(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 7 月 23 日 (23.07.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/147586 A1

(51) 国际专利分类号:
G06Q 20/40 (2012.01)

(21) 国际申请号: PCT/CN2020/070028

(22) 国际申请日: 2020 年 1 月 2 日 (02.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910035166.X 2019年1月15日 (15.01.2019) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 陈春宝 (**CHEN, Chunbao**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 陈卉佳 (**CHEN, Huijia**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 彭姝雯 (**PENG, Shuwen**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

(54) **Title:** RISK TRANSACTION PROCESSING METHOD AND APPARATUS, AND DEVICE

(54) 发明名称: 风险交易处理方法、装置及设备

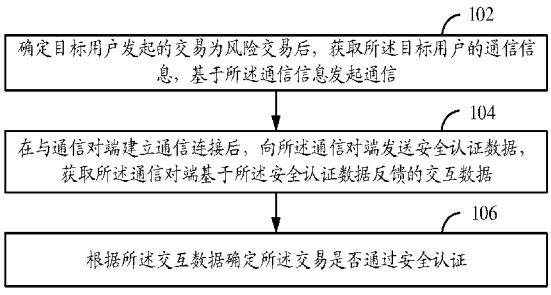

图 1A

102 After a transaction initiated by a target user is determined to be a risk transaction, obtain communication information of the target user, and initiate communication on the basis of the communication information

104 After a communication connection is established with a communication peer, send security authentication data to the communication peer so as to obtain interaction data fed back by the communication peer on the basis of the security authentication data

106 Determine whether the transaction passes security authentication according to the interaction data

(57) **Abstract:** A risk transaction processing method and apparatus, and a device. Communication can be initiated to a user being in a risk transaction, security authentication data is sent to a communication peer so as to obtain interaction data fed back by the communication peer on the basis of the security authentication data, and whether the transaction passes security authentication is determined according to the interaction data. Communication can be actively initiated to a user, and security authentication-based interaction data of the user is obtained by means of participation of the user, on the one hand, the user can be warned, whether the transaction passes the security authentication is determined, risks are directly released in the transaction process, the magnitude of manual disposal afterwards is reduced, and the pressure of a server is relieved; and on the other hand, security authentication is further performed on risk transactions to reduce transaction risks.

(57) 摘要: 一种风险交易处理方法、装置及设备，能够对风险交易的用户发起通信，通过向通信对端发送安全认证数据，以获取通信对端基于所述安全认证数据反馈的交互数据，并根据所述交互数据确定所述交易是否通过安全认证。能够主动向用户发起通信，通过用户的参与获取到用户基于安全认证的交互数据，一方面可以警示用户并确定交易是否通过安全认证，在交易过程中直接释放风险，减少事后再人工处置的量级，缓解服务端压力；另一方面对风险交易进一步安全认证，能够降低交易风险。

WO 2020/147586 A1

[见续页]

BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

风险交易处理方法、装置及设备

技术领域

[01] 本说明书涉及互联网交易技术领域，尤其涉及风险交易处理方法、装置及设备。

背景技术

[02] 随着网络技术的发展，用户通过网络进行交易变得越来越方便，网络交易在给用户带来便利的同时，也带来了一定的风险。网络交易等业务系统中

[03] 通常会有一套风险防控体系，在识别出用户的交易具有风险后，用户的交易会被阻断。基于此，需要提供一种更灵活的风险交易处理方案。

发明内容

[04] 为克服相关技术中存在的问题，本说明书提供了风险交易处理方法、装置及设备。

[05] 根据本说明书实施例的第一方面，提供一种风险交易处理方法，所述方法包括:

[06] 确定目标用户发起的交易为风险交易后，获取所述目标用户的通信信息，基于所述通信信息发起通信;

[07] 在与通信对端建立通信连接后，向所述通信对端发送安全认证数据，获取所述通信对端基于所述安全认证数据反馈的交互数据;

[08] 根据所述交互数据确定所述交易是否通过安全认证。

[09] 可选的，所述根据所述交互数据确定所述交易是否通过安全认证，包括:

[10] 根据所述交互数据确定通信对端侧用户与所述目标用户是否为同一用户，以确定所述交易是否通过安全认证。

[11] 可选的，所述根据所述交互数据确定所述交易是否通过安全认证，包括:

[12] 获取通信对端侧的语音数据后，获取所述语音数据的声纹特征与所述目标用户的声纹特征的匹配结果，根据匹配结果确定所述交易是否通过安全认证。

[13] 可选的，所述安全认证数据包括：认证问题数据;

[14] 所述根据所述交互数据确定所述交易是否通过安全认证，包括:

[15] 获取通信对端侧的答案数据后，根据所述通信对端侧的答案数据与所述认证问题数据对应答案数据的匹配结果，确定所述交易是否通过安全认证。

[16] 可选的，所述认证问题数据基于对应答案数据为数字而设定。

[17] 可选的，所述通信信息包括可信手机号码;

[18] 所述基于所述通信信息发起通信，包括:

[19] 向所述可信手机号码发起呼叫。

[20] 可选的，所述可信手机号码基于如下信息确定:

[21] 与目标用户的账户绑定的手机号码、与客服联系过的手机号码、手机号码的归属地信息或手机号码的绑定时间。

[22] 可选的，在所述发起通信前，还包括:

[23] 对如下一种或多种信息进行通信前的预告:

[24] 发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。

[25] 可选的，还包括:

[26] 若与通信对端一次或多次无法建立通信连接，阻断所述交易。

[27] 可选的，所述方法还包括:

[28] 若所述交易通过安全验证，执行交易流程;

[29] 若所述交易未通过验证，阻止所述交易。

[30] 根据本说明书实施例的第二方面，提供一种风险交易处理方法，包括:

[31] 获取目标用户发起的交易的交易信息;

[32] 在基于所述交易信息确定所述交易为风险交易后，展示通信预告信息，所述通信预告信息用于指示服务方需要基于目标用户的通信信息发起通信，并对本次交易进行安全认证。

[33] 可选的，还包括:

[34] 展示通信确认入口，通过所述通信确认入口获取指示用户是否接受通信的消息并发送给服务方，以供服务方确定是否发起通信。

[35] 可选的，所述通信预告信息包括:

[36] 发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。

[37] 根据本说明书实施例的第三方面，提供一种风险交易处理装置，包括:

[38] 通信模块，用于：确定目标用户发起的交易为风险交易后，获取所述目标用户的通信信息，基于所述通信信息发起通信;

[39] 数据获取模块，用于：在与通信对端建立通信连接后，向所述通信对端发送安全认证数据，获取所述通信对端基于所述安全认证数据反馈的交互数据;

