherwise specified in the context, the singular forms "one", "a", and "the" used herein can also include a plural form. When used in this specification, the terms "include", "comprise", and/or "have" indicate/indicates existence of an associated integer, step, operation, element, and/or component, but does not exclude existence of one or more other features, integers, steps, operations, elements, components, and/or groups, or another feature, integer, step, operation, element, component, and/or group can be added to the system/method.

[0022] In consideration of the following descriptions, these and other features of this specification, operations and functions of related components of the structure, and economy of combination and manufacturing of components can be significantly improved. With reference to the accompanying drawings, all of these form a part of this specification. However, it should be clearly understood that the accompanying drawings are merely used for the purpose of illustration and description, and are not intended to limit the scope of this specification. It should be further understood that the accompanying drawings are not drawn to scale.

[0023] The flowcharts used in this specification show operations implemented by the system according to some embodiments of this specification. It should be clearly understood that the operations in the flowcharts may not be sequentially implemented. On the contrary, the operations can be implemented in a reverse sequence or simultaneously. In addition, one or more other operations can be added to the flowchart, and one or more operations can be removed from the flowchart.

[0024] For ease of description, the terms that appear in the following descriptions of this

specification are first explained.

[0025] Term 1: Issuing bank. An issuing bank is a bank or financial institution that issues a bank card. The issuing bank is responsible for providing a bank card for a cardholder and managing accounts and transactions related to the bank card. In this specification, the bank card can include but is not limited to a credit card, a debit card, etc.

[0026] Term 2: Acquiring bank. An acquiring bank is a bank or financial institution that signs an agreement with a merchant and deals with transactions of the merchant. The acquiring bank is responsible for ensuring that the merchant can accept the payment of the cardholder and transfer the transaction amount to an account of the merchant.

[0027] Term 3: Card organization. A card organization is also referred to as a card scheme or a payment network, and is a network and rule system that manages and operates transactions executed using a bank card. The card organization is responsible for making transaction processing rules, providing technical support, and ensuring transaction security.

[0028] Term 4: Cardholder E-Commerce 3.0 (CE3.0) transaction standard. CE3.0 is a payment security standard designed to improve the security and reliability of e-commerce transactions. A transaction that meets the CE3.0 standard typically has the following characteristics: (1) Enhanced authentication, that is, a stronger authentication method such as multi-factor authentication (MFA) is used. (2) Higher transaction transparency, that is, detailed transaction information is provided to better identify and validate a transaction. Therefore, the transaction that meets the CE 3.0 transaction standard is less likely to be an unauthorized transaction.

[0029] Term 5: 3-D Secure 2.0 (3DS2.0) protocol, that is, the 3DS2.0 protocol. The 3DS2.0 protocol is a security protocol used for authentication in an online payment process. The 3DS2.0 protocol allows a merchant and an issuing bank to share more transaction data for more accurate risk assessment. Therefore, a transaction that complies with the 3DS2.0 protocol is less likely to be an unauthorized transaction.

[0030] Term 6: Refund. Refund is a process in which a merchant returns the transaction amount to a user, for example, full refund or partial refund. Generally, if the user has initiated a refund to the merchant for a transaction due to dissatisfaction with a purchased item, it indicates that the user is aware of this transaction. This indicates that the transaction is carried out by the user himself, rather than being an unauthorized transaction or a fraudulent transaction.

[0031] Term 7: Payment refusal. Payment refusal is a behavior that, within a certain period of

time after a transaction occurs, a cardholder can apply to an issuing bank to refuse to pay for the transaction for reasons such as unauthorized card usage or a fraudulent transaction. For example, after a cardholder trades with a merchant using a bank card, if the cardholder believes that the transaction is an unauthorized transaction, the cardholder can apply to an issuing bank for payment refusal against the transaction. If the payment refusal succeeds, funds involved in the transaction are returned to the bank card.

[0032] Term 8: Defense. Defense is a behavior that a merchant defends a transaction after receiving a payment refusal notification. When defending, the merchant needs to provide evidence for the transaction involved in the payment refusal notification, to prove to the issuing bank that the transaction is carried out by a cardholder himself. If the defense is accepted by the issuing bank, the merchant does not need to return the funds involved in the payment refusal notification.

[0033] The following describes an application scenario of this specification.

[0034] The technical solutions provided in this specification are applicable to a scenario of defending against a transaction payment refusal behavior. In this scenario, it is assumed that a target user pays for a target transaction using a bank card through a payment system. Within a certain period of time after payment, if the target user believes that the target transaction is not of his will, for example, is an unauthorized transaction or a fraudulent transaction, the target user can initiate a payment refusal behavior to an issuing bank corresponding to the bank card. The issuing bank can send a payment refusal notification to the payment system through a card organization. In this case, the payment system can defend against the payment refusal behavior of the target user, to prove that the target transaction is not an unauthorized transaction or a fraudulent transaction.

[0035] This specification provides a defense file generation method, and the defense file generation method can be performed by a payment system. After receiving a payment refusal notification corresponding to a target transaction, the payment system can determine a target defense template applicable to defense of the target transaction from a defense template set based on a transaction feature of the target transaction, and generate a defense file corresponding to the target transaction based on the target defense template. The defense file generated in this way can provide targeted evidence for different transaction scenarios, increase the persuasiveness of the defense file, and improve a defense success rate.

[0036] FIG. 1 is a schematic diagram of a scenario for defending against a transaction payment refusal behavior according to an embodiment of this specification. As shown in FIG. 1, the

application scenario 100 can include a target user 11, an issuing bank 12, a card organization 13, and a payment system 14.

