说明书

发明名称：一种交易支付方法和系统

本申请要求于2011年9月20日提交中国专利局、申请号为2011102801227、发明名称为'一种交易支付方法和系统'的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

【技术领域】

本发明涉及网络技术，尤其涉及一种交易支付方法和系统。

【背景技术】

随着电子商务的快速发展，以及银行电子化服务水平的提高，银行与第三方支付方式不断创新，目前已有的支付方式种类繁多，包括传统的 POS 支付、 ATM 机支付、网银支付、手机银行等多种支付方式，为人们提供了快速便捷的支付方式，大大方便了人们的日常生活。

传统的交易支付方式通常都采用单信道信息传输方式。例如，手机银行，其依托的是移动通信运营商的网络，基于 WAP 技术，为手机客户提供账户查询、转账、缴费付款、消费支付等金融服务。例如，互联网支付、网银支付是在互联网信道或即时通讯信道上传输交易数据。

然而，传统的这些交易支付方式，在确认用户身份信息时存在各种安全性的问题。如对于手机银行，手机容易丢失；对于互联网支付、网银支付，通常仅需要验证用户密码，验证用户身份信息的方式单一，在用户终端电脑中木马病毒时，容易导致数据被窃。因此，传统的交易支付方式的安全性并不高。

【发明内容】

基于此，有必要提供一种能提高安全性的交易支付方法。

一种交易支付方法，包括以下步骤：

获取用户的支付信息，所述支付信息包括通信号码；

通过互动式语音应答平台呼叫所述通信号码，获取用户输入的支付密码；

对所述支付密码和支付信息进行验证，验证通过则进行支付。

优选的，所述获取用户的支付信息的步骤为：通过互联网信道或即时通信信道

获取支付终端提交的用户的支付信息。

优选的，所述通信号码为移动通信号码；在通过互动式语音应答平台呼叫所述移动通信号码的步骤之前，还包括：

通过短信平台向所述移动通信号码对应的移动终端下发短信验证码；

接收所述移动终端返回的回复验证码；

判断所述回复验证码是否与所述短信验证码一致，若是，则验证通过，否则验证不通过。

优选的，在通过互动式语音应答平台呼叫所述移动通信号码的步骤之前，还包括：

获取返回回复验证码的移动终端的移动通信号码；

验证所述获取的移动通信号码是否与预先存储的开户信息中的移动通信号码一致，若是，则验证通过，否则验证不通过。

优选的，在回复验证码验证通过的步骤和 / 或返回回复验证码的移动终端的移动通信号码验证通过的步骤之后，还包括：

对所述支付信息进行风险信息校验。

优选的，在通过互动式语音应答平台呼叫所述通信号码的步骤之前，和 / 或在所述支付密码验证通过之后，还包括：

对所述支付信息进行风险信息校验。

优选的，所述对所述支付信息进行风险信息校验的步骤包括：

获取所述支付信息中的商户额度，检测所述商户额度是否大于设定阈值，若是，则校验不通过，否则校验通过；和 / 或

根据所述支付信息判断用户是否为黑名单用户，若是，则校验不通过，否则校验通过。

优选的，所述对所述支付信息进行风险信息校验的步骤还包括：

判断所述支付信息是否与预先存储的开户信息一致，若是，则校验通过，否则校验不通过。

此外，还有必要提供一种能提高安全性的交易支付系统。

一种交易支付系统，所述系统包括电话支付系统和银行系统，其中：

电话支付系统，包括：

支付信息获取模块，用于获取用户的支付信息，所述支付信息包括通信号码；

互动式语音应答平台，用于呼叫所述通信号码，获取用户输入的支付密码，并将所述支付密码和支付信息发送至银行系统；

银行系统，用于对所述支付密码和支付信息进行验证，验证通过则进行支付。

优选的，所述支付信息获取模块用于通过互联网信道或即时通信信道获取支付终端提交的用户的支付信息。优选的，所述通信号码为移动通信号码；所述电话支付系统还包括短信平台，用于通过短信向所述移动通信号码对应的移动终端下发短信验证码，接收所述移动终端返回的回复验证码，判断所述回复验证码是否与所述短信验证码一致，若是，则验证通过，否则验证不通过。