[40] 认证模块，用于：根据所述交互数据确定所述交易是否通过安全认证。

[41] 可选的，所述认证模块，用于:

[42] 根据所述交互数据确定通信对端侧用户与所述目标用户是否为同一用户，以确定所述交易是否通过安全认证。

[43] 可选的，所述认证模块，用于:

[44] 获取通信对端侧的语音数据后，获取所述语音数据的声纹特征与所述目标用户的声纹特征的匹配结果，根据匹配结果确定所述交易是否通过安全认证。

[45] 可选的，所述安全认证数据包括：认证问题数据;

[46] 所述认证模块，用于:

[47] 获取通信对端侧的答案数据后，根据所述通信对端侧的答案数据与所述认证问题数据对应答案数据的匹配结果，确定所述交易是否通过安全认证。

[48] 可选的，所述认证问题数据基于对应答案数据为数字而设定。

[49] 可选的，所述通信信息包括可信手机号码;

[50] 所述通信模块，用于:

[51] 向所述可信手机号码发起呼叫。

[52] 可选的，所述可信手机号码基于如下信息确定:

[53] 与目标用户的账户绑定的手机号码、与客服联系过的手机号码、手机号码的归属地信息或手机号码的绑定时间。

[54] 可选的，所述通信模块，还用于：在发起所述通信前，对如下一种或多种信息进行通信前的预告：

[55] 发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。

[56] 可选的，所述装置还包括阻断模块，用于：

[57] 若与通信对端一次或多次无法建立通信连接，阻断所述交易。

[58] 可选的，所述认证模块，还用于：

[59] 若所述交易通过安全验证，执行交易流程；

[60] 若所述交易未通过验证，阻止所述交易。

[61] 根据本说明书实施例的第四方面，提供一种风险交易处理装置，所述装置包括：

[62] 获取模块，用于：获取目标用户发起的交易的交易信息；

[63] 预告模块，用于：在基于所述交易信息确定所述交易为风险交易后，展示通信预告信息，所述通信预告信息用于指示服务方需要基于目标用户的通信信息发起通信，并对本次交易进行安全认证。

[64] 可选的，所述预告模块还用于：

[65] 展示通信确认入口，通过所述通信确认入口获取指示用户是否接受通信的消息并发送给服务方，以供服务方确定是否发起通信。

[66] 可选的，所述通信预告信息包括：

[67] 发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。

[68] 根据本说明书实施例的第五方面，提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现前述风险交易处理方法。

[69] 本说明书的实施例提供的技术方案可以包括以下有益效果：

[70] 本说明书实施例中，能够对风险交易的用户主动发起通信，通过向通信对端发送安全认证数据，以获取通信对端基于所述安全认证数据反馈的交互数据，并根据所述交互数据确定所述交易是否通过安全认证。本实施例提供了一种在交易过程中的主动安全

服务，能够主动向用户发起通信，通过用户的参与获取到用户基于安全认证的交互数据，一方面可以警示用户并确定交易是否通过安全认证，在交易过程中直接释放风险，减少事后再人工处置的量级，缓解服务端压力；另一方面对风险交易进一步安全认证，能够降低交易风险。

[71] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书。

附图说明

[72] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本说明书的实施例，并与说明书一起用于解释本说明书的原理。

[73] 图 1A 是本说明书根据一示例性实施例示出的一种风险交易处理方法的流程图。

[74] 图 1B 是本说明书根据一示例性实施例示出的一种风险交易示意图。

[75] 图 2A 是本说明书根据一示例性实施例示出的另一种风险交易处理方法的流程图。

[76] 图 2B 至图 2D 是本说明书根据一示例性实施例示出的一种风险交易处理示意图。

[77] 图 3 是本说明书根据一示例性实施例示出的一种风险交易处理装置所在计算机设备的结构框图。

[78] 图 4 是本说明书根据一示例性实施例示出的一种风险交易处理装置的框图。

[79] 图 5 是本说明书根据一示例性实施例示出的另一种风险交易处理装置的框图。

具体实施方式

[80] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的装置和方法的例子。

[81] 在本说明书使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书。在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[82] 应当理解，尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[83] 移动互联、密码技术、大数据和人工智能等新技术的快速发展，丰富了支付手段也提高了支付效率，但同时带来了新的风险隐患，对交易风险防控提出了更高要求。目前交易风险包括有欺诈类风险，主要是非本人交易和本人恶意进行的不当交易，例如账户盗用、伪卡欺诈、失窃卡欺诈、非面欺诈、营销欺诈、商户合谋等；还有一类是合规风险，主要是违反法律法规或监管要求的不当交易，例如洗钱、电信诈骗、非法集资、套现或移机切机等。

[84] 为应对这些风险，业务系统可以通过交易行为分析、机器学习等方式不断优化风控模型，提高欺诈交易拦截成功率和安全防护能力；在流程上通常采取防御型管控措施，以交易风险管控为例：

[85] 1）交易发起后风控模型识别风险；

[86] 2）根据风险类型和风险评级采取拦截阻断（如冻结账户、失败交易）、挂起确认（如二次身份认证）或批准通过等措施；

[87] 3）对于被阻断的交易，用户可向客服电话举证，通过后可重新发起交易。

[88] 基于此，本说明书实施例提供一种更为灵活的风险交易处理方法，能够对风险交易的用户发起通信，通过向通信对端发送安全认证数据，以获取通信对端基于所述安全认证数据反馈的交互数据，并根据所述交互数据确定所述交易是否通过安全认证。接下来对本说明书实施例进行详细说明。

[89] 如图 1A 所示，图 1A 是本说明书根据一示例性实施例示出的一种风险交易处理方法的流程图，包括以下步骤：

[90] 在步骤 102、确定目标用户发起的交易为风险交易后，获取所述目标用户的通信信息，基于所述通信信息发起通信。

[91] 在步骤 104、在与通信对端建立通信连接后，向所述通信对端发送安全认证数据，获取所述通信对端基于所述安全认证数据反馈的交互数据。

[92] 在步骤 106、根据所述交互数据确定所述交易是否通过安全认证。

[93] 本说明书实施例的方案可应用于提供交易服务的业务系统中，上述步骤的执行主体具体可以包括服务端或客户端，并且不限制是否只在其中一端执行。本实施例方案是在发现风险交易后，通过与用户的主动通信交互来进一步对交易进行安全认证。由于采用了主动通信的方式，在确定目标用户发起的交易为风险交易后，可以获取所述目标用户的通信信息，基于所述通信信息发起通信，可以警示用户并确定交易是否通过安全认证，在交易过程中直接释放风险，减少事后再人工处置的量级，缓解服务端压力。