[0037] The payment system 14 can be a service system that provides a payment service. In some embodiments, the payment system 14 can bind a bank card provided by the issuing bank 12, and allow the user to use the bank card in the payment system 14 to perform operations such as payment, transfer, etc. In this case, the payment system 14 can also be referred to as a wallet system. In some embodiments, the payment system 14 can provide more other services in addition to a service similar to an electronic wallet. A payment service provided by the payment system 14 can be a domestic payment service, or can be a cross-border payment service. This is not limited in this specification.

[0038] As shown in FIG. 1, when the target user 11 believes that a target transaction paid via a bank card is an unauthorized transaction or a fraudulent transaction, the target user 11 can initiate a payment refusal behavior for the target transaction. After the target user 11 initiates the payment refusal behavior for the target transaction, the issuing bank 12 receives a payment refusal request from the target user 11, and sends a payment refusal notification corresponding to the target transaction to the payment system 14 through the card organization 13 based on the payment refusal request. After receiving the payment refusal notification, the payment system 14 can generate a defense file corresponding to the target transaction. The payment system 14 can provide some defense evidence in the defense file to prove that the target transaction is not an unauthorized transaction or a fraudulent transaction. Further, the payment system 14 sends the defense file to the issuing bank 12 through the card organization 13. When the issuing bank 12 acknowledges content of the defense file, the payment system 14 does not need to be liable for compensating for the target transaction.

[0039] The payment system 14 can be a computing system that has a specific computing capability. The payment system 14 can include one or more computing systems. The defense file generation method provided in this specification can be performed by the payment system 14. The payment system 14 can store data or instructions for performing the defense file generation method described in this specification, and can execute or be configured to execute the data or the instructions. In some embodiments, the payment system 14 can include a hardware device with a data information processing function and a program required for driving the hardware device to work.

[0040] It should be understood that the payment system 14 can run on a separate server, or can run on a device such as a server group, a distributed server, or a cloud server.

[0041] FIG. 2 is a diagram of a hardware structure of a computing system 200 according to an embodiment of this specification. The computing system 200 can be used as the payment system 14 in FIG. 1 to perform the defense file generation method described in this specification.

[0042] As shown in FIG. 2, the computing system 200 can include at least one storage medium 230 and at least one processor 220. In some embodiments, the computing system 200 can further include a communication port 250 and an internal communication bus 210. The computing system 200 can further include an I/O component 260.

[0043] The internal communication bus 210 can be connected to different system components. For example, the internal communication bus 210 can be connected to the storage medium 230, the processor 220, the communication port 250, the I/O component 260, etc.

[0044] The I/O component 260 supports input/output between the computing system 200 and another component.

[0045] The communication port 250 is used for data communication between the computing system 200 and the outside. For example, the communication port 250 can be used for data communication between the computing system 200 and a network. The communication port 250 can be a wired communication port, or can be a wireless communication port.

[0046] The storage medium 230 can include a data storage apparatus. The data storage apparatus can be a non-transitory storage medium, or can be a transitory storage medium. For example, the data storage apparatus can include one or more of a disk 232, a read-only storage medium (ROM) 234, or a random access storage medium (RAM) 236. The storage medium 230 further includes at least one instruction set stored in the data storage apparatus. The instruction set can include computer program code. The computer program code can include a program, a routine, an object, a component, a data structure, a process, a module, etc.

[0047] The at least one processor 220 can be communicatively connected to the at least one storage medium 230. When the computing system 200 runs, the at least one processor 220 reads the at least one instruction set, and performs, based on an indication of the at least one instruction set, the defense file generation method provided in this specification. The processor 220 can perform steps included in the defense file generation method. The processor 220 can be in a form of one or more processors. In some embodiments, the processor 220 can include one or more

hardware processors, for example, a microcontroller, a microprocessor, a reduced instruction set computer (RISC), an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a central processing unit (CPU), a graphics processing unit (GPU), a physical processing unit (PPU), a microcontroller unit, a digital signal processor (DSP), a field programmable gate array (FPGA), an advanced RISC machine (ARM), a programmable logic device (PLD), any circuit, processor, etc. that can perform one or more functions, or any combination thereof.

[0048] For only the purpose of description, only one processor 220 is shown in the computing system 200 in the accompanying drawings. However, it should be noted that, the computing system 200 in this specification can further include a plurality of processors. Therefore, the operations and/or method steps disclosed in this specification can be performed by one processor, or can be jointly performed by a plurality of processors. For example, if the processor 220 in the computing system 200 in this specification performs step A and step B, it should be understood as that step A and step B can be jointly or respectively performed by two different processors 220 (for example, a first processor performs step A, and a second processor performs step B, or a first processor and a second processor jointly perform step A and step B).

[0049] FIG. 3 is a flowchart of a defense file generation method according to an embodiment of this specification. As described above, a payment system 14 can perform the defense file generation method in this specification.

[0050] As shown in FIG. 3, the defense file generation method can include the following steps.

[0051] S310: Receive a payment refusal notification corresponding to a target transaction, where the payment refusal notification indicates that a target user initiates a payment refusal behavior for the target transaction.

[0052] In some embodiments, the target user has carried out, at a historical moment, a target transaction with a merchant via a card organization using a bank card issued by an issuing bank. The payment refusal behavior is a behavior that after the target transaction occurs, if the target user believes that the target transaction is not of his will, for example, the target transaction is carried out under circumstances that the bank card is fraudulently charged or used for fraudulent transactions, the target user initiates a request to the issuing bank to refuse to pay funds involved in the target transaction and requests a refund.

[0053] In this specification, for the target user, the payment system is equivalent to a wallet

system. When the target user uses the payment system for transactions (such as transfer, shopping, or signing a direct debit agreement), it can be considered as that the target user first uses a bank card to trade with the payment system, and pays funds to the payment system. Then, the payment system trades with an actual transaction counterparty of the target user to complete a transaction process. In this case, the payment system is used to generate a transaction order and collect funds from the user. For the issuing bank, the payment system can be considered as a merchant. Therefore, the payment system in this specification can be used as a defense subject (the merchant) to receive the payment refusal notification from the issuing bank and to send a defense file to the issuing bank in response to the payment refusal notification to defend against payment refusal.