优选的，所述短信平台还用于获取返回回复验证码的移动终端的移动通信号码，将所述移动通信号码发送至所述银行系统；

所述银行系统还用于验证所述获取的移动通信号码是否与预先存储的开户信息中的移动通信号码一致，若是，则验证通过，否则验证不通过。

优选的，所述电话支付系统还包括用于在回复验证码验证通过和 / 或返回回复验证码的移动终端的移动通信号码验证通过之后，对所述支付信息进行风险信息校验的风险控制系统。

优选的，所述风险控制系统还用于在所述电话支付系统通过互动式语音应答平台呼叫所述通信号码的步骤之前，和 / 或在所述支付密码验证通过之后对所述支付信息进行风险信息校验。

优选的，所述风险控制系统用于获取所述支付信息中的商户额度，检测所述商户额度是否大于设定阈值，若是，则校验不通过，否则校验通过；和 / 或

所述风险控制系统用于根据所述支付信息判断用户是否为黑名单用户，若是，则校验不通过，否则校验通过。

优选的，所述风险控制系统还用于将所述支付信息发送至所述银行系统；

所述银行系统还用于判断所述支付信息是否与预先存储的开户信息一致，若是，则校验通过，否则校验不通过。

上述交易支付方法和系统中，电话支付系统在接收到支付信息后，通过互动式

语音应答平台自动呼叫支付信息中的移动通信号码，获取用户输入的支付密码并对支付密码和支付信息进行验证。由于获取支付终端所提交的支付信息所采用的通道与互动式语言应答平台所采用的通道不相同，在对支付密码和支付信息进行验证时，减少了不法分子通过假网站、木马病毒截获用户的支付信息的可能，因此能够提高安全性。

【附图说明】

图 1 为一个实施例中交易支付方法的流程示意图；

图 2 为另一个实施例中交易支付方法的流程示意图；

图 3 为一个实施例中进行风险信息校验的流程图；

图 4 为一个实施例中交易支付系统的结构示意图；

图 5 为另一个实施例中电话支付系统的结构示意图。

【具体实施方式】

如图 1 所示，在一个实施例中，一种交易支付方法，包括以下步骤：

步骤 S102，支付终端获取用户的支付信息，该支付信息包括通信号码，支付终端将支付信息提交到电话支付系统。

支付终端可以是计算机、电视机、移动通信终端及其他嵌入式电子设备，可以通过 Web 浏览器提交订单，也可以通过即时通讯工具提交订单，从而生成订单数据。订单数据包括用户信息、商户信息、购买的商品信息等。其中，用户信息包括用户注册帐号、用户名称、收货地址、联系方式等；商户信息即商家信息，例如店铺名称、地址、联系方式等；购买的商品信息包括购买数量、购买价格、应付金额等。

通过支付终端提交订单并确认支付后，获取用户的支付信息。用户的支付信息包括银行卡号、用户身份信息、订单相关信息，其中用户身份信息包括但不限于身份证信息（包括用户姓名和身份证号码等）、支付密码、通信号码（可以是移动通信号码，也可以是固定通信号码）、即时通信号码、联系地址等，订单相关信息包括应付金额等。在一个实施例中，在用户提交订单数据后，可弹出提示框提示用户填写支付信息。具体的，支付终端通过互联网信道或即时通信信道将支付信息提交到电话支付系统，电话支付系统则通过互联网信道或即

时通信信道获取支付终端提交的用户的支付信息。

步骤 S104，电话支付系统通过互动式语音应答平台呼叫所述通信号码，获取用户输入的支付密码，并将支付密码和支付信息发送到银行系统。

具体的，电话支付系统设置有互动式语音应答平台（Interactive Voice Response，IVR），通过 IVR 平台呼叫支付信息中的通信号码。该通信号码对应的通信终端会收到呼叫，持有该通信终端的用户接听后，通信终端与 IVR 平台建立连接，通信终端会收到 IVR 平台通过语音信道下发的语音提示，用户根据语音提示输入支付密码，终端将支付密码上传到电话支付系统，由电话支付系统将支付密码和支付信息组织成交易报文，并发送至银行系统。