[94] 其中，发起通信的方式可以根据需要灵活配置，可选的，可以是语音通信，以达到与用户语音交互的效果。具体的，可以是结合视频的语音通信，也可以是单纯的语音通信。实际实现时，可以是服务端向客户端发起网络通信，此种方式需要客户端与服务端处于连接状态；作为例子，用户通过个人计算机中的浏览器发起交易，本实施例的方案可以要求用户利用智能手机等移动设备的客户端登录服务端，并由服务端获取该目标用户的通信信息，具体可以包括用户的常用设备的通信地址（如 IP 地址、设备 MAC 地址），服务端可以基于通信地址向客户端发起网络通信，例如语音通话或视频通话等方式。或者，也可以是用户登录服务端发起交易，服务端可以直接向客户端发起语音通信。

[95] 在另一些例子中，通信信息可以是用户的可信手机号码，服务端可以向所述可信手机号码发起呼叫。可选的，本实施例可以通过智能语音技术实现，可以预先配置智能呼叫程序，以用于自动发起电话呼叫，减少人工压力。可选的，用户可能有一个或多个手机号码，本实施例方案中，可以确定目标用户的可信手机号码，以防止呼叫错误、确保能够呼叫给正确的用户。可选的，目标用户的可选手机号码可以基于如下信息确定：与目标用户的账户绑定的手机号码、与客服联系过的手机号码、手机号码的归属地信息或手机号码的绑定时长。作为例子，目标用户的账户可能绑定过一个或多个手机号码，可以获取各个手机号码的绑定时间综合考虑；还可以是获取目标用户与客户服务电话的历史联系记录，以通过历史联系记录获取目标用户利用哪个电话号码与客服联系；由于涉及到目标用户的多个手机号码，还可以根据手机号码的归属地信息进一步综合考虑，与用户的常用所在地相匹配的手机号码会更为可选。实际应用中，作为一个可选的方式，可以根据需要建立可信手机模型，该可信手机模型可以根据支付宝账户绑定手机、近期来电和客服沟通手机、支付宝账户使用时的设备指纹、手机号码的归属地信息、手机号码的绑定时间等信息作为特征，用以判断用户当前真正在使用的手机号码，确定呼叫给正确的用户。

[96] 可以理解，发起的通信可能能够成功建立通信连接，也可能无法建立通信连接。可选的，若与通信对端一次或多次无法建立通信连接，因为无法通过与用户交互而对交易进行安全认证，可以直接阻断所述交易。

[97] 在能够成功建立通信连接的情况下，可以向所述通信对端发送安全认证数据，获取所述通信对端基于所述安全认证数据反馈的交互数据。上述处理是考虑到风控模型只是基于交易信息而做出的判断，风险模型并未经过用户交互而将交易直接判定为风险交易，本实施例希望能够通过主动通信与用户交互、通过用户的参与进一步对交易进行更为可靠的安全认证。可选的，考虑到实际盗刷或诈骗等场景的特点，安全认证可以是对通信对端用户进行活体认证，可以是确定通信对端侧用户与所述目标用户是否为同一用户，可以是对通信对端侧用户进行询问以对交易进一步确认风险等等。作为例子，可以基于问答用户的个人身份信息、可以询问用户是否是本人的正常交易、可以对交易发起对象进行活体认证或可以获取用户的生物特征(如人脸特征或声纹特征等)等多种方式，实际应用中可以根据需要灵活配置安全认证数据的实现方式，以获取所述通信对端基于所述安全认证数据反馈的交互数据。

[98] 作为例子，可以要求通信对端侧发声，以获取通信对端侧的语音数据作为交互数据，通过获取所述语音数据的声纹特征与所述目标用户的声纹特征的匹配结果，根据匹配结果确定所述交易是否通过安全认证。可选的，服务方可以预先通过多种方式获取用户的语音数据，以提取出表征用户身份的语音特征。通过上述方式，可以判断通信对端侧是否是活体、判断通信对端侧的用户与发起交易的用户是否是同一用户。

[99] 在另一些例子中，还可以与通信对端侧视频通话，通过获取摄像头采集视频数据，从视频数据中获取通信对端侧用户的人脸特征，将通信对端侧用户的人脸特征与目标用户的人脸特征匹配，根据匹配结果确定所述交易是否通过安全认证。

[100] 可选的，可以通过问答的方式对通信对端侧用户与目标用户进行验证，其中，安全认证数据可以包括：认证问题数据；所述根据所述交互数据确定所述交易是否通过安全认证，包括：获取通信对端侧发送的答案数据后，根据所述通信对端侧发送的答案数据与所述认证问题数据对应的答案数据的匹配结果，确定所述交易是否通过安全认证。可选的，认证问题数据可以是一表征问题的语音数据，播放该语音数据后，由用户对该问题进行回答，可选的，实际实现时可以由用户通过语音回答，也可以由用户触发设备展示的虚拟键盘进行回答等。可选的，本实施例的认证问题数据可以基于对应答案数据为数字而设定，例如可以是表征询问身份证号码、询问随机数、询问年龄等认证问题数

据，由于此类问题数据的答案是数字，可以令用户便捷地通过数字键盘输入，从而可提高处理效率。

[101] 作为例子，认证问题数据可以是一表征询问用户身份证号码的语音数据，通信对端侧设备可以播放该认证问题数据，通信对端侧设备还可以展示数字键盘，以供用户输入对应答案；发起通信的服务端可以获取通信对端侧的答案数据，以通过答案数据识别出用户所输入的数字是否与发起交易的用户的身份证号码匹配。

[102] 在另一些例子中，认证问题数据可以是一表征随机数的语音数据，该随机数可以根据需要实时生成，并可利用智能语音技术生成表征该随机数的语音数据，通信对端侧设备可以播放该认证问题数据，以使用户收听到该认证问题数据后，可以输入对应的随机数；通信对端侧设备还可以展示数字键盘，以供用户输入；发起通信的服务端可以获取通信对端侧的答案数据，以通过答案数据识别出用户所输入的数字是否与生成的随机数匹配。

[103] 通过上述方式，可以确定通信对端侧用户与所述目标用户是否为同一用户，可以确定发起交易的对象是否为活体用户，也可以确定目标用户是否真的有发起交易防止账户盗用，还可以在用户真正付款前起到安全警示的作用。

