

## 一种支付信息处理的方法、装置、设备及介质

### 技术领域

[01]本申请涉及计算机技术领域，尤其涉及一种支付信息处理的方法、装置、设备及介质。

### 背景技术

[02]随着计算机技术的发展，越来越多的用户采用线上购物的方式购买所需物品，其中用户选购所需商品后在进行线上支付时，需要唤起第三方支付服务，选择支付渠道，输入支付密码等信息，完成线上支付，整个过程需要用户进行一定的操作，例如，用户进行多次线上支付时，需要用户重复性输入支付密码等信息，用户操作繁琐。

[03]因此，如何使用户快速安全的进行支付处理是亟待解决的技术问题。

### 发明内容

[04]本说明书实施例提供一种支付信息处理的方法、装置、设备及介质，使用户可以快速安全的进行支付处理。

[05]本说明书实施例是这样实现的：本说明书实施例提供一种支付信息处理的方法，包括：获取目标机构发送的基于用户的支付操作生成的支付请求；所述支付请求包括授权支付账户的标识信息；所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户；确定所述授权支付账户的账户状态信息；基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险，得到第一判断结果；若所述第一判断结果表示所述交易不存在交易风险，则执行第一支付流程；若所述第一判断结果表示所述交易存在交易风险，则执行包含第一核身验证过程的第二支付流程。

[06]本说明书实施例提供一种支付信息处理的装置，包括：请求获取模块，用于获取目标机构发送的基于用户的支付操作生成的支付请求；所述支付请求包括授权支付账户的标识信息；所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户；信息确定模块，用于确定所述授权支付账户的账户状态信息；第一判断模块，用于基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险，得到第一判断结果；第一流程模块，用于若所述第一判断结果表示所述交易不存在交易风险，则执行第一支付流程；第二流程模块，用于若所述第一判断结果表示所述交易存在交易风险，则执行包含第一核身验证过程的第二支付流程。

[07]本说明书实施例提供一种支付信息处理的设备，包括：至少一个处理器；以及，与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：获取目标机构发送的基于用户的支付操作生成的支付请求；所述支付请求包括授权支付账户的标识信息；所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户；确定所述授权支付账户的账户状态信息；基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险，得到第一判断结果；若所述第一判断结果表示所述交易不存在交易风险，则执行第一支付流程；若所述第一判断结果表示所述交易存在交易风险，则执行包含第一核身验证过程的第二支付流程。

[08]本说明书实施例提供一种计算机可读介质，其上存储有计算机可读指令，所述计算机可读指令可被处理器执行以实现上述一种支付信息处理的方法。

[09]本说明书一个实施例实现了能够达到以下有益效果：本说明书实施例中授权支付账户可以与目标机构建立免密支付授权关系，可以利用授权支付账户进行免密支付，其中通过判断支付请求对应的交易是否存在交易风险，确定是否可以进行免密支付，若交易不存在风险，可进行免密支付，提高支付效率，若交易存在风险时，可进行核身验证，通过核身验证的方式进行支付，无需重新发起支付请求，进而在保证支付安全的同时可简化支付流程。另一方面，也可减少目标机构发起支付请求的次数，降低目标机构以及进行支付信息处理的第三方支付服务机构的数据处理量，提高支付信息的处理效率。

## 附图说明

[10]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[11]图1为本说明书实施例中一种支付信息处理的方法在实际应用场景中的整体方案架构示意图；

[12]图2为本说明书实施例提供的一种支付信息处理的方法的流程示意图；

[13]图3为本说明书实施例中提供的一种生成授权凭证的泳道图；

[14]图4为本说明书实施例中提供的一种支付信息处理方法的泳道图；

[15]图5为本说明书实施例提供的一种支付信息处理的装置的结构示意图；

[16]图6为本说明书实施例提供的一种支付信息处理的设备的结构示意图。

## 具体实施方式

[17]为使本说明书一个或多个实施例的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书一个或多个实施例的技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本说明书一个或多个实施例保护的范围。

[18]以下结合附图，详细说明本说明书各实施例提供的技术方案。

[19]为了解决现有技术中的缺陷，本方案给出了以下实施例：图1为本说明书实施例中一种支付信息处理的方法在实际应用场景中的整体方案架构示意图。如图1所示，该方案主要包括：第三方支付服务平台1、可为用户提供业务需求服务的目标机构2以及用户终端3。其中，用户可以通过终端3在目标机构2提供的服务平台中获取业务，例如，用户可以通过终端在某购物平台中购买物品，目标机构2基于用户的支付操作生成支付请求，发送至第三方支付服务平台1，第三方支付服务平台1判断支付请求对应的交易是否存在交易风险，若不存在交易风险，可利用支付请求对应的授权免密支付账户进行免密支付，若存在交易风险可进入包括核身验证的支付流程，用户可以通过输入密码的方式进行支付，用户无需重新进行支付操作，目标机构也无需重新基于用户的支付操作重新提交支付请求，在保证支付安全的基础上也可提高支付效率。

[20]接下来，将针对说明书实施例提供的一种支付信息处理的方法结合附图进行具体说明：图2为本说明书实施例提供的一种支付信息处理的方法的流程示意图。从程序角度而言，流程的执行主体可以为搭载于应用服务器的程序或应用客户端，从硬件角度而言，

流程的执行主体可以为可进行支付信息处理的第三方支付服务平台。

[21]如图 2 所示，该流程可以包括以下步骤：步骤 202：获取目标机构发送的基于用户的支付操作生成的支付请求；所述支付请求包括授权支付账户的标识信息；所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户。

[22]本说明书实施例中目标机构可以是为用户提供目标业务的机构，例如，目标机构可以是为用户提供购物平台的机构，用户可以在目标机构提供的平台中购买物品；也可以是为用户提供新闻资讯、文学作品、业务咨询服务的机构等。目标机构可以基于用户的支付操作生成支付请求，发送至支付服务平台，以便支付服务平台处理目标机构发送的支付请求。

[23]本说明书实施例中支付服务平台还可以根据用户的授权，建立目标机构与支付账户之间的免密支付授权关系，用户在基于目标机构办理业务时，可以利用授权的支付账户进行免密支付，简化用户的支付操作。

[24]步骤 204：确定所述授权支付账户的账户状态信息。

[25]本说明书实施例中目标机构发送的支付请求中可以包括授权支付账户的标识信息，支付服务平台可以根据支付请求确定授权支付账户的账户状态信息，其中，账户状态信息可以是与授权支付账户的相关联的信息，可以包括但不限于登录授权支付账户的终端的信息、授权支付账户余额信息等。