[0054] It should be noted that, in the above-mentioned transaction process, the target transaction refers to a step in which the target user first trades with the payment system using the bank card, and pays the funds to the payment system.

[0055] In some embodiments, after the target user initiates the payment refusal behavior to the issuing bank, the issuing bank generates the payment refusal notification based on the target transaction, and delivers the payment refusal notification to the payment system via the card organization. After receiving the payment refusal notification corresponding to the target transaction, the payment system can defend to the issuing bank against the payment refusal behavior of the target user based on the payment refusal notification, to prove that the target transaction is not carried out under circumstances that the bank card is fraudulently charged or used for fraudulent transactions.

[0056] In some embodiments, the payment refusal notification can include related information of the target transaction, including but not limited to user information of the target user, a transaction order number, a bank transaction reference number, a bank card number, transaction time, a transaction amount, etc.

[0057] S320: Determine a target defense template applicable to defense of the target transaction from a defense template set based on a transaction feature of the target transaction, where different defense templates in the defense template set respectively correspond to different transaction features.

[0058] In some embodiments, the transaction feature includes a defense difficulty and a transaction type. A defense difficulty of the target transaction is obtained based on at least one of the following: whether the target transaction meets a predetermined transaction security standard;

whether the target transaction complies with a predetermined transaction security protocol; or whether an execution process of the target transaction includes a refund step.

[0059] In some embodiments, the transaction security standard can be the CE3.0 standard. A transaction that meets the CE3.0 transaction standard is less likely to be an unauthorized transaction, and has a high defense success rate. Therefore, when the target transaction meets the CE3.0 standard, the payment system can determine that the defense difficulty of the target transaction is lower than a predetermined difficulty.

[0060] In some embodiments, the transaction security protocol can be the 3DS2.0 protocol. A transaction that complies with the 3DS2.0 protocol is also less likely to be an unauthorized transaction, and also has a high defense success rate. Therefore, when the target transaction complies with the 3DS2.0 protocol, the payment system can determine that the defense difficulty of the target transaction is lower than the predetermined difficulty.

[0061] In some embodiments, when the target user has initiated a refund for the target transaction, the target transaction can be considered as a transaction carried out by the target user himself, and is not an unauthorized transaction or a fraudulent transaction, and has a high defense success rate. Therefore, when the execution process of the target transaction includes the refund step, the payment system can determine that the defense difficulty of the target transaction is lower than the predetermined difficulty.

[0062] In some embodiments, when the target transaction does not meet the predetermined transaction security standard and does not comply with the predetermined transaction security protocol, if the target transaction does not include the refund step, it is difficult to prove, by using simple evidence, that the target transaction is carried out by the target user himself, and a defense success rate of the target transaction is low. Therefore, in this case, the payment system can determine that the defense difficulty of the target transaction is higher than the predetermined difficulty.

[0063] In some embodiments, a transaction type of the target transaction can include an offline payment type, a network shopping type, a transfer type (also referred to as P2P), a direct debit type, etc. The transaction type can be determined based on a transaction product code corresponding to the target transaction. For example, the payment system can obtain the transaction product code based on a transaction order number corresponding to the target transaction, and each transaction product code corresponds to one transaction type. The transaction type of the target transaction

can be confirmed based on the transaction product code obtained by the payment system.

[0064] In some embodiments, the defense template set includes a basic template subset and an enhanced template subset. Defense templates in the enhanced template subset cover more defense dimensions than defense templates in the basic template subset. The defense template in the enhanced template subset is applicable to a scenario with a relatively high defense difficulty, and the defense template in the basic template subset is applicable to a scenario with a relatively low defense difficulty. Therefore, the payment system can first determine, based on the defense difficulty of the target transaction, whether to determine the target defense template from the basic template subset or from the enhanced template subset.

[0065] In some embodiments, when at least one of the following is met: the target transaction meets the predetermined transaction security standard, a target defense template that complies with the predetermined transaction security protocol, or the execution process of the target transaction includes the refund step, it can be determined that the defense difficulty of the target transaction is lower than the predetermined difficulty.

[0066] In some embodiments, when the target transaction does not meet the predetermined transaction security standard and does not comply with the predetermined transaction security protocol, and the execution process of the target transaction does not include the refund step, it can be determined that the defense difficulty of the target transaction is higher than the predetermined difficulty.

[0067] FIG. 4 is a flowchart of determining a target defense template based on a transaction feature of a target transaction according to an embodiment of this specification.

[0068] In some embodiments, as shown in FIG. 4, when the defense difficulty of the target transaction is lower than the predetermined difficulty, the payment system can determine the target defense template applicable to defense of the target transaction from the basic template subset. The payment system can determine the target defense template applicable to defense of the target transaction from the enhanced template subset based on the transaction type of the target transaction when the defense difficulty of the target transaction is higher than the predetermined difficulty.

[0069] A corresponding template subset is determined based on the defense difficulty of the target transaction, and the target defense template is obtained from the corresponding template subset, so that the generated defense file can be more targeted, thereby improving a defense success

rate.

[0070] In some embodiments, the defense dimensions covered by the defense templates in the basic template subset include a first defense dimension. The defense dimensions covered by the defense templates in the enhanced template subset include the first defense dimension, and further include at least one of a second defense dimension or a third defense dimension.

[0071] Transaction data of the target transaction is used as defense evidence in the first defense dimension, historical transaction data of the target user is used as defense evidence in the second defense dimension, and personalized defense information related to the transaction type of the target transaction is used as defense evidence in the third defense dimension.

[0072] FIG. 5 is a schematic diagram of a basic template subset according to an embodiment of this specification.