[104] 可选的，为了提高通信效率、防止用户未接受服务方发起的通信，本实施例中，在所述发起通信前，还可以包括：对如下一种或多种信息进行通信前的预告：发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。可选的，上述提醒可以在目标用户发起交易的设备中实现，例如，如图 1B 所示，是本说明书实施例提供的一客户端示意图，目标用户采用客户端发起交易，可以由客户端展示上述预告，其中，图 1B 的预告中示出了表征发起呼叫的电话号码的“0571-88880123”，表征可信手机号码的“187****1234”，表征发起呼叫的服务方标识的“支付宝”，表征本次呼叫用于进行针对交易的安全认证的“为保障交易安全，请使用 187****1234 接听支付宝来电，并根据提示验证身份”等信息。在另一些例子中，若目标用户采用浏览器登录服务页面发起交易，可以在服务页面中输出一窗口以展示上述提醒。通过上述提醒，可以使用户获知服务方即将发起通信以对交易进行安全认证，从而可以提高通信连接的概率，提高通信效率，防止用户拒绝通信。

[105] 由前述描述可知，本说明书对上述风险交易处理实施例的执行主体并未限制；接下来从客户端的角度进一步提供另一风险交易处理实施例，该实施例可应用于客户端，当用户使用客户端发起交易后，客户端可执行如图 2A 所示实施例的方法，包括如下步

骤:

[106] 在步骤 202 中，获取目标用户发起的交易的交易信息。

[107] 在步骤 204 中，在基于所述交易信息确定所述交易为风险交易后，展示通信预告信息，所述通信预告信息用于指示服务方需要基于目标用户的通信信息发起通信，并对本次交易进行安全认证。

[108] 本实施例可应用于提供交易功能的客户端中，用户可以通过客户端发起交易，客户端通过检测用户发起的交易操作后，确定目标用户的账户、以及交易地点、交易时间、交易金额等交易相关信息。利用上述交易信息，可以利用风控模型识别交易的风险及类型，其中，上述对交易的风险识别过程可以是在客户端本端执行，也可以是在服务端执行。若是在服务端执行，客户端可以接收服务端对该笔交易的识别结果，若是在客户端执行，客户端可以向服务端发送识别结果。在确定该笔交易为风险交易后，服务方需要进一步对本次交易发起通信以进行安全认证。为了保证能够顺利与用户通信，本实施例中客户端可以展示通信预告信息，用于指示服务方需要基于目标用户的通信信息发起通信，并对本次交易进行安全认证。其中，该通信预告信息可以是存储在客户端本地，也可以是从服务端侧获取到。

[109] 结合图 2B 至图 2D 所示的风险交易处理示意图进一步描述，本实施例中用户利用客户端发起交易，服务方在确定交易发起后，可以判断本次交易是否适用通信认证，可选的，条件可以包括:

[110] 1）风控模型判断本笔交易具有高风险，按照原有流程本次交易将被直接阻断拦截;

[111] 2）风控模型确定本次交易符合骗盗结合或欺诈场景，原有核身产品不再有效;

[112] 3）发起交易的用户具有可信手机号码，能确保语音拨给用户本人。

[113] 可选的，在通信发起之前，服务端可以利用客户端进行通信前的预告提醒，以通知用户服务方将与其电话交互，由用户根据所处环境决定是否接听，通知内容可以包括:

[114] 1）发起呼叫的电话号码，以防诈骗电话趁机而入。

[115] 2）用户的可信手机号码，以便用户提前准备接听。

[116] 3）发起呼叫的服务方标识，以使用户获知呼入者为服务方；可选的，服务方标识可以是服务方的名称、简称或其他等为用户熟知的名称。

[117] 4）文案内容，以对本次呼叫用于进行针对交易的安全认证进行提示，例如本次交

互是为保障资金安全而做的身份核实。

[118] 5）接听选项；可选的，本实施例提供有通信确认入口，通过所述通信确认入口获取指示用户是否接受通信的消息并发送给服务方，以供服务方确定是否发起通信；在图2B 中，该通信确认入口包括“立即接听”选项及“无法接听”选项，通过提供该接听选项，可以供用户触发，以确定用户愿意接受来电呼入。

[119] 接通后，服务端与通信对端成功建立了通信连接，进一步可以与用户交互，包括如下一种或多种：

[120] 1）需要与用户确认交易，服务端生成随机数后生成表征该随机数的语音数据并发送给通信对端，以使通信对端设备能够播放该语音数据后，用户输入语音播报的随机数；

[121] 2）身份核实，例如服务端生成表征询问身份证号码的语音数据并发送给通信对端播放，使用户可以按语音提示输入身份证号；或者，可以是让用户说话后通过声纹比对，可选的，还可以生成认证问题数据并发送给通信对端播放，使用户可以按语音提示说话以提供答案数据，以通过答案数据进一步进行安全认证；

[122] 3）用户问答，如用户有其他问题可直接语音交互或选择进入人工服务。

[123] 其中，如未接通，可以重新拨打一次或多次，重播一次或多次后仍未接通则按原有流程操作，对交易阻断拦截，进入服务环节。

[124] 最后，服务端根据实际的语音交互情况对该笔交易进行处理，包括：

[125] 1）核实通过，提示交易成功，执行交易流程；

[126] 2）核实不通过，提示交易失败并指引用户按照固有安全方式重新发起交易；

[127] 3）核实不通过，也根据风险情况继续阻断拦截，引导进入人工审核。

[128] 本实施例提供的方案可以与风险防控策略相结合而解决社工、欺诈类风控难点。因信息泄露导致的社工欺骗和欺诈是交易风险的主要成因，黑产团伙冒充商家、公检法或采用提升额度、办理贷款及大额信用卡等骗术骗取用户短信验证码或身份证件等信息，用户在被骗或者无意识情况下帮助黑产团伙通过身份认证，这类风险由于用户参与其中，防范难度较大。

[129] 另外，由于风控系统的保护，用户处于无感知被保护状态，风险暴露后敞口持续存在，容易发生二次风险。一些风控模型在侦测到交易风险之后，出于交易体验的考虑，有可能并非全部进行阻断或者要求身份认证，在风险评级较低、金额较小或特定时期，

可能会批准通过一部分风险交易；对于不关注账户的用户来说并不能马上感知到风险，未对账户做出加强安全的措施，风控系统也可能因缺乏用户反馈而将本次交易判定为安全交易，下一次再发生时可能会继续批准，从而发生二次风险。

[130] 本实施例方案通过主动发起的通信，可以采用声纹、语音+X（X 可以是上述实施例中的随机数、身份证或安保问题等）等认证技术对交易进行安全认证，让黑产团伙无法绕过安全认证。通过语音交互的直接沟通能唤起用户安全意识，进一步降低用户被骗的几率。语音认证技术相较密码可以降低安全验证失败率，提升用户支付体验。