[26]步骤 206：基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险，得到第一判断结果。

[27]步骤 208：若所述第一判断结果表示所述交易不存在交易风险，则执行第一支付流程。

[28]步骤 210：若所述第一判断结果表示所述交易存在交易风险，则执行包含第一核身验证过程的第二支付流程。

[29]本说明书实施例中可以基于授权支付账户的账户状态信息判断支付请求对应的交易是否存在交易风险，若不存在交易风险，则可以执行第一支付流程，进行免密支付，无需用户输入密码、指纹或人脸等核身信息，也可以完成当前交易；若存在交易风险，则可跳转到执行包含第一核身验证过程的第二支付流程，进行核身验证支付，在用户输入正确的密码、指纹或人脸等核身信息后，完成当前交易，此流程无需结束本次交易，也无需用户重新进行支付操作，目标机构也无需重新向支付服务平台发起支付请求，可简化用户操作，减少目标机构与支付服务平台的交互，节省资源，提高支付效率。

[30]应当理解，本说明书一个或多个实施例所述的方法其中部分步骤的顺序可以根据实际需要相互交换，或者其中的部分步骤也可以省略或删除。

[31]图 2 中的方法，授权支付账户可以与目标机构建立免密支付授权关系，可以利用授权支付账户进行免密支付，其中通过判断支付请求对应的交易是否存在交易风险，确定是否可以进行免密支付，若交易不存在风险，可进行免密支付，提高支付效率，若交易存在风险时，可进行核身验证，通过核身验证的方式进行支付，无需重新发起支付请求，进而在保证支付安全的同时可简化支付流程，也可减少目标机构发起支付请求的次数，降低目标机构以及进行支付信息处理的第三方支付服务机构的数据处理量，提高支付信息的处理效率。

[32]基于图 2 的方法，本说明书实施例还提供了该方法的一些具体实施方案，下面进行说明。

[33]可选的，本说明书实施例中还可以基于交易的支付金额确定支付流程，具体的，上述步骤 202 中的支付请求可以包括支付金额；所述基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险之前，还可以包括：基于所述支付请求，判断所述支付金额是否小于或等于预设支付金额，得到第二判断结果；若所述第二判断结果表示所述支付金额大于所述预设支付金额，则执行包含第二核身验证过程的第三支付流程；所述判断所述支付请求对应的交易是否存在交易风险，具体包括：若所述第二判断结果表示所述支付金额小于或等于所述预设支付金额，则基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险。

[34]本说明书实施例中在建立授权支付账户与目标机构的免密支付授权关系时，还可以由用户或者目标机构或者支付服务机构设定免密支付的金额，例如，预设支付金额为 100 元，则用户在支付时，若支付金额大于 100 元，则需要用户提供支付密码、指纹或人脸等核身信息，进行核身支付；如果支付金额小于或等于 100 元，则可以进一步判断是否存在交易风险进而确定是否可以进行免密支付。本说明书实施例中可以设定免密支付的限定金额，提高支付的安全性。

[35]本说明书实施例中可以建立授权支付账号与目标机构之间的免密支付授权关系，具体的，本说明书实施例中提供的支付信息处理的方法中还可以包括：接收所述目标机构发送的免密支付授权申请；所述免密支付授权申请是基于所述用户在终端中的授权申请操作生成的；所述免密支付授权申请包括所述终端登录的待授权支付账户的账户信息以及所述目标机构的机构标识信息；发送针对所述待授权支付账户的第一支付验证指示信息至所述终端；接收所述终端发送的响应于所述第一支付验证指示信息的第一支付验证信息；判断所述第一支付验证信息是否与针对所述待授权支付账户预先设置的支付验证信息一致，得到第三判断结果；其中，第一支付验证信息可以包括指纹信息、人脸信息、虹膜信息、密码信息中至少一种；若所述第三判断结果表示所述支付验证信息与针对所述待授权支付账户预先设置的支付验证信息一致，则生成用于免密支付的授权凭证；所述用于免密支付的授权凭证表示所述待授权支付账户与所述目标机构建立了免密支付授权的关系。

[36]实际应用中，用户可以登录终端中目标机构的应用程序或网页进行业务办理，用户可以在该应用程序或网页中执行免密支付的授权申请操作，建立支付账户与目标机构的免密支付授权关系，以便后续使用该支付账户进行免密支付。为保证用户账户安全，在建立授权关系时，用户需要提供针对该支付账户的支付验证信息，当验证通过时，才可以建立授权关系。

[37]本说明书实施例中，在建立授权关系时，用户可以基于目标机构的应用客户端或网页执行授权申请操作，目标机构发送的免密支付授权申请中可以包含目标机构的机构标识以及待授权的支付账户的账户信息，支付服务平台可以基于该机构标识以及支付账户的账户信息生成待确认授权凭证信息发送至终端。其中，免密支付授权申请中也不包含待授权的支付账户的账户信息，支付服务平台可以将终端当前登录的支付账户确认为待授权的支付账户，基于机构标识以及终端当前登录的支付账户生成待确认授权凭证信息发送至终端。用户经过对该待确认授权凭证信息确认后，支付服务平台根据用户的确认信息可以生成确认后的授权凭证。

[38]支付服务平台可以保存目标机构、支付账户以及生成的授权凭证的对应关系，以便后续进行免密支付的验证。支付服务平台也可以将该授权凭证发送至目标机构，后续目标机构在发送支付请求时，可以携带该授权凭证，以便支付服务平台判断目标机构发送的授权凭证是否有效，以及目标机构与支付账户之间的授权关系是否成立，进而确定是否可以进行免密支付。

[39]本说明书实施例中，与目标机构建立授权关系的账户可以是在用户执行授权申请操作时，用户终端中登录的支付账户，若用户终端当前登录有多个支付账户，用户可以选择其中至少一个支付账户建立与目标机构之间的授权关系。实施应用中，不同的支付账户可以对应不同的支付服务平台，支付服务平台也可以管理与该平台具有关联关系的其他平台的支付账户。

[40]实际应用中，目标机构也可以根据用户的历史交易信息确定用户可使用的支付账户，当将用户可使用的支付账户提供给用户以便用户选择与目标机构建立授权关系的支付账户。