步骤 S106，银行系统对支付密码和支付信息进行验证，验证通过则进行支付。

具体的，银行系统可以是银行支付系统，也可以是任意交易平台上的支付系统。银行系统预先存储了用户的开户信息，包括身份证信息、开通的银行卡卡号、联系地址、移动通信号码、支付密码等。银行系统在收到支付密码和支付信息后，验证用户输入的支付密码是否正确，并验证支付信息是否与用户的开户信息相符，如果正确，则验证通过，则直接扣款。

在一个实施例中，银行系统完成支付后，通知电话支付系统，由电话支付系统修改用户订单状态等。

在一个实施例中，在步骤 S104 之前，还包括对支付信息进行风险信息校验的步骤。在支付信息的风险信息校验通过后 IVR 平台才呼叫通信号码，从而能够确保在呼叫之前的安全性。在本实施例或另一个实施例中，在步骤 S106 中对支付密码进行验证通过后，还包括对支付信息进行风险信息校验的步骤。由于支付密码验证通过后支付信息还可能更改，在支付信息的风险信息校验通过后银行系统才进行扣款，能够进一步提高支付的安全性。

由于支付终端提交支付信息和 IVR 平台获取支付密码分别是通过不同的信道进行数据传输的，可以在两个信道上对支付信息进行验证，从而提高了安全性。另外，电话支付系统在收到支付信息后，通过 IVR 平台自动呼叫支付信息中的通信号码来获取支付密码，相对于传统的用户主动呼叫 IVR 平台提供支付密码

的方式，能确保提供支付密码的用户为通信号码对应的终端的持有人。如果支付密码被盗取，也能通过自动呼叫提供的通信号码来有效阻止支付，因此，进一步提高了安全性。

如图 2 所示，在另一个实施例中，一种交易支付方法，包括以下步骤：

步骤 S202，支付终端获取用户的支付信息，该支付信息包括移动通信号码，支付终端将支付信息提交到电话支付系统。

步骤 S204，通过短信平台向移动通信号码对应的移动终端下发短信验证码。

步骤 S206，接收移动终端返回的回复验证码。

具体的，移动终端接收到短信后，用户输入回复验证码，回复验证码返回到短信平台。

步骤 S208，判断回复验证码是否与短信验证码一致，若是，则进入步骤 S210，否则结束。

在一个实施例中，如果回复验证码与短信验证码不一致，可下发短信提示用户返回的验证码不正确，不能完成支付。这样，通过短信信道进行数据传输，再次对支付信息进行验证，进一步提高了安全性。

步骤 S210，获取返回回复验证码的移动终端的移动通信号码。

步骤 S212，通过银行系统验证获取的移动通信号码是否与预先存储的开户信息中的移动通信号码一致，若是，则进入步骤 S214，否则结束。

在银行系统中预先存储了用户的开户信息，包括用户开通银行卡时所提供的移动通信号码。如果银行系统获取的移动通信号码与预先存储的开户信息中的移动通信号码一致，则通过验证，否则，验证不通过。

在一个实施例中，如果验证不通过，银行系统可以通知电话支付系统，电话支付系统通过短信平台下发短信到移动终端，提示用户验证不通过，不能完成支付。通过银行系统对返回回复验证码的移动通信号码进行验证，确保了移动终端的持有者即为银行卡用户，避免了因为移动终端丢失而银行卡资金丢失的风险，进一步提高了安全性。

此外，由于在呼叫移动通信号码之前，对短信验证码进行了验证，以及对获取返回回复验证码的移动通信号码进行了验证，因此能够避免由于移动通信终端

的转移呼叫而造成的安全性问题。

步骤 S214，对支付信息进行风险信息校验，如果校验通过，则进入步骤 S216。

步骤 S216，电话支付系统通过 IVR平台呼叫移动通信号码，获取用户输入的支付密码，并将支付密码和支付信息发送至银行系统。

如上所述，具体的，移动通信号码对应的移动终端会收到呼叫，持有该移动终端的用户接听后，移动终端与 IVR 平台建立起连接，移动终端会收到 IVR 平台通过语音信道下发的语音提示，用户根据语音提示输入支付密码，移动终端将支付密码上传到电话支付系统，电话支付系统将支付密码和支付信息组织成交易报文，并发送到银行系统。