[131] 本实施例通过主动提醒可以提升账户安全水位。针对大量存在的低免疫账户和易被骗/诈人群、每日风险暴露人群，因缺少合适的触达方式而放置不理直至发生风险，借助语音开展尽责提醒和主动沟通，有助于在事前化解风险，同时增强用户安全感。

[132] 对于骗盗结合等风险类型，由于支付过程中缺乏有效的风险释放渠道，往往采取失败交易或冻结账户的措施，用户事后来电举证以恢复账户，审核负荷就传递到了服务端，对服务方造成了一定的人工压力。本实施例在交易过程中主动发起通信进行认证，能够释放风险、减少拦截阻断交易外，对于已经冻结账户的用户可以及时通过语音外呼引导至自助服务渠道，因此可以有效缓解服务端资源压力。

[133] 传统的风险交易直接会被阻断或挂起，部分用户误以为网络或者账户出现了问题，在服务方没有及时提醒和沟通的情况下，用户可能会采用其他渠道完成本次交易，甚至后续也不再使用该账户，从而造成一定的用户流失。本实施例根据测算，被拦截阻断交易的用户中 30%将转为睡眠（一个月内不再发生交易），而 80%的风险可以在支付过程中沟通、确认，但因客服人力有限，本实施例采用主动发起通信的方式能及时解决风险交易问题，借助语音技术能够解决上述弊端，进而可以提升用户活跃率。

[134] 本实施例方案提供了的主动安全的服务，相对传统的识别风险——账户管控——用户通过核身或来电举证的防御型风控流程相比，通过事前主动提醒、事中主动沟通和事后跟进关怀的主动式安全服务，建立起用户参与的闭环风控流程，解决信息泄露、社工欺骗等风控难题。

[135] 与前述风险交易处理方法的实施例相对应，本说明书还提供了风险交易处理装置及其所应用的终端的实施例。

[136] 本说明书风险交易处理装置的实施例可以应用在计算机设备上，例如服务器或终端设备。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。

以软件实现为例，作为一个逻辑意义上的装置，是通过其所在文件处理的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图3所示，为本说明书风险交易处理装置所在计算机设备的一种硬件结构图，除了图3所示的处理器310、内存330、网络接口320、以及非易失性存储器340之外，实施例中装置331所在的服务器或电子设备，通常根据该计算机设备的实际功能，还可以包括其他硬件，对此不再赘述。

[137] 如图4所示，图4是本说明书根据一示例性实施例示出的一种风险交易处理装置的框图，所述装置包括:

[138] 通信模块41，用于：确定目标用户发起的交易为风险交易后，获取所述目标用户的通信信息，基于所述通信信息发起通信;

[139] 数据获取模块42，用于：在与通信对端建立通信连接后，向所述通信对端发送安全认证数据，获取所述通信对端基于所述安全认证数据反馈的交互数据;

[140] 认证模块43，用于：根据所述交互数据确定所述交易是否通过安全认证。

[141] 可选的，所述认证模块，用于:

[142] 根据所述交互数据确定通信对端侧用户与所述目标用户是否为同一用户，以确定所述交易是否通过安全认证。

[143] 可选的，所述认证模块，用于:

[144] 获取通信对端侧的语音数据后，获取所述语音数据的声纹特征与所述目标用户的声纹特征的匹配结果，根据匹配结果确定所述交易是否通过安全认证。

[145] 可选的，所述安全认证数据包括：认证问题数据;

[146] 所述认证模块，用于:

[147] 获取通信对端侧的答案数据后，根据所述通信对端侧的答案数据与所述认证问题数据对应答案数据的匹配结果，确定所述交易是否通过安全认证。

[148] 可选的，所述认证问题数据基于对应答案数据为数字而设定。

[149] 可选的，所述通信信息包括可信手机号码;

[150] 所述通信模块，用于:

[151] 向所述可信手机号码发起呼叫。

[152] 可选的，所述可信手机号码基于如下信息确定:

[153] 与目标用户的账户绑定的手机号码、与客服联系过的手机号码、手机号码的归属地信息或手机号码的绑定时间。

[154] 可选的，所述通信模块，还用于：在发起所述通信前，对如下一种或多种信息进行通信前的提醒:

[155] 发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。

[156] 可选的，所述装置还包括阻断模块，用于:

[157] 若与通信对端一次或多次无法建立通信连接，阻断所述交易。

[158] 可选的，所述认证模块，还用于:

[159] 若所述交易通过安全验证，执行交易流程;

[160] 若所述交易未通过验证，阻止所述交易。

[161] 如图 5 所示，图 5 是本说明书根据一示例性实施例示出的一种风险交易处理装置的框图，所述装置包括:

[162] 获取模块 51，用于：获取目标用户发起的交易的交易信息;

[163] 预告模块 52，用于：在基于所述交易信息确定所述交易为风险交易后，展示通信预告信息，所述通信预告信息用于指示服务方需要基于目标用户的通信信息发起通信，并对本次交易进行安全认证。

[164] 可选的，所述预告模块还用于:

[165] 展示通信确认入口，通过所述通信确认入口获取指示用户是否接受通信的消息并发送给服务方，以供服务方确定是否发起通信。

[166] 可选的，所述通信预告信息包括:

[167] 发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。

[168] 上述风险交易处理装置中各个模块的功能和作用的实现过程具体详见上述风险交易处理方法中对应步骤的实现过程，在此不再赘述。

[169] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实

施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[170] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[171] 本领域技术人员在考虑说明书及实践这里申请的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未申请的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。

[172] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。

[173] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

权利要求书

1、一种风险交易处理方法，包括:

确定目标用户发起的交易为风险交易后，获取所述目标用户的通信信息，基于所述通信信息发起通信;

在与通信对端建立通信连接后，向所述通信对端发送安全认证数据，获取所述通信对端基于所述安全认证数据反馈的交互数据;

根据所述交互数据确定所述交易是否通过安全认证。

2、根据权利要求 1 所述的方法，所述根据所述交互数据确定所述交易是否通过安全认证，包括:

根据所述交互数据确定通信对端侧用户与所述目标用户是否为同一用户，以确定所述交易是否通过安全认证。

3、根据权利要求 1 所述的方法，所述根据所述交互数据确定所述交易是否通过安全认证，包括:

获取通信对端侧的语音数据后，获取所述语音数据的声纹特征与所述目标用户的声纹特征的匹配结果，根据匹配结果确定所述交易是否通过安全认证。

4、根据权利要求 1 所述的方法，所述安全认证数据包括：认证问题数据;

所述根据所述交互数据确定所述交易是否通过安全认证，包括:

获取通信对端侧的答案数据后，根据所述通信对端侧的答案数据与所述认证问题数据对应答案数据的匹配结果，确定所述交易是否通过安全认证。

5、根据权利要求 4 所述的方法，所述认证问题数据基于对应答案数据为数字而设定。

6、根据权利要求 1 所述的方法，所述通信信息包括可信手机号码;

所述基于所述通信信息发起通信，包括:

向所述可信手机号码发起呼叫。

7、根据权利要求 5 所述的方法，所述可信手机号码基于如下信息确定:

与目标用户的账户绑定的手机号码、与客服联系过的手机号码、手机号码的归属地信息或手机号码的绑定时间。

8、根据权利要求 5 所述的方法，在所述发起通信前，还包括:

对如下一种或多种信息进行通信前的预告:

发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。

9、根据权利要求 1 所述的方法，还包括:

若与通信对端一次或多次无法建立通信连接，阻断所述交易。

10、根据权利要求 1 所述的方法，所述方法还包括:

若所述交易通过安全验证，执行交易流程;

若所述交易未通过验证，阻止所述交易。

11、一种风险交易处理方法，包括:

获取目标用户发起的交易的交易信息;

在基于所述交易信息确定所述交易为风险交易后，展示通信预告信息，所述通信预告信息用于指示服务方需要基于目标用户的通信信息发起通信，并对本次交易进行安全认证。

12、根据权利要求 11 所述的方法，还包括:

展示通信确认入口，通过所述通信确认入口获取指示用户是否接受通信的消息并发送给服务方，以供服务方确定是否发起通信。

13、根据权利要求 11 所述的方法，所述通信预告信息包括:

发起呼叫的电话号码、所述可信手机号码、发起呼叫的服务方标识或本次呼叫用于进行针对交易的安全认证。

14、一种风险交易处理装置，包括:

通信模块，用于：确定目标用户发起的交易为风险交易后，获取所述目标用户的通信信息，基于所述通信信息发起通信;

数据获取模块，用于：在与通信对端建立通信连接后，向所述通信对端发送安全认证数据，获取所述通信对端基于所述安全认证数据反馈的交互数据;

认证模块，用于：根据所述交互数据确定所述交易是否通过安全认证。

15、一种风险交易处理装置，包括:

获取模块，用于：获取目标用户发起的交易的交易信息;

预告模块，用于：在基于所述交易信息确定所述交易为风险交易后，展示通信预告信息，所述通信预告信息用于指示服务方需要基于目标用户的通信信息发起通信，并对本次交易进行安全认证。

16、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如权利要求 1 至 13 任一所述的方法。

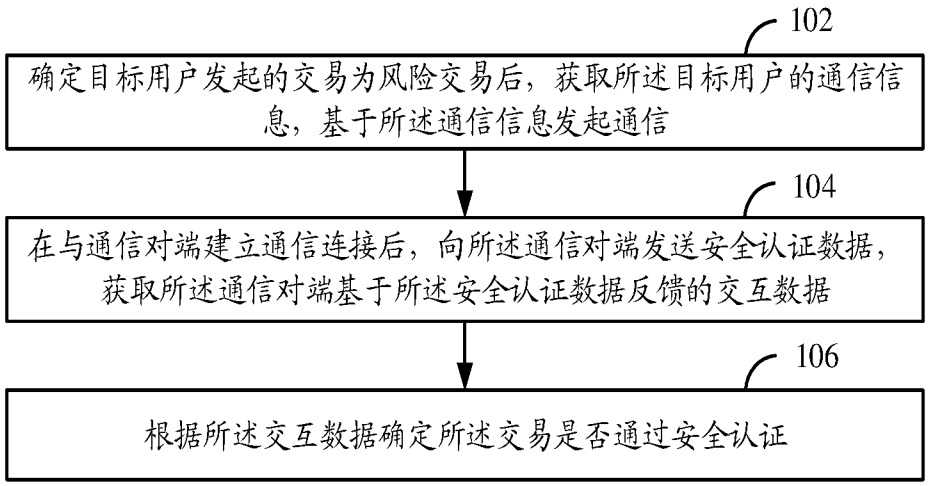
102
确定目标用户发起的交易为风险交易后，获取所述目标用户的通信信息，基于所述通信信息发起通信
104
在与通信对端建立通信连接后，向所述通信对端发送安全认证数据，获取所述通信对端基于所述安全认证数据反馈的交互数据
106
根据所述交互数据确定所述交易是否通过安全认证

图 1A

图 1B

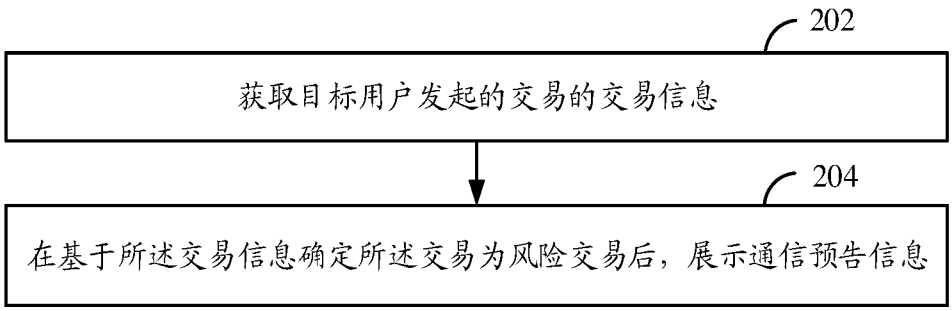
202
获取目标用户发起的交易的交易信息
204
在基于所述交易信息确定所述交易为风险交易后，展示通信预告信息