[41]为提高支付的安全性，本说明书实施例中的免密支付可以是基于终端当前登录的支付账户的免密支付，若终端当前登录的支付账户是与目标机构建立免密支付授权关系的支付账户则可以基于该支付账户进行免密支付，若终端当前登录的支付账户不是与目标机构建立免密支付授权关系的支付账户，则可以基于终端当前登录的支付账户执行核身验证的支付流程，具体的，本说明书实例中的支付请求可以包括所述目标机构对应的机构标识和接收所述用户的支付操作的终端的设备标识；所述判断所述支付请求对应的交易是否存在交易风险之前，还可以包括：根据所述设备标识，确定所述终端中当前登录的登录支付账户；根据所述授权凭证，判断所述登录支付账户与所述授权凭证对应的授权支付账户是否一致，得到第四判断结果；若所述第四判断结果表示所述登录支付账户与所述授权凭证对应的支付账户不一致，则执行包含第三核身验证过程的第四支付流程；所述判断所述支付请求对应的交易是否存在交易风险，具体可以包括：若所述第四判断结果表示所述登录支付账户与所述授权凭证对应的授权支付账户一致，则基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险。

[42]作为另一种实施方式，本说明书实施例中还可以根据终端中当前登录的登录支付账户，确定与该登录支付账户建立免密支付授权关系的机构是否是发送支付请求的目标机构，若是，则可以进一步判断交易是否存在交易风险，若不是，则需要执行包含核身验证的支付流程。

[43]实际应用中，用户在目标机构进行业务办理时，可能需要登录用户在该目标机构注册的账号后再进行业务办理，本说明书实施例中，目标机构对应的机构标识可以携带用户在目标机构中的用户标识，例如，用户在目标机构中的注册账号、注册名称等用于区分目标机构中不同用户的用户标识。支付服务平台可以根据授权凭证判断发起支付请求的目标机构的用户是否是授权支付账户建立授权关系的用户，若是，则可以进一步判断交易是否存在交易风险，若否，则需要执行核身验证流程。

[44]当用户无需注册成为目标机构的用户或者无需登录用户在目标机构中的注册账号也可以进行业务办理时，授权凭证可以是针对目标机构的机构标识与授权支付账户建立的免密支付授权关系。

[45]本说明书实施例中当确定终端中登录的支付账户为目标机构的授权支付账户后，若交易存在交易风险，则可以执行针对该授权支付账户的核身验证，具体的，步骤210中所述第一核身验证过程具体可以为针对所述授权凭证对应的授权支付账户的核身验证过程。

[46]相应的，上述第三核身验证过程具体可以为针对所述登录支付账户的核身验证过程。

[47]考虑到授权凭证可能存在时效性，即生成授权凭证后的预设时间段内，可以根据该授权凭证进行免密授权支付。本说明书实施例中步骤206所述判断所述支付请求对应的交易是否存在交易风险之前，还可以包括：基于所述支付请求，确定发起所述支付请求的发起时间；判断所述发起时间是否在所述授权凭证的有效期限内，得到第五判断结果；

若所述第五判断结果表示所述发起时间不在所述授权凭证的有效期限内,则进行包含第四核身验证的第五支付流程;所述判断所述支付请求对应的交易是否存在交易风险,具体包括:若所述第五判断结果表示所述发起时间在所述授权凭证的有效期限内,则基于所述账户状态信息,判断所述支付请求对应的交易是否存在交易风险。

[48]其中,授权凭证的有效期限可以由用户设定,也可以由支付服务平台根据用户以及目标机构的资质确定,例如,对于信誉度较好的用户以及目标机构,可以将有效期限设定的较长。实施应用中,当授权凭证的有效期限到达时或者有效期限达到前的预设时间,目标机构可以发送提示续签的信息至用户终端,用户可以根据提示信息选择续签或者终止。

[49]为提高免密支付的安全性,本说明书实施例中,在生成用于授权凭证之前,支付服务平台可以对待授权的支付账户以及目标机构进行授权资质的审核,例如,目标机构需要提交机构注册信息,根据机构注册信息判断该目标机构的合法性,还可以根据机构注册信息确定机构的注册资金,判断该注册资金是否大于或等于预设资金标准,注册资金大于或等于预设资金标准,该目标机构才可能被允许免密支付;又如,还可以根据目标机构之前的历史业务的处理结果,判断目标机构的可信度;又如,也可以根据用户支付账户的账户状态,判断该支付账户的合法性,以及是否为可用账户以及信用度满足要求的账户。

[50]本说明书实施例步骤 206 中基于所述账户状态信息,判断所述支付请求对应的交易是否存在交易风险,具体可以包括:基于所述账户状态信息,确定风险评估依据信息;其中,所述风险评估依据信息可以包括接收所述用户的支付操作的终端的设备标识、所述终端的 GPS 位置信息、所述终端的 IP 地址信息中至少一种;基于所述风险评估依据信息,判断所述支付请求对应的交易是否存在交易风险。

[51]实际应用中,目标机构发送的支付请求中可以包括用户执行支付操作的终端的设备标识、该终端的 GPS 位置信息以及该终端的 IP 地址信息中至少一种信息。作为另一种实施方式,支付服务平台也可以根据支付请求,向目标机构发送获取风险评估依据信息的请求,目标机构可以根据该请求,向支付服务平台反馈相应的信息。本说明书实施例中对支付服务平台获取风险评估依据信息的方式不作限定,只要支付服务平台能够根据风险评估依据信息进行判断交易是否存在交易风险即可。

[52]作为一种实施方式,本说明书实施例中所述基于所述风险评估依据信息,判断所述支付请求对应的交易是否存在交易风险,具体可以包括:基于所述账户状态信息,确定所述授权支付账户的常用登录设备的设备标识;判断所述接收所述用户的支付操作的终端的设备标识与所述常用登录设备的设备标识是否一致;若一致,则确定所述支付请求对应的交易不存在交易风险;若不一致,则确定所述支付请求对应的交易存在交易风险;或者,基于所述账户状态信息,确定所述授权支付账户的绑定设备的设备标识;所述绑定设备为预先与所述支付账户设定为绑定关系的设备;判断所述接收所述用户的支付操作的终端的设备标识与所述绑定设备的设备标识是否一致;若一致,则确定所述支付请求对应的交易不存在交易风险;若不一致,则确定所述支付请求对应的交易存在交易风险。

[53]其中,常用登录设备可以为预设时间段内支付账户成功登录的设备集合中占比大于或等于预设占比的设备,例如,最近一个月内成功登录该支付账户次数最多的终端设备,或者登录时间的累计时长最长的终端设备。

[54]实际应用中,用户可以在支付服务平台对应的应用客户端中设定支付账户的绑定设备,支付服务平台也可以将该支付账户首次登陆的终端设备设定为绑定设备,用户还可以根据需要进行更改,这里对绑定设备的设定不作具体限定。