[0073] The basic template subset includes a fixed template, and the fixed template is used for a target transaction with a defense difficulty lower than the predetermined difficulty. For example, when at least one of the following is met: the target transaction meets the predetermined transaction security standard, the target transaction complies with the predetermined transaction security protocol, or the execution process of the target transaction includes the refund step, it is determined that the defense difficulty of the target transaction is lower than the predetermined difficulty, and the fixed template can be used to generate the defense file.

[0074] As shown in FIG. 5, the fixed template includes a first template part corresponding to the first defense dimension and used to populate the transaction data of the target transaction. The fixed template can further include description text, and the description text can respond to a defense notification. For example, the description text can include a title, an identifier of a recipient, situation description text. etc.

[0075] In some embodiments, the first template part can include a first defense dimension table. The first defense dimension table can be used to populate the transaction data of the target transaction. For example, Table 1 shows a possible first defense dimension table.

Table 1

Details of a disputed transaction:
1. Transaction detail:

Details of a disputed transaction:		
Bank transaction reference number	Transaction time	Transaction amount
Identifier of the buyer	Product description	Device number
Delivery address	Identifier of the counterparty	IP address of the buyer

[0076] In some embodiments, the payment system can obtain the transaction data of the target transaction based on the transaction order number of the target transaction provided in the payment refusal notification. As an example, the transaction data of the target transaction can include at least one of the following: a bank transaction reference number, transaction time, a transaction amount, an identifier of a buyer, an IP address of the buyer, a product description, a device number, a delivery address, or an identifier of a counterparty.

[0077] In some embodiments, the payment system can use the transaction data of the target transaction as defense evidence, populate the transaction data into the first defense dimension table, and add, into situation description text, description text indicating that the target transaction meets the predetermined transaction security standard/complies with the predetermined transaction security protocol/the execution process of the target transaction includes the refund step. Then, the payment system can generate the defense file based on the fixed template.

[0078] The payment system provides the issuing bank with the transaction data of the target transaction through the defense file, and indicates that the target transaction meets the predetermined transaction security standard/complies with the predetermined transaction security protocol/the execution process of the target transaction includes the refund step, so that a defense for the target transaction has a relatively high defense success rate.

[0079] FIG. 6 is a schematic diagram of an enhanced template subset according to an embodiment of this specification.

[0080] As shown in FIG. 6, the enhanced template subset includes defense templates respectively corresponding to a plurality of transaction types. The payment system can use a

defense template corresponding to the transaction type of the target transaction in the enhanced template subset as the target defense template.

[0081] For example, if the target transaction corresponds to transaction type A, the payment system can use a defense template corresponding to transaction type A in the enhanced template subset as the target defense template. If the target transaction corresponds to transaction type B, the payment system can use a defense template corresponding to transaction type B in the enhanced template subset as the target defense template. If the target transaction corresponds to transaction type C, the payment system can use a defense template corresponding to transaction type C in the enhanced template subset as the target defense template. The defense templates corresponding to transaction type A and transaction type B include three defense dimensions: a first defense dimension, a second defense dimension, and a third defense dimension. The defense template corresponding to transaction type C includes two defense dimensions: a first defense dimension and a second defense dimension.

[0082] In some embodiments, for example, the transaction type of the target transaction is a transfer type, and the target defense template includes: a first template part, corresponding to the first defense dimension and used to populate the transaction data of the target transaction; a second template part, corresponding to the second defense dimension and used to populate the historical transaction data of the target user; and a third template part, corresponding to the third defense dimension and used to populate the personalized defense information, where the personalized defense information includes first user information corresponding to the target user and second user information corresponding to another participant of the target transaction.

[0083] In some embodiments, the target defense template can further include description text. The description text can respond to a defense notification. For example, the description text can include a title, an identifier of a recipient, situation description text, etc.

[0084] In some embodiments, the first template part can include a first defense dimension table. The first defense dimension table can be used to populate the transaction data of the target transaction. For example, the first defense dimension table shown in Table 1 can be used as a first defense dimension table corresponding to the first template part in the target defense template of the transfer type.

[0085] In some embodiments, for a method of obtaining the transaction data of the target transaction, reference can be made to the method of obtaining the transaction data of the target

transaction in the above-mentioned fixed template, and details are not described herein again.

[0086] In some embodiments, the second template part can include a second defense dimension table. The second defense dimension table can be used to populate the historical transaction data of the target user.

[0087] In some embodiments, the historical transaction data of the target user can include at least one of the following: transaction data of at least one historical transaction that is carried out by the target user through the payment system using the same bank card as that used in the target transaction and that is not defended, time of the first transaction carried out by the target user through the payment system, time of the last transaction carried out by the target user through the payment system, a quantity of historical transactions carried out by the target user, time of the first transaction carried out through the payment system using the bank card corresponding to the target transaction, time of the last transaction carried out through the payment system using the bank card corresponding to the target transaction, a quantity of historical transactions carried out using the bank card corresponding to the target transaction, time of the first transaction carried out by a device corresponding to the target transaction through the payment system, time of the last transaction carried out by the device corresponding to the target transaction through the payment system, or a quantity of historical transactions carried out by the device corresponding to the target transaction.

[0088] When the payment system uses historical transactions from 120 days to 365 days before the target transaction as defense evidence, the payment system can better prove that the target transaction is carried out by the target user rather than an unauthorized transaction or a fraudulent transaction. Therefore, when obtaining transaction data of at least one historical transaction, the payment system can preferentially obtain historical transactions from 120 days to 365 days before the target transaction. When a matched historical transaction cannot be obtained in this time interval, the payment system obtains historical transactions from another time interval. It should be noted that transaction data of the historical transaction is similar to the transaction data of the target transaction, and details are not described herein again.