图 2A


¥18.40
判断是否命中条件
判断可信手机号是否可用
是

图 2B

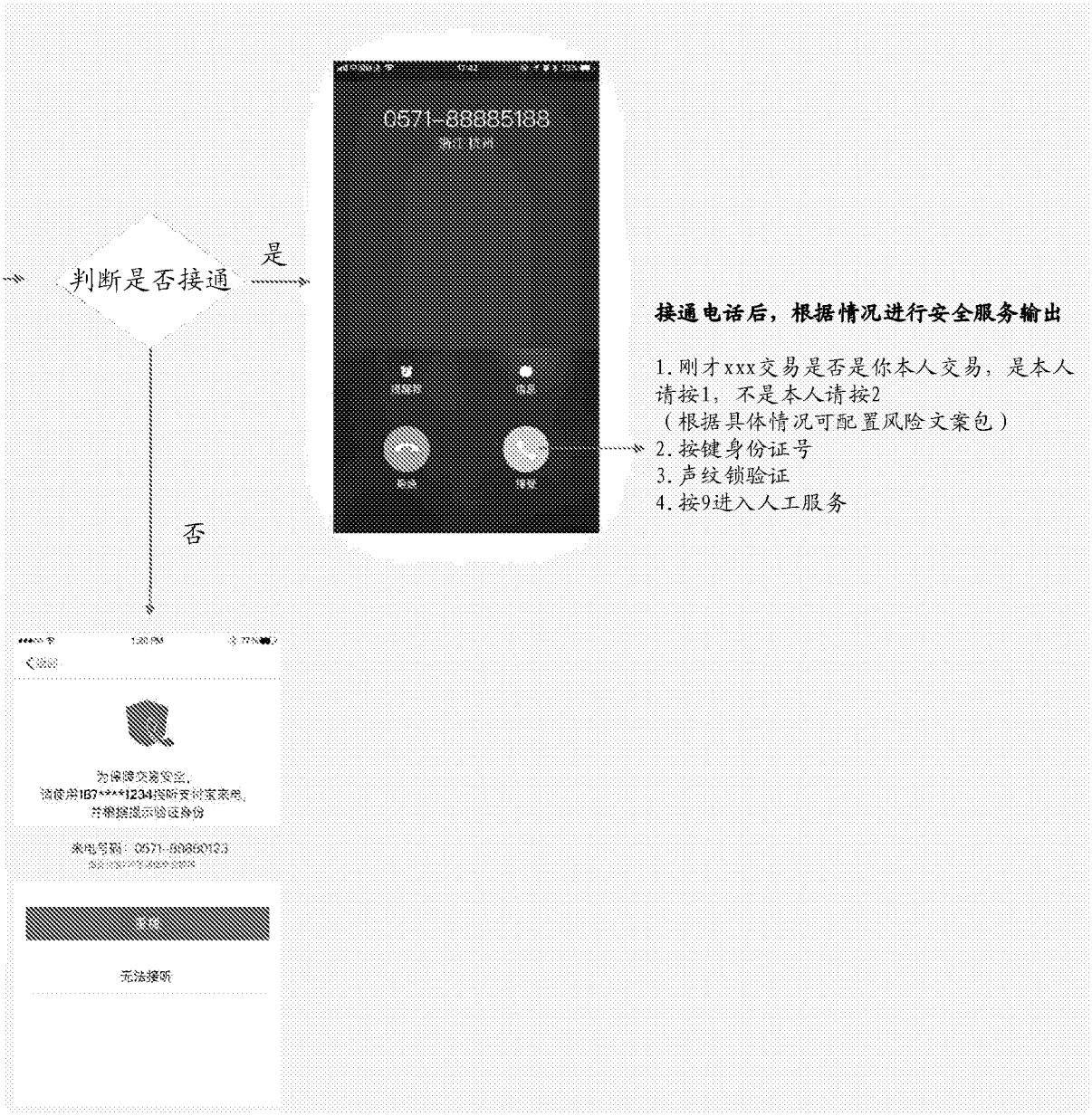
判断是否接通
是
否
0571-88885188
接通
挂断
接通电话后，根据情况进行安全服务输出
1.刚才xxx交易是否是你本人交易，是本人请按1，不是本人请按2
（根据具体情况可配置风险文案包）
2.按键身份证号
3.声纹锁验证
4.按9进入人工服务
无法接听