[55]作为另一种实施方式,本说明书实施例中基于所述风险评估依据信息,判断所述支付请求对应的交易是否存在交易风险,具体包括:基于所述账户状态信息,确定所述终端的IP地址信息;根据所述授权支付账户的标识信息,确定所述授权支付账户的前一次成功交易的IP地址信息;判断所述终端的IP地址信息与所述授权支付账户的前一次成功交易的IP地址信息是否一致;若一致,则确定所述支付请求对应的交易不存在交易风险;若不一致,则确定所述支付请求对应的交易存在交易风险;或者,基于所述账户状态信息,确定所述终端的IP地址信息;根据所述授权支付账户的标识信息,确定所述授权支付账户的常用交易IP地址信息;判断所述终端的IP地址信息与所述授权支付账户的常用交易IP地址信息是否一致;若一致,则确定所述支付请求对应的交易不存在交易风险;若不一致,则确定所述支付请求对应的交易存在交易风险。

[56]实际应用中,用户在终端中执行支付操作,目标机构发起交易请求,该支付请求中可以携带该终端的IP地址信息,支付服务平台可以根据授权支付账户的历史交易信息确定该授权支付账户的前一次成功交易的IP地址,以及该授权支付账户的常用IP地址。

[57]其中,常用IP地址可以是预设时间段内支付账户成功交易的IP地址集合中占比大于或等于预设占比的IP地址,例如,最近三个月内该支付账户成功交易次数最多的IP地址。

[58]实际应用中,当用户使用目标机构的客户端时,用户可以同意目标机构获取用户终端的地理位置信息,如用户可以同意目标机构获取用户终端的GPS定位信息,本说明书实施例中可以基于用户终端的地理位置信息判断交易是否存在交易风险,具体的,所述基于所述风险评估依据信息,判断所述支付请求对应的交易是否存在交易风险,具体可以包括:基于所述账户状态信息,确定所述终端的设备标识;基于所述终端的设备标识,确定所述终端的地理位置信息;根据所述授权支付账户的标识信息,确定所述授权支付账户对应的成功交易的常用地理位置信息;判断所述终端的地理位置信息与所述授权支付账户对应的成功交易的常用地理位置信息是否一致;若一致,则确定所述支付请求对应的交易不存在交易风险;若不一致,则确定所述支付请求对应的交易存在交易风险。

[59]其中,常用地理位置信息可以是预设时间段内支付账户成功交易的地理位置信息集合中占比大于或等于预设占比的地理位置信息,例如,最近两个月内该支付账户成功交易次数最多的地理位置的信息。

[60]实际应用中,支付服务平台可以从目标机构获取交易终端的地理位置信息,当用户同意支付服务平台可以获取用户终端的地理位置信息时,支付服务平台可以自行确定用户终端的地理位置,具体地理位置信息的获取方式这里不作具体限定。

[61]作为一种实施方式,还可以通过判断当前交易的地理位置信息是否与授权支付账户前一次成功交易的地理位置信息一致来确定当前交易是否存在交易风险,具体的,本说明书实施例中,所述基于所述风险评估依据信息,判断所述支付请求对应的交易是否存在交易风险,具体可以包括:基于所述账户状态信息,确定所述终端的设备标识;基于所述终端的设备标识,确定所述终端的地理位置信息;根据所述授权支付账户的标识信息,确定所述授权支付账户前一次成功交易对应的终端的地理位置信息;判断所述终端的地理位置信息与所述授权支付账户前一次成功交易对应的终端的地理位置信息是否一致;若一致,则确定所述支付请求对应的交易不存在交易风险;若不一致,则确定所述支付请求对应的交易存在交易风险。

[62]考虑到实际应用中,用户在目标机构进行交易的可用支付账户可能有多个,又或者,用户一个支付账户可能与多个支付账户相关联,进而用户可以使用多个支付账户中的一个支付账户进行交易支付。

[63]本说明书实施例中所述授权支付账户可以包括至少一个支付子账户；所述执行第一支付流程，具体可以包括：确定针对各个支付子账户预设的第一支付顺序；按照所述第一支付顺序，将所述各个支付子账户中首个账户余额大于或等于所述支付请求对应的支付金额的支付子账户确定为第一目标支付账户；从所述第一目标支付账户中扣除所述支付金额。

[64]本说明书实施例中当授权支付账户包含多个支付子账户时，可选用其中能够支付当前交易金额的账户进行免密支付，可以理解为，当授权支付账户中存在任一个可以执行免密支付的账户时，就可以执行免密支付，进而可提高免密支付的成功率。实际应用中，当交易支付完成后，支付服务平台还可以向目标机构以及用户对应的支付服务平台的客户端发送交易成功的信息。

[65]本说明书实施例中，当确定交易存在风险时，即使用户终端当前登录的支付账户为授权支付账户，目标机构与该支付账户的授权凭证是有效凭证，也需要执行包含针对该授权支付账户进行核身验证的支付流程，具体的，所述执行包含第一核身验证过程的第二支付流程，具体可以包括：发送第二支付验证指示信息至所述终端，以便所述用户根据所述第二支付验证指示信息输入第二支付验证信息；其中，第二支付验证信息包括指纹信息、人脸信息、密码信息、虹膜信息中至少一种信息；接收所述用户输入的所述第二支付验证信息；判断所述第二支付验证信息是否与针对所述授权凭证对应的授权支付账户预先设置的支付验证信息一致；若一致，则从所述授权支付账户中扣除所述支付请求对应的支付金额。

[66]本说明书实施例中所述的在确定支付金额大于预设支付金额后，执行包含第二核身验证过程的第三支付流程，可以是针对授权支付账户的核身验证的支付流程，该具体过程可与上述所描述的执行包含第一核身验证过程的第二支付流程相同，均针对授权支付账户进行核身验证，验证通过后，可用该授权支付账户进行支付。

[67]本说明书实施例中，所述授权支付账户可以包括至少一个授权支付子账户；所述发送第二支付验证指示信息至所述终端之前，还可以包括：确定针对各个授权支付子账户预设的第二支付顺序；按照所述第二支付顺序，将所述各个授权支付子账户中首个账户余额大于或等于所述支付请求对应的支付金额的授权支付子账户确定为第二目标支付账户；所述发送第二支付验证指示信息至所述终端，具体可以包括：发送针对所述第二目标支付账户的第二支付验证指示信息至所述终端；所述判断所述第二支付验证信息是否与针对所述授权凭证对应的授权支付账户预先设置的支付验证信息一致，具体可以包括：所述判断所述第二支付验证信息是否与针对所述第二目标支付账户预先设置的支付验证信息一致；所述从所述授权支付账户中扣除所述支付请求对应的支付金额，具体包括：从所述第二目标支付账户中扣除所述支付请求对应的支付金额。