步骤 S218，银行系统对支付密码和支付信息进行验证，验证通过则进行支付。

具体的，银行系统验证支付密码是否正确以及验证支付信息是否与预先存储的开户信息相符，若是，则验证通过，直接扣款，否则，通知电话支付系统，由 IVR 平台下发语音提示给移动终端，提示用户密码输入不正确或支付信息不对。

在一个实施例中，上述对支付信息进行风险信息校验的步骤包括：获取交易信息中的商户额度，检测该商户额度是否大于设定阈值，若是，则校验不通过，否则校验通过。商户额度是订单的交易额度，如一次交易的数量、金额等，超过设定阈值的数量、金额的交易认为有风险的（如可能银行卡被盗用等），则校验不通过。这样，可以有效提高支付的安全性。

在本实施例中或另一个实施例中，对支付信息进行风险信息交易的步骤还包括：根据支付信息判断用户是否为黑名单用户，若是，则校验不通过，否则校验通过。如果用户交易存在不良记录，例如支付信息验证失败2次则认为该用户非法，则将用户身份信息加入到黑名单中。对于黑名单中的用户，在进行风险信息校验时，校验不通过，即非法用户不能完成支付。这样，避免了非法用户再次进行交易，进一步提高了支付的安全性。

在一个实施例中，对支付信息进行风险校验的步骤还包括：电话支付系统将支

付信息发送至银行系统，银行系统判断支付信息是否与预先存储的开户信息一致，若是，则校验通过，否则校验不通过。

如图3所示，在一个实施例中，步骤S214中，对支付信息进行风险信息校验的过程具体如下：

步骤S302，根据支付信息判断用户是否为黑名单用户，若是，则流程结束，否则进入步骤S304。

步骤S304，根据支付信息判断商户额度是否大于设定阈值，若是，则流程结束，否则进入步骤S306。

步骤S306，判断是否存在已校验的支付信息，若是，则进入步骤S216，进入后续流程，否则，进入步骤S308。

步骤S308，提示用户填写支付信息。

步骤S310，对用户填写的支付信息进行风险信息校验。

步骤S310中对支付信息进行风险信息校验的过程如上所示，在此不再赘述。

在一个实施例中，在步骤S218中支付密码验证通过，还可再对支付信息进行风险信息校验，例如，根据支付信息判断商户额度是否大于设定阈值等。由于在支付密码验证通过后，用户可能会更改支付信息，通过再次进行风险信息校验，能进一步提高安全性。

如图4所示，在一个实施例中，一种交易支付系统，包括支付终端10、电话支付系统20和银行系统30，其中：

支付终端10用于获取用户的支付信息，该支付信息包括通信号码，支付终端10还用于将支付信息提交到电话支付系统20。

电话支付系统20，包括IVR平台202，IVR平台202用于呼叫通信号码，获取用户输入的支付密码，并将支付密码和支付信息发送到银行系统30。

银行系统30用于对支付密码和支付信息进行验证，验证通过则进行支付。

在一个实施例中，用户通过支付终端10提交订单，订单数据包括用户信息、商户信息、购买的商品信息等。其中，用户信息包括用户注册帐号、用户名称、收货地址、联系方式等；商户信息即商家信息，例如店铺名称、地址、联系方式等；购买的商品信息包括购买数量、购买价格、应付金额等。

通过支付终端提交订单并确认支付后，获取用户的支付信息。用户的支付信息包括银行卡号、用户身份信息、订单相关信息，其中用户身份信息包括但不限于身份证信息（包括用户姓名、身份证号码等）、支付密码、通信号码（可以是移动通信号码，也可以是固定通信号码）、即时通信号码、联系地址等，订单相关信息包括应付金额等。在一个实施例中，在用户提交订单数据后，可弹出提示框提示用户填写支付信息。具体的，支付终端 10 通过互联网信道或即时通信信道将支付信息提交到电话支付系统 20。