[0089] In some embodiments, the second defense dimension table can include two parts. A first part of the table is used to populate the transaction data of the historical transaction, and a second part of the table is used to populate remaining data. As an example, Table 2 shows a possible first part of the table.

Table 2

Details of an undisputed transaction:		
1. Transaction detail:		
Bank transaction reference number	Transaction time	Transaction amount
Identifier of the buyer	Product description	Device number
Delivery address	Identifier of the counterparty	IP address of the buyer
2. Transaction detail:		
Bank transaction reference number	Transaction time	Transaction amount
Identifier of the buyer	Product description	Device number
Delivery address	Identifier of the counterparty	IP address of the buyer

[0090] Table 2 shows the first part of the table using transaction data of two historical transactions as defense evidence. In this specification, no limitation is imposed on how much transaction data of historical transactions is used as defense evidence, and the first part of the table can be expanded or reduced based on a specific quantity of historical transactions. The payment system uses an undisputed historical transaction corresponding to the target transaction as defense evidence, which can prove that the target user has carried out a plurality of transactions using the bank card corresponding to the target transaction within a historical period of time, to help prove that the bank card is used by the target user himself and there is a relatively low probability of an unauthorized transaction and a fraudulent transaction, thereby improving a defense success rate.

[0091] As an example, Table 3 shows a possible second part of the table.

Table 3

Details of a purchase record:			
	Time of the first transaction	Time of the last transaction	Total quantity of transactions
Bank card number:			
Device number:			
Buyer account:			
The above-mentioned information includes an identifier of a buyer, a device number, and a bank card number. At least two of the above-mentioned information match each other in disputed transactions and previously undisputed transactions.			

[0092] In the second part of the table, in addition to populating in the time of the first transaction carried out by the target user through the payment system, the time of the last transaction carried out by the target user through the payment system, the quantity of historical transactions carried out by the target user, the time of the first transaction carried out through the payment system using the bank card corresponding to the target transaction, the time of the last transaction carried out through the payment system using the bank card corresponding to the target transaction, the quantity of historical transactions carried out using the bank card corresponding to the target transaction, the time of the first transaction carried out by the device corresponding to the target transaction through the payment system, the time of the last transaction carried out by the device corresponding to the target transaction through the payment system, and the quantity of historical transactions carried out by the device corresponding to the target transaction, the payment system can further fill summary text in the first table part and the second table part. For example, the summary text can be "The above-mentioned information includes an identifier of a buyer, a device number, and a bank card number. At least two of the above-mentioned information match each other in disputed transactions and previously undisputed transactions." shown in Table 3. It is further described that the target user has carried out a plurality of transactions using the bank card corresponding to the target transaction within a historical period of time, and this helps

prove that the bank card is used by the target user himself and there is a relatively low probability of an unauthorized transaction and a fraudulent transaction, thereby improving a defense success rate.

[0093] In some embodiments, the third template part can include a third defense dimension table. The third defense dimension table can be used to populate personalized defense information related to the transfer type.

[0094] In some embodiments, for the transfer type, the personalized defense information can be user information of both parties of the transaction, which is used to describe an interpersonal relationship between the two parties to prove that there is a relatively low probability of an unauthorized transaction or a fraudulent transaction between both parties of the transaction. As an example, the user information can include a usual place of residence, a geographic area to which the user belongs, an identifier, a delivery address, etc. The payment system can obtain the first user information of the target user from historical transactions of the target user. For example, the payment system can obtain the delivery address, the identifier, the geographic area to which the user belongs, the usual place of residence, etc. based on logistics information that the target user frequently uses in historical transactions. Second user information corresponding to another participant (counterparty) of the target transaction can also be obtained in a similar manner, and details are not described herein again.

[0095] As an example, Table 4 shows a possible third defense dimension table.

Table 4

Details of a transfer transaction			
Usual place of residence of the counterparty		Usual place of residence of the target user	
Identifier of the counterparty		Identifier of the target user	
Geographic area to which the counterparty belongs		Geographic area to which the target user belongs	
Delivery address 1 of the counterparty		Delivery address 1 of the target user	
Delivery address 2 of the		Delivery address 2 of the	

Details of a transfer transaction			
counterparty		target user	

[0096] In some embodiments, the target defense template can further include summary text. For example, the summary text includes text, signatures, etc. summarizing the above-mentioned defense evidence.

[0097] In some embodiments, for example, transaction type B of the target transaction is a direct debit type, and the target defense template includes: a first template part, corresponding to the first defense dimension and used to populate the transaction data of the target transaction; a second template part, corresponding to the second defense dimension and used to populate the historical transaction data of the target user; and a third template part, corresponding to the third defense dimension and used to populate the personalized defense information, where the personalized defense information includes related information of direct debit subscription corresponding to the target transaction.

[0098] In some embodiments, the first template part corresponding to the direct debit type is similar to the first template part corresponding to the transfer type, and details are not described herein again.

[0099] In some embodiments, in the second template part corresponding to the direct debit type, content populated in the first table part and a table format of the first table part are similar to those of the first table part corresponding to the transfer type, and related data of the device number are omitted in a table format of the second table part in comparison with the second table part corresponding to the transfer type, and correspondingly, populated content does not include the related data of the device number.

[0100] In some embodiments, the third template part corresponding to the direct debit type also includes the third defense dimension table. The third defense dimension table can be used to populate personalized defense information related to the direct debit type.

[0101] In some embodiments, for the direct debit type, the personalized defense information can be related information of the direct debit subscription, and is used to indicate that the target transaction occurs after the target user made the direct debit subscription at a historical moment. After the direct debit subscription at the historical moment is proved to be carried out by the target user, it can prove that the target transaction is not an unauthorized transaction or a fraudulent

transaction.