[68]实际应用中，当授权支付账户中存在多个可用的授权支付子账户时，还可以按照第二支付顺序，将多个可用的授权支付子账户从前到后排序，将排序后的多个可用的授权支付子账户发送至用户终端，终端可以呈现包含排序后的多个可用的授权支付子账户的账户选择页面，用户可以选择其中一个账户作为第二目标支付账户。

[69]本说明书实施例中，当用户终端当前登录的支付账户不是授权支付账户时，也可以使用当前登录的支付账户进行支付，无需结束支付流程，具体的，所述执行包含第三核身验证过程的第四支付流程，具体可以包括：发送第三支付验证指示信息至所述终端，以便所述用户根据所述第三支付验证指示信息输入第三支付验证信息；其中，第三支付验证信息可以包括指纹信息、人脸信息、密码信息、虹膜信息中至少一种信息；接收所述用户输入的所述第三支付验证信息；判断所述第三支付验证信息是否与针对所述登录支付账户预先设置的支付验证信息一致；若一致，则从所述登录支付账户中扣除所述支

付请求对应的支付金额。

[70]其中，所述登录支付账户可以包括至少一个登录支付子账户；所述发送第三支付验证指示信息至所述终端之前，还包括：确定针对各个所述登录支付子账户预设的第三支付顺序；按照所述第三支付顺序，将所述各个登录支付子账户中首个账户余额大于或等于所述支付请求对应的支付金额的登录支付子账户确定为第三目标支付账户；所述发送第三支付验证指示信息至所述终端，具体包括：发送针对所述第三目标支付账户的第三支付验证指示信息至所述终端；所述判断所述第三支付验证信息是否与针对所述登录支付账户预先设置的支付验证信息一致，具体包括：所述判断所述第三支付验证信息是否与针对所述第三目标支付账户预先设置的支付验证信息一致；所述从所述登录支付账户中扣除所述支付请求对应的支付金额，具体包括：从所述第三目标支付账户中扣除所述支付请求对应的支付金额。

[71]实际应用中，上述第一支付顺序，第二支付顺序以及第三支付顺序，用户均可以在支付服务平台的客户端中设定，支付服务平台也可以根据用户的习惯为用户推荐支付顺序，用户还可以根据需要进行支付顺序的修改或设定，这里对支付顺序的设定不作具体限定。

[72]实际应用中，还可以设定免密支付的次数，例如，可以设定预设时间段内，可以进行免密支付的次数，如，设定一个月内可以进行8次免密支付，当进行第9次支付时，需要用户输入核身信息进行支付验证。

[73]本说明书实施例中，在不同的支付流程中针对同一账户的核身验证信息可以相同，例如，当第一核身验证过程与第二核身验证过程均为针对同一个授权支付账户时，用户输入的支付验证信息可以是相同的；也可以设置为不同的，例如，第一核身验证过程用户可以输入指纹信息进行验证，第二核身验证过程用户可以输入人脸信息进行验证。同理，针对不同的支付账户的支付流程，用户也可以设定不同的核身验证信息，也可以设置相同的核身验证信息，这些均可根据用户需求进行设定，这里不作具体限定。

[74]为更清楚的说明本说明书实施例中提供的支付信息处理的方法，图3为本说明书实施例中提供的一种生成授权凭证的泳道图，如图3所述，生成授权凭证的授权阶段具体可以包括：步骤302：终端接收用户执行的授权申请操作。

[75]步骤304：目标机构基于用户的授权申请操作生成免密支付授权申请，发送至支付服务平台；所述免密支付授权申请包括所述终端登录的待授权支付账户的账户信息以及所述目标机构的机构标识信息；其中，目标机构还可以根据免密支付授权声明模板生成待确认的授权声明发送至用户终端，以便用户了解免密支付的具体内容以及对授权声明进行确认，目标机构还可以将用户确认后的授权声明发送至支付服务平台。

[76]作为另一种实施方式，支付服务平台也可以基于免密支付授权申请生成待确认的授权声明发送目标机构，目标机构在将该待确认的授权声明发送至用户终端，以便用户确认。实际应用中支付服务平台也可以基于免密支付授权申请生成待确认的授权声明发送至用户终端，当用户确认后，将确认后的授权声明发送至目标机构。具体的过程，这里不作限定，只要支付服务平台能够接收到表示用户确认的信息即可。

[77]步骤306：支付服务平台发送针对所述待授权支付账户的第一支付验证指示信息至所述终端，终端中可以显示需要用户提供第一支付验证信息的界面，用户需要根据指示提供第一支付验证信息。

[78]步骤308：终端基于第一支付验证指示信息显示相应的指示页面。

[79]步骤310：用户在终端中输入第一支付验证信息，发送至支付服务平台。

[80]步骤 312: 接收终端发送的响应于第一支付验证指示信息的第一支付验证信息。

[81]步骤 314: 判断所述第一支付验证信息是否与针对终端当前登录的待授权支付账户预先设置的支付验证信息一致, 得到第三判断结果。

[82]步骤 316: 若所述第三判断结果表示所述第一支付验证信息与针对所述待授权支付账户预先设置的支付验证信息一致, 则生成用于免密支付的授权凭证; 所述用于免密支付的授权凭证表示所述待授权支付账户与所述目标机构建立了免密支付授权的关系。其中, 支付服务平台还可以将生成的授权凭证发送至目标机构。

[83]步骤 318: 目标机构保存支付服务平台发送的该授权凭证或授权凭证的标识, 以便后续目标机构携带授权凭证或者授权凭证的标识发起支付请求。

[84]图 4 为本说明书实施例中提供的一种支付信息处理方法的泳道图, 如图 4 所述, 该方法主要包括判断阶段以及支付阶段, 具体可以包括: 步骤 402: 终端接收用户执行的支付操作。实际应用中, 用户的支付操作可以是用户对待支付账单的确认操作, 例如, 目标机构可以基于用户选购的商品, 生成待支付账单, 用户点击“提交订单”或者“确认支付”, 可以向目标机构发送表示支付操作的指令。