进一步的，电话支付系统 20 可包括支付信息获取模块，用于通过互联网信息或即时通信信道获取支付终端 10 提交的用户的支付信息。

在一个实施例中，通过 IVR 平台 202 呼叫支付信息中的通信号码，该通信号码对应的通信终端会收到呼叫，持有该通信终端的用户接听后，通信终端与 IVR 平台 202 建立连接，通信终端会收到 IVR 平台 202 通过语音信道下发的语音提示，用户根据语音提示输入支付密码，通信终端将支付密码上传到电话支付系统 20，由电话支付系统 20 将支付密码和支付信息组织成交易报文，并发送至银行系统 30。

具体的，银行系统 30 可以是银行支付系统，也可以是任意交易平台上的支付系统。在银行系统 30 预先存储了用户的开户信息，包括用户的身份证信息、开通的银行卡卡号、联系地址、移动通信号码、支付密码等。银行系统 30 在收到支付密码和支付信息后，验证用户输入的支付密码是否正确，并验证支付信息是否与用户的开户信息相符，如果正确，则验证通过，则直接扣款，完成支付。

在一个实施例中，电话支付系统20还包括核心支付系统（图中未示出），用于管理订单等。当银行系统30完成支付后，通知核心支付系统，由核心支付系统修改订单状态，并将该订单状态返回到支付终端10。

在另一个实施例中，如图 5 所示，电话支付系统 20 还包括短信平台 204，短信平台 204 用于通过短信向支付信息中的移动通信号码对应的移动终端下发短信验证码，接收该移动终端返回的回复验证码，判断回复验证码是否与短信验证码一致，若是，则验证通过，否则验证不通过。

在一个实施例中，短信平台 204 还用于获取返回回复验证码的移动终端的移动通信号码，将该移动通信号码发送至银行系统 30。本实施例中，银行系统 30 还用于验证获取的移动通信号码是否与预先存储的开户信息中的移动通信号码一致，若是，则验证通过，否则验证不通过。

在一个实施例中，如图 5 所示，电话支付系统 20 还包括用于回复验证码验证通过和 / 或返回回复验证码的移动终端的移动通信号码验证通过之后，对支付信息进行风险信息校验的风险控制系统 206。

在一个实施例中，风险控制系统 206 还用于在电话支付系统 20 通过 IVR 平台 202 呼叫通信号码的步骤之前对支付信息进行风险信息校验。在本实施例或另一个实施例中，风险控制系统 206 还用于在支付密码验证通过之后对支付信息进行风险信息校验。

在一个实施例中，风险控制系统 206 用于获取支付信息中的商户额度，检测商户额度是否大于设定阈值，若是，则校验不通过，否则校验通过。在本实施例或另一实施例中，风险控制系统 208 还用于根据支付信息判断用户是否为黑名单用户，若是，则校验不通过，否则校验通过。

在一个实施例中，风险控制系统206还用于将支付信息发送到银行系统30。本实施例中，银行系统30还用于判断支付信息是否与预先存储的开户信息一致，若是，则校验通过，否则校验不通过。

上述交易支付方法和系统中，通过使用移动终端、互联网、IVR平台、短信平台等多个通信通道采集用户的支付信息，大大增加了用户的支付信息被全部盗取的难度，因此增加了非面对面支付的安全性。

上述交易支付方法和系统中，通过短信验证确认移动终端持有人，通过银行系统确认银行卡持有人的身份、移动通信号码等信息，通过多个通信通道来验证用户身份信息，确保了安全支付。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，