[0102] For example, if the target user has carried out a plurality of direct debit transactions through the payment system after signing a direct debit agreement at the historical moment, and a payment refusal behavior is initiated for none of these direct debit transactions, it can prove that the direct debit subscription is carried out by the target user himself, and further, it is proved that the target transaction is not an unauthorized transaction or a fraudulent transaction.

[0103] The payment system can obtain related information of the direct debit subscription from historical transactions of the target user. For example, the payment system can obtain a direct debit product that the target user subscribes to at the historical moment, subscription time, a subscription device number, time of paying for a direct debit transaction on a subscription device for the first time, time of paying for the direct debit transaction on the subscription device for the last time, a quantity of payment transactions of the subscription device, a network address at the time of subscription, etc.

[0104] As an example, Table 5 shows a possible third defense dimension table.

Table 5

Details of direct debit subscription			
Direct debit product:	Time of the first transaction	Time of the last transaction	Total quantity of transactions
Subscription time:	-	-	-
Subscription device number:			
Network address at the time of subscription:	-	-	-

[0105] S330: Generate a defense file corresponding to the target transaction based on the target defense template.

[0106] Here, a process of generating the defense file corresponding to the target transaction based on the target defense template is described by using an example in which the transaction type of the target transaction is the transfer type and the direct debit type.

[0107] FIG. 7 is a schematic diagram of generating a defense file based on a target defense

template of a transfer type according to an embodiment of this specification.

[0108] In some embodiments, with reference to the example of the target defense template in FIG. 7 and S320, the payment system can populate data corresponding to the transfer type into a corresponding template part (e.g., a table) to obtain a file part corresponding to each template part. Then, the payment system generates a defense file of the transfer type based on obtained file parts.

[0109] For example, the payment system can first obtain the transaction data of the target transaction, and populate the transaction data of the target transaction into the first template part to obtain a first file part. Then, the payment system obtains the historical transaction data of the target user, and populates the historical transaction data into the second template part to obtain a second file part. Then, the payment system obtains the first user information corresponding to the target user and the second user information corresponding to the another participant of the target transaction, and populates the first user information and the second user information into the third template part to obtain a third file part. Finally, the payment system generates the defense file based on the first file part, the second file part, and the third file part.

[0110] FIG. 8 is a schematic diagram of generating a defense file based on a target defense template of a direct debit type according to an embodiment of this specification.

[0111] In some embodiments, as shown in FIG. 8, a process in which the payment system generates a defense file of the direct debit type is similar to a process of generating the defense file of the transfer type. For example, the payment system can first obtain the transaction data of the target transaction, and populate the transaction data of the target transaction into the first template part to obtain a first file part. Then, the payment system obtains the historical transaction data of the target user, and populates the historical transaction data into the second template part to obtain a second file part. Then, the payment system obtains related information of direct debit subscription corresponding to the target transaction, and populates the related information of the direct debit subscription into the third template part to obtain a third file part. Finally, the payment system generates the defense file based on the first file part, the second file part, and the third file part.

[0112] It should be noted that the defense file generated by the payment system can be stored in a manner of a text document, a portable document format (PDF), an email, an extensible markup language (XML), etc.

[0113] In conclusion, in the defense file generation method and system provided in this

specification, after the payment refusal notification corresponding to the target transaction is received, the target defense template applicable to defense of the target transaction is determined from the defense template set based on the transaction feature of the target transaction, and the defense file corresponding to the target transaction is generated based on the target defense template. The defense file generated in this way can provide targeted evidence for different transaction scenarios, increase the persuasiveness of the defense file, and improve a defense success rate.

[0114] In this specification, the target defense template is described in simplified Chinese as an example. However, in actual application, a working language of the issuing bank may be another language, such as English, Japanese, or Traditional Chinese.

[0115] In some embodiments, defense template sets for different languages can be set in advance based on the working language of the issuing bank. The payment system can determine the target defense template from a defense template set of the corresponding language based on the working language of the issuing bank.

[0116] It should be noted that user data obtained in this specification is authorized by the user, and does not relate to user privacy.

[0117] Another aspect of this specification provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set used to generate a defense file. When the at least one instruction set is executed by a processor, the at least one instruction set instructs the processor to implement steps of the defense file generation method described in this specification. In some possible implementations, aspects of this specification can further be implemented in a form of a program product, including program code. When the program product runs on a computing system 200, the program code is used to enable the computing system 200 to perform steps of the defense file generation method described in this specification. The program product used to implement the above-mentioned method can be a portable compact disk read-only memory (CD-ROM) including program code, and can run on the computing system 200. However, the program product in this specification is not limited thereto. In this specification, a readable storage medium can be any tangible medium that includes or stores a program, and the program can be used by or in combination with an instruction execution system. The program product can be any combination of one or more readable media. The readable medium can be a readable signal medium or a readable storage medium. For example,

the readable storage medium can be but is not limited to an electrical system, apparatus, or device, a magnetic system, apparatus, or device, an optical system, apparatus, or device, an electromagnetic system, apparatus, or device, an infrared system, apparatus, or device, or a semiconductor system, apparatus, or device, or any combination thereof. More specific examples of the readable storage medium include: a portable disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage component, a magnetic storage component, or any proper combination thereof. The computer-readable storage medium can include a data signal propagated in a baseband as a part of a carrier, and carries readable program code. The data signal propagated in such a way can be in a plurality of forms, and includes but is not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium can further be any readable medium other than the readable storage medium, and the readable medium can be used to send, propagate, or transmit a program used by or in combination with an instruction execution system, apparatus, or component. The program code included in the readable storage medium can be transmitted in any proper medium, including but not limited to a wireless medium, a wired medium, an optical cable, an RF medium, et., or any proper combination thereof. The program code for performing operations in this specification can be written in any combination of one or more program design languages. The program design language includes an object-oriented program design language, such as Java or C++, and further includes a conventional procedural program design language, such as a "C" language or a similar program design language. The program code can be completely executed on the computing system 200, partially executed on the computing system 200, executed as an independent software package, partially executed on the computing system 200 and partially executed on a remote computing device, or completely executed on a remote computing device.