[85]步骤 404: 目标机构基于用户的支付操作生成的支付请求; 所述支付请求包括授权支付账户的标识信息。

[86]步骤 406: 支付服务平台获取目标机构发送的支付请求; 所述支付请求包括所述目标机构对应的机构标识和接收所述用户的支付操作的终端的设备标识

[87]步骤 408: 根据所述设备标识, 确定所述终端中当前登录的登录支付账户。

[88]步骤 410: 根据授权凭证, 判断登录支付账户与授权凭证对应的授权支付账户是否一致。

[89]步骤 412: 若不一致, 则利用该登录支付账户进行当前交易支付, 执行包含针对当前登录的支付账户进行第三核身验证过程的第四支付流程, 具体的可以包括: 步骤 414: 发送针对该登录支付账户的第三支付验证指示信息至终端; 步骤 416: 用户在终端中输入的针对该登录支付账户的第三支付验证信息; 步骤 418: 支付服务平台接收终端输入的第三支付验证信息, 对该第三支付验证信息进行验证; 步骤 420: 若用户输入的针对该登录支付账户的第三支付验证信息与预设的针对该登录支付账户的验证信息一致, 则验证通过, 利用该登录支付账户进行当前交易的支付; 步骤 422: 用户输入的针对该登录支付账户的第三支付验证信息与预设的针对该登录支付账户的验证信息不一致或者不一致的次数超过预设次数, 则验证不通过, 结束当前交易。

[90]步骤 424: 若一致, 基于所述支付请求, 判断支付请求对应的支付金额是否小于或等于预设支付金额。

[91]步骤 426: 若支付金额大于预设支付金额, 则执行包含针对授权支付账户的第二核身验证过程的第三支付流程, 具体可以包括: 步骤 428: 发送针对授权支付账户的第二支付验证指示信息至终端; 步骤 430: 用户在终端中输入的针对授权支付账户的第二支付验证信息, 终端将该信息发送至支付服务机构; 步骤 432: 支付服务机构接收用户输入的第二支付验证信息, 对用户输入的针对授权支付账户的第二支付验证信息进行验证, 判断用户输入的针对授权支付账户的第二支付验证信息是否与预设的针对授权支付账户的核身验证信息一致; 步骤 434: 若一致, 则验证通过, 利用该授权支付账户完成本次交易; 若用户输入的针对授权支付账户的核身验证信息与预设的针对授权支付账户的核身验证信息不一致的次数超过预设次数, 则表示验证不通过, 可同步步骤 422 结束本次交易。

[92]步骤 436: 若支付金额小于或等于预设支付金额, 基于所述账户状态信息, 判断所述支付请求对应的交易是否存在交易风险。其中, 可以基于终端的设备标识、终端的 GPS 位置信息、终端的 IP 地址信息等进行风险判断。

[93]步骤 438: 若所述支付请求对应的交易不存在交易风险, 则基于授权支付账户进行免密支付, 完成当前交易。

[94]步骤 440: 若所述支付请求对应的交易存在交易风险, 则执行包含针对授权支付账户的核身验证过程的支付流程, 具体过程可与上述步骤 428 至步骤 434 相同, 这里不再赘述。

[95]基于同样的思路, 本说明书实施例还提供了上述方法对应的装置。图 5 为本说明书实施例提供的一种支付信息处理的装置的结构示意图。如图 5 所示, 该装置可以包括: 请求获取模块 502, 用于获取目标机构发送的基于用户的支付操作生成的支付请求; 所述支付请求包括授权支付账户的标识信息; 所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户; 信息确定模块 504, 用于确定所述授权支付账户的账户状态信息; 第一判断模块 506, 用于基于所述账户状态信息, 判断所述支付请求对应的交易是否存在交易风险, 得到第一判断结果; 第一流程模块 508, 用于若所述第一判断结果表示所述交易不存在交易风险, 则执行第一支付流程; 第二流程模块 510, 用于若所述第一判断结果表示所述交易存在交易风险, 则执行包含第一核身验证过程的第二支付流程。

[96]基于图 5 的装置, 本说明书实施例还提供了该方法的一些具体实施方案, 下面进行说明。

[97]可选的, 本说明书实施例中的支付请求还可以包括支付金额; 所述装置还可以包括: 第二判断模块, 用于基于所述支付请求, 判断所述支付金额是否小于或等于预设支付金额, 得到第二判断结果; 第三流程模块, 用于若所述第二判断结果表示所述支付金额大于所述预设支付金额, 则执行包含第二核身验证过程的第三支付流程; 所述第一判断模块, 具体可以用于: 若所述第二判断结果表示所述支付金额小于或等于所述预设支付金额, 则基于所述账户状态信息, 判断所述支付请求对应的交易是否存在交易风险。

[98]可选的, 本说明书实施例中所述第一判断模块具体可以用于: 基于所述账户状态信息, 确定风险评估依据信息; 所述风险评估依据信息包括接收所述用户的支付操作的终端的设备标识、所述终端的 GPS 位置信息、所述终端的 IP 地址信息中至少一种; 基于所述风险评估依据信息, 判断所述支付请求对应的交易是否存在交易风险。

[99]基于同样的思路, 本说明书实施例还提供了上述方法对应的设备。

[100]图 6 为本说明书实施例提供的一种支付信息处理的设备的结构示意图。如图 6 所示, 设备 600 可以包括: 至少一个处理器 610; 以及, 与所述至少一个处理器通信连接的存储器 630; 其中, 所述存储器 630 存储有可被所述至少一个处理器 610 执行的指令 620, 所述指令被所述至少一个处理器 610 执行, 以使所述至少一个处理器 610 能够: 获取目标机构发送的基于用户的支付操作生成的支付请求; 所述支付请求包括授权支付账户的标识信息; 所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户; 确定所述授权支付账户的账户状态信息; 基于所述账户状态信息, 判断所述支付请求对应的交易是否存在交易风险, 得到第一判断结果; 若所述第一判断结果表示所述交易不存在交易风险, 则执行第一支付流程; 若所述第一判断结果表示所述交易存在交易风险, 则执行包含第一核身验证过程的第二支付流程。

[101]基于同样的思路, 本说明书实施例还提供了上述方法对应的计算机可读介质。计算机可读介质上存储有计算机可读指令, 所述计算机可读指令可被处理器执行以实现上述