图 2C

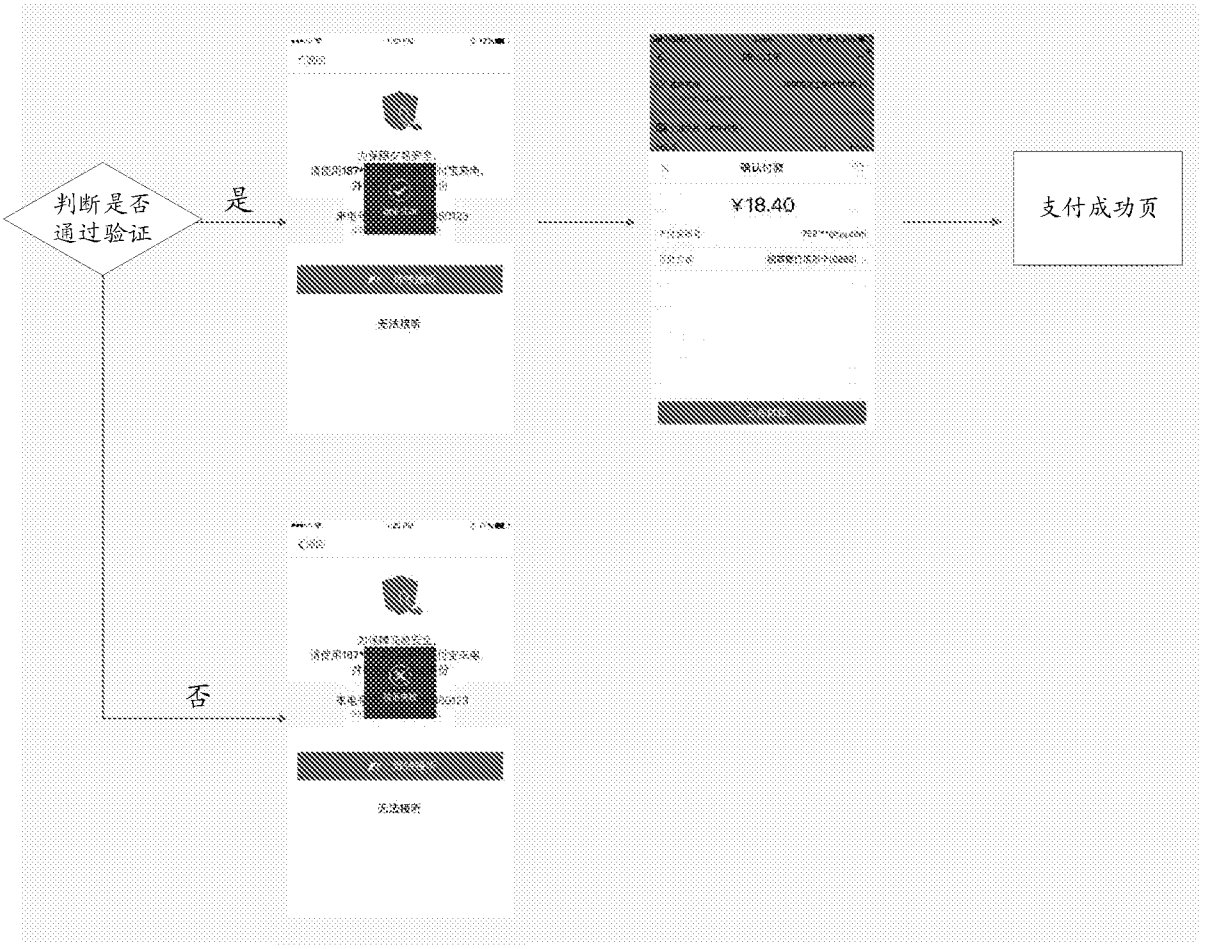
判断是否
通过验证
是
否
¥18.40
支付成功页

图 2D

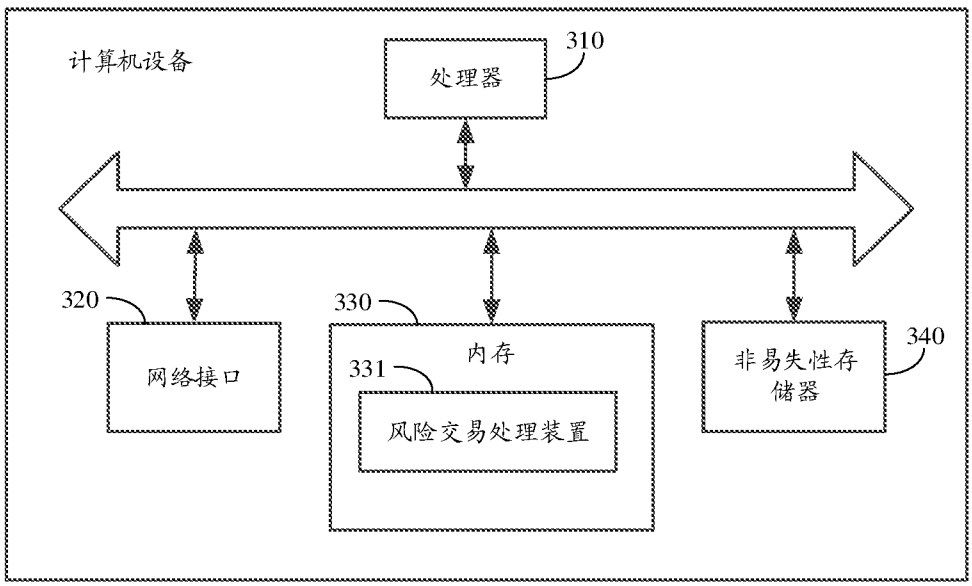
计算机设备
处理器
310
320
网络接口
330
内存
331
风险交易处理装置
非易失性存储器
340

图 3

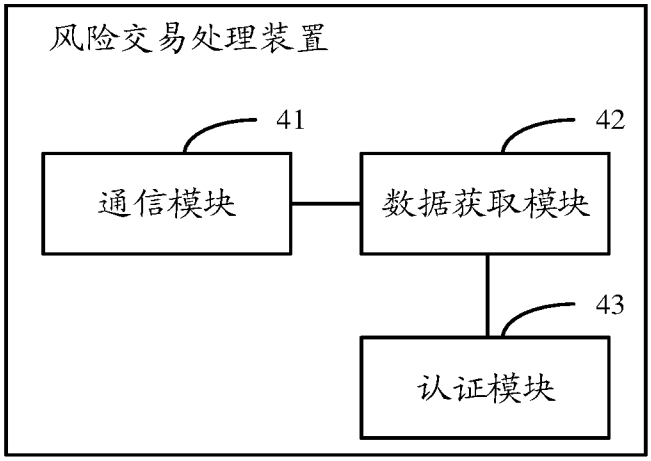

图 4

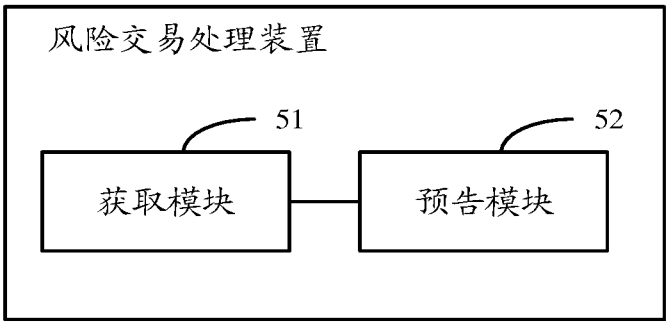

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/070028

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNKI, CNPAT, IEEE, GOOGLE: 风险, 交易, 安全, 认证, 验证, 反馈, risk, transaction, security, authentication, feedback

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110046902 A (ALIBABA GROUP HOLDING LIMITED) 23 July 2019 (2019-07-23) claims 1-16	1-16
X	CN 104753868 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.) 01 July 2015 (2015-07-01) description, paragraphs [0043]-[0058], and figure 1	1-16
X	CN 1801228 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 12 July 2006 (2006-07-12) description, page 7, line 22 to page 9, line 4, and figure 2	1-16
A	US 2014297522 A1 (JPMORGAN CHASE BANK, N.A.) 02 October 2014 (2014-10-02) entire document	1-16

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 March 2020	**26 March 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/070028

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110046902 A	23 July 2019	None	
CN 104753868 A	01 July 2015	WO 2015101036 A1	09 July 2015
		US 2015186892 A1	02 July 2015
CN 1801228 A	12 July 2006	None	
US 2014297522 A1	02 October 2014	US 8788410 B1	22 July 2014

国际检索报告

国际申请号
PCT/CN2020/070028

A. 主题的分类

G06Q 20/40(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI, EPODOC, CNKI, CNPAT, IEEE, GOOGLE: 风险, 交易, 安全, 认证, 验证, 反馈, risk, transaction, security, authentication, feedback

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 110046902 A (阿里巴巴集团控股有限公司) 2019年 7月 23日 (2019-07-23) 权利要求1-16	1-16
X	CN 104753868 A (腾讯科技深圳有限公司) 2015年 7月 1日 (2015-07-01) 说明书第43-58段, 附图1	1-16
X	CN 1801228 A (北京邮电大学) 2006年 7月 12日 (2006-07-12) 说明书第7页第22行-第9页第4行, 附图2	1-16
A	US 2014297522 A1 (JPMORGAN CHASE BANK, N.A.) 2014年 10月 2日 (2014-10-02) 全文	1-16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 3月 16日	2020年 3月 26日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 王艳臣 电话号码 86-(10)-53961435

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/070028

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	110046902	A	2019年 7月 23日		无		
CN	104753868	A	2015年 7月 1日	WO	2015101036	A1	2015年 7月 9日
				US	2015186892	A1	2015年 7月 2日
CN	1801228	A	2006年 7月 12日		无		
US	2014297522	A1	2014年 10月 2日	US	8788410	B1	2014年 7月 22日