[0118] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular order or consecutive order to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

[0119] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the above-mentioned detailed disclosure can be presented only in an example manner, and can impose no limitation. Although it is not explicitly stated herein, a person skilled in the art can understand that the requirements of this specification include various proper changes, improvements, and modifications to the embodiments. These changes, improvements, and modifications are intended to be proposed in this specification, and fall within the spirit and scope of the example embodiments of this specification.

[0120] In addition, some terms in this specification are used to describe the embodiments of this specification. For example, "one embodiment", "an embodiment", and/or "some embodiments" mean that particular features, structures, or characteristics described with reference to the embodiments can be included in at least one embodiment of this specification. Therefore, it can be emphasized and understood that two or more of "an embodiment", "one embodiment", or "alternative embodiments" referred in parts of this specification do not necessarily indicate the same embodiment. In addition, particular features, structures, or characteristics can be properly combined in one or more embodiments of this specification.

[0121] It should be understood that in the above-mentioned descriptions of the embodiments of this specification, to help understand a feature, for the purpose of simplifying this specification, various features are combined in a single embodiment, accompanying drawing, or description thereof in this specification. However, this does not mean that the combination of these features is necessary. It is entirely possible for a person skilled in the art to mark some devices and understand the devices as separate embodiments when reading this specification. In other words, the embodiments in this specification can also be understood as an integration of a plurality of secondary embodiments. Content of each secondary embodiment is also true when features are less than all features in one of the above-mentioned disclosed embodiments.

[0122] Each patent, patent application, publication of a patent application, and other materials, for example, articles, books, instructions, publications, documents, and products, that are cited in this specification and that are other than any document that is inconsistent or conflict with this document or that imposes limiting impact on the widest scope of the claims can be incorporated herein by reference and used for all purposes now or later associated with this document. In addition, the term in this document shall prevail when there is any inconsistency or conflict between the description, definition and/or use of a related term in any material and the description,

definition and/or use of a related term in this document.

[0123] Finally, it should be understood that the principles of the implementation solutions of this specification are described in the implementation solutions of the application disclosed in this specification. Other modified embodiments also fall within the scope of this specification. Therefore, the embodiments disclosed in this specification are merely examples and not limitations. A person skilled in the art can use an alternative configuration according to the embodiments of this specification to implement the application in this specification. Therefore, the embodiments of this specification are not limited to the embodiments accurately described in the application.

CLAIMS

What is claimed is:

1. A defense file generation method, comprising:

receiving a payment refusal notification corresponding to a target transaction, wherein the payment refusal notification indicates that a target user initiates a payment refusal behavior for the target transaction;

determining a target defense template applicable to defense of the target transaction from a defense template set based on a transaction feature of the target transaction, wherein different defense templates in the defense template set respectively correspond to different transaction features; and

generating a defense file corresponding to the target transaction based on the target defense template.

2. The method according to claim 1, wherein the transaction feature comprises a defense difficulty and a transaction type, the defense template set comprises a basic template subset and an enhanced template subset, and defense templates in the enhanced template subset cover more defense dimensions than defense templates in the basic template subset; and

the determining a target defense template applicable to defense of the target transaction from a defense template set based on a transaction feature of the target transaction comprises:

determining the target defense template applicable to defense of the target transaction from the enhanced template subset based on a transaction type of the target transaction when a defense difficulty of the target transaction is higher than a predetermined difficulty.

3. The method according to claim 2, wherein the enhanced template subset comprises defense templates respectively corresponding to a plurality of transaction types, and the determining the target defense template applicable to defense of the target transaction from the enhanced template subset based on a transaction type of the target transaction comprises:

using a defense template corresponding to the transaction type of the target transaction in the enhanced template subset as the target defense template.

4. The method according to claim 2, wherein the defense dimensions covered by the defense templates in the basic template subset comprise a first defense dimension; and

the defense dimensions covered by the defense templates in the enhanced template subset

comprise the first defense dimension, and further comprise at least one of a second defense dimension or a third defense dimension, wherein

transaction data of the target transaction is used as defense evidence in the first defense dimension;

historical transaction data of the target user is used as defense evidence in the second defense dimension; and

personalized defense information related to the transaction type of the target transaction is used as defense evidence in the third defense dimension.

5. The method according to claim 4, wherein the transaction type of the target transaction is a transfer type, and the target defense template comprises:

a first template part, corresponding to the first defense dimension, and used to populate the transaction data of the target transaction;

a second template part, corresponding to the second defense dimension, and used to populate the historical transaction data of the target user; and

a third template part, corresponding to the third defense dimension, and used to populate the personalized defense information, wherein the personalized defense information comprises first user information corresponding to the target user and second user information corresponding to another participant of the target transaction.

6. The method according to claim 5, wherein the generating a defense file corresponding to the target transaction based on the target defense template comprises:

obtaining the transaction data of the target transaction, and populating the transaction data of the target transaction into the first template part to obtain a first file part;

obtaining the historical transaction data of the target user, and populating the historical transaction data into the second template part to obtain a second file part;

obtaining the first user information corresponding to the target user and the second user information corresponding to the another participant of the target transaction, and populating the first user information and the second user information into the third template part to obtain a third file part; and

generating the defense file based on the first file part, the second file part, and the third file part.

7. The method according to claim 4, wherein the transaction type of the target transaction is

a direct debit type, and the target defense template comprises:

a first template part, corresponding to the first defense dimension, and used to populate the transaction data of the target transaction;

a second template part, corresponding to the second defense dimension, and used to populate the historical transaction data of the target user; and

a third template part, corresponding to the third defense dimension, and used to populate the personalized defense information, wherein the personalized defense information comprises related information of direct debit subscription corresponding to the target transaction.