提供的一种信息处理的方法。

[102]本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于图6所示的设备而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[103]在20世纪90年代,对于一个技术的改进可以很明显地区分是硬件上的改进(例如,对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而,随着技术的发展,当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此,不能说一个方法流程的改进就不能用硬件实体模块来实现。例如,可编程逻辑器件(Programmable Logic Device, PLD)(例如现场可编程门阵列(Field Programmable Gate Array, FPGA))就是这样一种集成电路,其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上,而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且,如今,取代手工地制作集成电路芯片,这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现,它与程序开发撰写时所用的软件编译器相类似,而要编译之前的原始代码也得用特定的编程语言来撰写,此称之为硬件描述语言(Hardware Description Language, HDL),而HDL也并非仅有一种,而是有许多种,如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDL、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDH(Ruby Hardware Description Language)等,目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚,只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中,就可以很容易得到实现该逻辑方法流程的硬件电路。

[104]控制器可以按任何适当的方式实现,例如,控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit, ASIC)、可编程逻辑控制器和嵌入微控制器的形式,控制器的例子包括但不限于以下微控制器:ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20以及Silicone Labs C8051F320,存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道,除了以纯计算机可读程序代码方式实现控制器以外,完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件,而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至,可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[105]上述实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的,计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[106]为了描述的方便,描述以上装置时以功能分为各种单元分别描述。当然,在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[107]本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面



块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[117]以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

## 权利要求书

1、一种支付信息处理的方法，包括：

获取目标机构发送的基于用户的支付操作生成的支付请求；所述支付请求包括授权支付账户的标识信息；所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户；

确定所述授权支付账户的账户状态信息；

基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险，得到第一判断结果；

若所述第一判断结果表示所述交易不存在交易风险，则执行第一支付流程；

若所述第一判断结果表示所述交易存在交易风险，则执行包含第一核身验证过程的第二支付流程。

2、根据权利要求1所述的方法，所述支付请求包括支付金额；所述基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险之前，还包括：

基于所述支付请求，判断所述支付金额是否小于或等于预设支付金额，得到第二判断结果；

若所述第二判断结果表示所述支付金额大于所述预设支付金额，则执行包含第二核身验证过程的第三支付流程；

所述判断所述支付请求对应的交易是否存在交易风险，具体包括：

若所述第二判断结果表示所述支付金额小于或等于所述预设支付金额，则基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险。

3、根据权利要求1所述的方法，所述方法还包括：

接收所述目标机构发送的免密支付授权申请；所述免密支付授权申请是基于所述用户在终端中的授权申请操作生成的；所述免密支付授权申请包括所述终端登录的待授权支付账户的账户信息以及所述目标机构的机构标识信息；

发送针对所述待授权支付账户的第一支付验证指示信息至所述终端；

接收所述终端发送的响应于所述第一支付验证指示信息的第一支付验证信息；

判断所述第一支付验证信息是否与针对所述待授权支付账户预先设置的支付验证信息一致，得到第三判断结果；

若所述第三判断结果表示所述第一支付验证信息与针对所述待授权支付账户预先设置的支付验证信息一致，则生成用于免密支付的授权凭证；所述用于免密支付的授权凭证表示所述待授权支付账户与所述目标机构建立了免密支付授权的关系。

4、根据权利要求3所述的方法，所述支付请求包括所述目标机构对应的机构标识和接收所述用户的支付操作的终端的设备标识；

所述判断所述支付请求对应的交易是否存在交易风险之前，还包括：

根据所述设备标识，确定所述终端中当前登录的登录支付账户；

根据所述授权凭证，判断所述登录支付账户与所述授权凭证对应的授权支付账户是否一致，得到第四判断结果；

若所述第四判断结果表示所述登录支付账户与所述授权凭证对应的支付账户不一致，则执行包含第三核身验证过程的第四支付流程；

所述判断所述支付请求对应的交易是否存在交易风险，具体包括：

若所述第四判断结果表示所述登录支付账户与所述授权凭证对应的授权支付账户一致，则基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险。

5、根据权利要求4所述的方法，所述第一核身验证过程具体为针对所述授权凭证对应的授权支付账户的核身验证过程。

6、根据权利要求3所述的方法，所述判断所述支付请求对应的交易是否存在交易风险之前，还包括：

基于所述支付请求, 确定发起所述支付请求的发起时间;

判断所述发起时间是否在所述授权凭证的有效期限内, 得到第五判断结果;

若所述第五判断结果表示所述发起时间不在所述授权凭证的有效期限内, 则进行包含第四核身验证的第五支付流程;

所述判断所述支付请求对应的交易是否存在交易风险, 具体包括:

若所述第五判断结果表示所述发起时间在所述授权凭证的有效期限内, 则基于所述账户状态信息, 判断所述支付请求对应的交易是否存在交易风险。

7、根据权利要求 1 所述的方法, 所述基于所述账户状态信息, 判断所述支付请求对应的交易是否存在交易风险, 具体包括:

基于所述账户状态信息, 确定风险评估依据信息; 所述风险评估依据信息包括接收所述用户的支付操作的终端的设备标识、所述终端的 GPS 位置信息、所述终端的 IP 地址信息中至少一种;

基于所述风险评估依据信息, 判断所述支付请求对应的交易是否存在交易风险。

8、根据权利要求 7 所述的方法, 所述基于所述风险评估依据信息, 判断所述支付请求对应的交易是否存在交易风险, 具体包括:

基于所述账户状态信息, 确定所述授权支付账户的常用登录设备的设备标识;

判断所述接收所述用户的支付操作的终端的设备标识与所述常用登录设备的设备标识是否一致;

若一致, 则确定所述支付请求对应的交易不存在交易风险;

若不一致, 则确定所述支付请求对应的交易存在交易风险;

或者,

基于所述账户状态信息, 确定所述授权支付账户的绑定设备的设备标识; 所述绑定设备为预先与所述支付账户设定为绑定关系的设备;

判断所述接收所述用户的支付操作的终端的设备标识与所述绑定设备的设备标识是否一致;

若一致, 则确定所述支付请求对应的交易不存在交易风险;

若不一致, 则确定所述支付请求对应的交易存在交易风险。

9、根据权利要求 7 所述的方法, 所述基于所述风险评估依据信息, 判断所述支付请求对应的交易是否存在交易风险, 具体包括:

基于所述账户状态信息, 确定所述终端的 IP 地址信息;

根据所述授权支付账户的标识信息, 确定所述授权支付账户的前一次成功交易的 IP 地址信息;

判断所述终端的 IP 地址信息与所述授权支付账户的前一次成功交易的 IP 地址信息是否一致;

若一致, 则确定所述支付请求对应的交易不存在交易风险;

若不一致, 则确定所述支付请求对应的交易存在交易风险;

或者,

基于所述账户状态信息, 确定所述终端的 IP 地址信息;