ROM）或随机存储记忆体（Random Access Memory， RAM）等。

以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

权利要求书

[权利要求 1] 一种交易支付方法，包括以下步骤：

获取用户的支付信息，所述支付信息包括通信号码；

通过互动式语音应答平台呼叫所述通信号码，获取用户输入的支付密码；

对所述支付密码和支付信息进行验证，验证通过则进行支付。

[权利要求 2] 根据权利要求1所述的交易支付方法，其特征在于，所述获取用户的支付信息的步骤为：通过互联网信道或即时通信信道获取支付终端提交的用户的支付信息。

[权利要求 3] 根据权利要求1所述的交易支付方法，其特征在于，所述通信号码为移动通信号码；在通过互动式语音应答平台呼叫所述移动通信号码的步骤之前，还包括：

通过短信平台向所述移动通信号码对应的移动终端下发短信验证码；

接收所述移动终端返回的回复验证码；

判断所述回复验证码是否与所述短信验证码一致，若是，则验证通过，否则验证不通过。

[权利要求 4] 根据权利要求3所述的交易支付方法，其特征在于，在通过互动式语音应答平台呼叫所述移动通信号码的步骤之前，还包括：

获取返回回复验证码的移动终端的移动通信号码；

验证所述获取的移动通信号码是否与预先存储的开户信息中的移动通信号码一致，若是，则验证通过，否则验证不通过。

[权利要求 5] 根据权利要求4所述的交易支付方法，其特征在于，在回复验证码验证通过的步骤和/或返回回复验证码的移动终端的移动通信号码验证通过的步骤之后，还包括：

对所述支付信息进行风险信息校验。

[权利要求 6] 根据权利要求1所述的交易支付方法，其特征在于，在通过互动式语音应答平台呼叫所述通信号码的步骤之前，和/或在所述支付密

码验证通过之后，还包括：

对所述支付信息进行风险信息校验。

[权利要求 7] 根据权利要求 5 或 6 所述的交易支付方法，其特征在于，所述对所述支付信息进行风险信息校验的步骤包括：

获取所述支付信息中的商户额度，检测所述商户额度是否大于设定阈值，若是，则校验不通过，否则校验通过；和 / 或

根据所述支付信息判断用户是否为黑名单用户，若是，则校验不通过，否则校验通过。

[权利要求 8] 根据权利要求7所述的交易支付方法，其特征在于，所述对所述支付信息进行风险信息校验的步骤还包括：

判断所述支付信息是否与预先存储的开户信息一致，若是，则校验通过，否则校验不通过。

[权利要求 9] 一种交易支付系统，其特征在于，所述系统包括电话支付系统和银行系统，其中：

电话支付系统包括：

支付信息获取模块，用于获取用户的支付信息，所述支付信息包括通信号码；

互动式语音应答平台，用于呼叫所述通信号码，获取用户输入的支付密码，并将所述支付密码和支付信息发送至银行系统；

银行系统，用于对所述支付密码和支付信息进行验证，验证通过则进行支付。

[权利要求 10] 根据权利要求9所述的交易支付系统，其特征在于，所述支付信息获取模块用于通过互联网信道或即时通信信道获取支付终端提交的用户的支付信息。

[权利要求 11] 根据权利要求9所述的交易支付系统，其特征在于，所述通信号码为移动通信号码；所述电话支付系统还包括短信平台，用于通过短信向所述移动通信号码对应的移动终端下发短信验证码，接收所述移动终端返回的回复验证码，判断所述回复验证码是否与所

述短信验证码一致，若是，则验证通过，否则验证不通过。

[权利要求 12] 根据权利要求11所述的交易支付系统，其特征在于，所述短信平台还用于获取返回回复验证码的移动终端的移动通信号码，将所述移动通信号码发送至所述银行系统；

所述银行系统还用于验证所述获取的移动通信号码是否与预先存储的开户信息中的移动通信号码一致，若是，则验证通过，否则验证不通过。

[权利要求 13] 根据权利要求12所述的交易支付系统，其特征在于，所述电话支付系统还包括用于在回复验证码验证通过和/或返回回复验证码的移动终端的移动通信号码验证通过之后，对所述支付信息进行风险信息校验的风险控制系统。

[权利要求 14] 根据权利要求13所述的交易支付系统，其特征在于，所述风险控制系统还用于在所述电话支付系统通过互动式语音应答平台呼叫所述通信号码的步骤之前，和/或在所述支付密码验证通过之后对所述支付信息进行风险信息校验。

[权利要求 15] 根据权利要求13或14所述的交易支付系统，其特征在于，所述风险控制系统用于获取所述支付信息中的商户额度，检测所述商户额度是否大于设定阈值，若是，则校验不通过，否则校验通过；

和/或

所述风险控制系统用于根据所述支付信息判断用户是否为黑名单用户，若是，则校验不通过，否则校验通过。

[权利要求 16] 根据权利要求15所述的交易支付系统，其特征在于，所述风险控制系统还用于将所述支付信息发送至所述银行系统；

所述银行系统还用于判断所述支付信息是否与预先存储的开户信息一致，若是，则校验通过，否则校验不通过。