8. The method according to claim 7, wherein the generating a defense file corresponding to the target transaction based on the target defense template comprises:

obtaining the transaction data of the target transaction, and populating the transaction data of the target transaction into the first template part to obtain a first file part;

obtaining the historical transaction data of the target user, and populating the historical transaction data into the second template part to obtain a second file part;

obtaining the related information of the direct debit subscription corresponding to the target transaction, and populating the related information of the direct debit subscription into the third template part to obtain a third file part; and

generating the defense file based on the first file part, the second file part, and the third file part.

9. The method according to claim 2, wherein the determining a target defense template applicable to defense of the target transaction from a defense template set based on a transaction feature of the target transaction further comprises:

determining the target defense template applicable to defense of the target transaction from the basic template subset when the defense difficulty of the target transaction is lower than the predetermined difficulty.

10. The method according to claim 2, wherein the defense difficulty of the target transaction is obtained based on at least one of the following:

whether the target transaction meets a predetermined transaction security standard;

whether the target transaction complies with a predetermined transaction security protocol; and

whether an execution process of the target transaction comprises a refund step.

11. A defense file generation system, comprising:

at least one storage medium, storing at least one instruction set and configured to generate a defense file; and

at least one processor, communicatively connected to the at least one storage medium, wherein when the defense file generation system runs,

the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set:

receiving a payment refusal notification corresponding to a target transaction, wherein the payment refusal notification indicates that a target user initiates a payment refusal behavior for the target transaction;

determining a target defense template applicable to defense of the target transaction from a defense template set based on a transaction feature of the target transaction, wherein different defense templates in the defense template set respectively correspond to different transaction features; and

generating a defense file corresponding to the target transaction based on the target defense template.

12. The system according to claim 11, wherein the transaction feature comprises a defense difficulty and a transaction type, the defense template set comprises a basic template subset and an enhanced template subset, and defense templates in the enhanced template subset cover more defense dimensions than defense templates in the basic template subset; and

to determine the target defense template applicable to defense of the target transaction from the defense template set based on the transaction feature of the target transaction, the at least one processor performs the following operation:

determining the target defense template applicable to defense of the target transaction from the enhanced template subset based on a transaction type of the target transaction when a defense difficulty of the target transaction is higher than a predetermined difficulty.

13. The system according to claim 12, wherein the enhanced template subset comprises defense templates respectively corresponding to a plurality of transaction types, and to determine the target defense template applicable to defense of the target transaction from the enhanced template subset based on the transaction type of the target transaction, the at least one processor performs the following operation:

using a defense template corresponding to the transaction type of the target transaction in the enhanced template subset as the target defense template.

14. The system according to claim 12, wherein the defense dimensions covered by the defense templates in the basic template subset comprise a first defense dimension; and

the defense dimensions covered by the defense templates in the enhanced template subset comprise the first defense dimension, and further comprise at least one of a second defense dimension or a third defense dimension, wherein

transaction data of the target transaction is used as defense evidence in the first defense dimension;

historical transaction data of the target user is used as defense evidence in the second defense dimension; and

personalized defense information related to the transaction type of the target transaction is used as defense evidence in the third defense dimension.

15. The system according to claim 14, wherein the transaction type of the target transaction is a transfer type, and the target defense template comprises:

a first template part, corresponding to the first defense dimension, and used to populate the transaction data of the target transaction;

a second template part, corresponding to the second defense dimension, and used to populate the historical transaction data of the target user; and

a third template part, corresponding to the third defense dimension, and used to populate the personalized defense information, wherein the personalized defense information comprises first user information corresponding to the target user and second user information corresponding to another participant of the target transaction.

16. The system according to claim 15, wherein to generate the defense file corresponding to the target transaction based on the target defense template, the at least one processor performs the following operations:

obtaining the transaction data of the target transaction, and populating the transaction data of the target transaction into the first template part to obtain a first file part;

obtaining the historical transaction data of the target user, and populating the historical transaction data into the second template part to obtain a second file part;

obtaining the first user information corresponding to the target user and the second user

information corresponding to the another participant of the target transaction, and populating the first user information and the second user information into the third template part to obtain a third file part; and

generating the defense file based on the first file part, the second file part, and the third file part.

17. The system according to claim 14, wherein the transaction type of the target transaction is a direct debit type, and the target defense template comprises:

a first template part, corresponding to the first defense dimension, and used to populate the transaction data of the target transaction;

a second template part, corresponding to the second defense dimension, and used to populate the historical transaction data of the target user; and

a third template part, corresponding to the third defense dimension, and used to populate the personalized defense information, wherein the personalized defense information comprises related information of direct debit subscription corresponding to the target transaction.

18. The system according to claim 17, wherein to generate the defense file corresponding to the target transaction based on the target defense template, the at least one processor performs the following operations:

obtaining the transaction data of the target transaction, and populating the transaction data of the target transaction into the first template part to obtain a first file part;

obtaining the historical transaction data of the target user, and populating the historical transaction data into the second template part to obtain a second file part;

obtaining the related information of the direct debit subscription corresponding to the target transaction, and populating the related information of the direct debit subscription into the third template part to obtain a third file part; and

generating the defense file based on the first file part, the second file part, and the third file part.

19. The system according to claim 12, wherein to determine the target defense template applicable to defense of the target transaction from the defense template set based on the transaction feature of the target transaction, the at least one processor performs the following operation:

determining the target defense template applicable to defense of the target transaction from

the basic template subset when the defense difficulty of the target transaction is lower than the predetermined difficulty.

20. A computer-readable nonvolatile storage medium, wherein the computer-readable nonvolatile storage medium stores at least one instruction set, and the at least one instruction set is executed by at least one processor to implement the method according to any one of claims 1 to 10.