根据所述授权支付账户的标识信息, 确定所述授权支付账户的常用交易 IP 地址信息;

判断所述终端的 IP 地址信息与所述授权支付账户的常用交易 IP 地址信息是否一致;

若一致, 则确定所述支付请求对应的交易不存在交易风险;

若不一致, 则确定所述支付请求对应的交易存在交易风险。

10、根据权利要求 7 所述的方法, 所述基于所述风险评估依据信息, 判断所述支付请求对应的交易是否存在交易风险, 具体包括:

基于所述账户状态信息, 确定所述终端的设备标识;

基于所述终端的设备标识, 确定所述终端的地理位置信息;

根据所述授权支付账户的标识信息, 确定所述授权支付账户对应的成功交易的常用地理位置信息;

判断所述终端的地理位置信息与所述授权支付账户对应的成功交易的常用地理位置信息是否一致;

若一致, 则确定所述支付请求对应的交易不存在交易风险;

若不一致, 则确定所述支付请求对应的交易存在交易风险。

11、根据权利要求 1 所述的方法, 所述授权支付账户包括至少一个支付子账户;

所述执行第一支付流程, 具体包括:

确定针对各个支付子账户预设的第一支付顺序;

按照所述第一支付顺序, 将所述各个支付子账户中首个账户余额大于或等于所述支付请求对应的支付金额的支付子账户确定为第一目标支付账户;

从所述第一目标支付账户中扣除所述支付金额。

12、根据权利要求 5 所述的方法, 所述执行包含第一核身验证过程的第二支付流程, 具体包括:

发送第二支付验证指示信息至所述终端, 以便所述用户根据所述第二支付验证指示信息输入第二支付验证信息;

接收所述用户输入的所述第二支付验证信息;

判断所述第二支付验证信息是否与针对所述授权凭证对应的授权支付账户预先设置的支付验证信息一致;

若一致, 则从所述授权支付账户中扣除所述支付请求对应的支付金额。

13、根据权利要求 12 所述的方法, 所述授权支付账户包括至少一个授权支付子账户;

所述发送第二支付验证指示信息至所述终端之前, 还包括:

确定针对各个授权支付子账户预设的第二支付顺序;

按照所述第二支付顺序, 将所述各个授权支付子账户中首个账户余额大于或等于所述支付请求对应的支付金额的授权支付子账户确定为第二目标支付账户;

所述发送第二支付验证指示信息至所述终端, 具体包括:

发送针对所述第二目标支付账户的第二支付验证指示信息至所述终端;

所述判断所述第二支付验证信息是否与针对所述授权凭证对应的授权支付账户预先设置的支付验证信息一致, 具体包括:

所述判断所述第二支付验证信息是否与针对所述第二目标支付账户预先设置的支付验证信息一致;

所述从所述授权支付账户中扣除所述支付请求对应的支付金额, 具体包括:

从所述第二目标支付账户中扣除所述支付请求对应的支付金额。

14、根据权利要求 4 所述的方法, 所述执行包含第三核身验证过程的第四支付流程, 具体包括:

发送第三支付验证指示信息至所述终端, 以便所述用户根据所述第三支付验证指示信息输入第三支付验证信息;

接收所述用户输入的所述第三支付验证信息;

判断所述第三支付验证信息是否与针对所述登录支付账户预先设置的支付验证信息一致;

若一致, 则从所述登录支付账户中扣除所述支付请求对应的支付金额。

15、根据权利要求 14 所述的方法, 所述登录支付账户包括至少一个登录支付子账户;

所述发送第三支付验证指示信息至所述终端之前, 还包括:

确定针对各个所述登录支付子账户预设的第三支付顺序；

按照所述第三支付顺序，将所述各个登录支付子账户中首个账户余额大于或等于所述支付请求对应的支付金额的登录支付子账户确定为第三目标支付账户；

所述发送第三支付验证指示信息至所述终端，具体包括：

发送针对所述第三目标支付账户的第三支付验证指示信息至所述终端；

所述判断所述第三支付验证信息是否与针对所述登录支付账户预先设置的支付验证信息一致，具体包括：

所述判断所述第三支付验证信息是否与针对所述第三目标支付账户预先设置的支付验证信息一致；

所述从所述登录支付账户中扣除所述支付请求对应的支付金额，具体包括：

从所述第三目标支付账户中扣除所述支付请求对应的支付金额。

16、一种支付信息处理的装置，包括：

请求获取模块，用于获取目标机构发送的基于用户的支付操作生成的支付请求；

所述支付请求包括授权支付账户的标识信息；所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户；

信息确定模块，用于确定所述授权支付账户的账户状态信息；

第一判断模块，用于基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险，得到第一判断结果；

第一流程模块，用于若所述第一判断结果表示所述交易不存在交易风险，则执行第一支付流程；

第二流程模块，用于若所述第一判断结果表示所述交易存在交易风险，则执行包含第一核身验证过程的第二支付流程。

17、根据权利要求 16 所述的装置，所述支付请求包括支付金额；所述装置还包括：

第二判断模块，用于基于所述支付请求，判断所述支付金额是否小于或等于预设支付金额，得到第二判断结果；

第三流程模块，用于若所述第二判断结果表示所述支付金额大于所述预设支付金额，则执行包含第二核身验证过程的第三支付流程；

所述第一判断模块，具体用于：

若所述第二判断结果表示所述支付金额小于或等于所述预设支付金额，则基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险。

18、根据权利要求 16 所述的装置，所述第一判断模块具体用于：

基于所述账户状态信息，确定风险评估依据信息；所述风险评估依据信息包括接收所述用户的支付操作的终端的设备标识、所述终端的 GPS 位置信息、所述终端的 IP 地址信息中至少一种；

基于所述风险评估依据信息，判断所述支付请求对应的交易是否存在交易风险。

19、一种支付信息处理的设备，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

获取目标机构发送的基于用户的支付操作生成的支付请求；所述支付请求包括授权支付账户的标识信息；所述授权支付账户为预先与所述目标机构建立免密支付授权关系的支付账户；

确定所述授权支付账户的账户状态信息；

基于所述账户状态信息，判断所述支付请求对应的交易是否存在交易风险，得到第一判断结果；

若所述第一判断结果表示所述交易不存在交易风险，则执行第一支付流程；

若所述第一判断结果表示所述交易存在交易风险，则执行包含第一核身验证过程的第二支付流程。

20、一种计算机可读介质，其上存储有计算机可读指令，所述计算机可读指令可被处理器执行以实现权利要求 1 至 15 中任一项所述的支付信息处理的方法。