



(12) 发明专利申请

(10) 申请公布号 CN 102439617 A

(43) 申请公布日 2012. 05. 02

(21) 申请号 201080005968. 3

(51) Int. Cl.

(22) 申请日 2010. 01. 28

G06Q 20/34 (2012. 01)

(30) 优先权数据

G06Q 40/02 (2012. 01)

0901407. 7 2009. 01. 28 GB

(85) PCT申请进入国家阶段日

2011. 07. 28

(86) PCT申请的申请数据

PCT/GB2010/000139 2010. 01. 28

(87) PCT申请的公布数据

W02010/086608 EN 2010. 08. 05

(71) 申请人 瓦里德索弗特英国有限公司

地址 英国伦敦

(72) 发明人 P·卡罗尔 J·皮特森

J·阿尔福德

(74) 专利代理机构 中国国际贸易促进委员会专

利商标事务所 11038

代理人 李颖

权利要求书 3 页 说明书 7 页 附图 2 页

(54) 发明名称

卡片误报预防

(57) 摘要

公开了一种用于验证交易的方法。该方法包括步骤:接收识别请求交易的区域的数据;接收识别与请求该交易的人相关的移动通信设备的数据;从用于移动通信设备的位置寄存器(LR)数据确定识别该移动通信设备所在的区域的数据;比较识别所请求交易的区域的数据与识别该移动通信设备所在的区域的数据;以及根据比较结果验证该交易。

1. 一种验证交易的方法,包括步骤:
接收识别请求交易的区域的数据;
从用于与请求交易的人相关的移动通信设备的位置寄存器(LR)数据确定识别该移动通信设备所在的区域的数据;
比较识别请求交易的区域的数据与识别该移动通信设备所在的区域的数据;以及
根据比较结果验证该交易。
2. 根据权利要求1的方法,还包括步骤:接收识别与请求交易的人相关的移动通信设备的数据。
3. 根据任意前述权利要求的方法,还包括步骤:接收用于与请求交易的人相关的移动通信设备的位置寄存器数据。
4. 根据权利要求2或3的方法,其中识别与请求交易的人相关的移动通信设备的数据被用来从LR数据确定该移动通信设备所在的区域。
5. 根据任意前述权利要求的方法,还包括步骤:通过搜索交易数据,从接收自用于执行交易的装置的交易数据中提取识别请求交易的区域的数据。
6. 根据任意前述权利要求的方法,其中识别移动通信设备所在的区域的数据是从归属位置寄存器数据或者访问者位置寄存器数据确定的。
7. 根据任意前述权利要求的方法,其中LR数据是从存储与不同移动业务提供方注册的多个移动设备的LR数据的移动网络聚合器接收的。
8. 根据任意前述权利要求的方法,其中交易在两个区域之间发生。
9. 根据任意前述权利要求的方法,其中交易在单独一个区域中发生。
10. 根据任意前述权利要求的方法,其中识别移动通信设备所在的区域的数据包括移动国家代码(MCC)数据或者识别州或城市的数据。
11. 根据任意前述权利要求的方法,其中识别请求交易的区域的数据包括交易国家数据或者识别州或城市的数据。
12. 根据任意前述权利要求的方法,还包括步骤:如果该交易被确定为可信的,则允许该交易。
13. 根据任意前述权利要求的方法,其中如果识别请求交易的区域的数据与识别移动通信设备所在的区域的数据相匹配,则该交易被确定为是可信的。
14. 根据任意前述权利要求的方法,还包括步骤:如果该交易被确定为不是可信的,则拒绝该交易。
15. 根据任意前述权利要求的方法,其中如果识别请求交易的区域的数据与识别移动通信设备所在的区域的数据不相匹配,则该交易被确定为不是可信的。
16. 根据权利要求14的方法,还包括步骤:在请求交易的用户的移动通信设备和该交易的业务提供方之间建立连接,优选地该连接借助实时语音电话技术或者通过短消息业务(SMS)。
17. 根据任意前述权利要求的方法,其中识别请求交易的区域的数据,以及特别是识别该移动通信设备所在的区域的数据,是从金融业务提供方或者从用于执行该交易的装置接收的。
18. 根据任意前述权利要求的方法,还包括步骤:根据比较结果控制用于执行交易的

装置。

19. 一种用于取得关于所请求的金融交易的有效性的概率数据的方法,包括步骤:

接收识别请求交易的区域的数据;

从用于与请求交易的人相关的移动通信设备的位置寄存器(LR)数据确定识别该移动通信设备所在的区域的数据;

比较识别请求交易的区域的数据与识别该移动通信设备所在的区域的数据;以及

根据比较结果确定关于所请求交易的有效性的概率数据。

20. 根据权利要求19的方法,还包括步骤:接收识别与请求交易的人相关的移动通信设备的数据。

21. 一种用于验证交易的设备,包括:

用于接收识别请求交易的区域的数据的装置;

用于从用于与请求交易的人相关的移动通信设备的位置寄存器(LR)数据确定识别该移动通信设备所在的区域的数据的装置;

用于比较识别请求交易的区域的数据与识别该移动通信设备所在的区域的数据的装置;以及

用于根据比较结果验证该交易的装置。

22. 根据任意前述权利要求的设备,还包括用于接收识别与请求交易的人相关的移动通信设备的数据的装置。

23. 根据任意前述权利要求的设备,其中用于与请求交易的人相关的移动通信设备的位置寄存器数据是从移动网络业务提供方接收的。

24. 根据权利要求22或23的设备,其中识别与请求交易的人相关的移动通信设备的数据被用来从LR数据确定该移动通信设备所在的区域。

25. 根据任意前述权利要求的设备,还包括用于通过搜索交易数据,从接收自用于执行交易的装置的交易数据中提取识别请求交易的区域的数据的装置。

26. 根据任意前述权利要求的设备,其中识别移动通信设备所在的区域的数据是从归属位置寄存器数据或者访问者位置寄存器数据确定的。

27. 根据任意前述权利要求的设备,还包括存储与不同移动业务提供方注册的多个移动设备的LR细节的移动网络聚合器。

28. 根据任意前述权利要求的设备,其中识别移动通信设备所在的区域的数据包括移动国家代码(MCC)数据或者识别州或城市的数据。

29. 根据任意前述权利要求的设备,还包括用于如果该交易被确定为可信的,则允许该交易的装置。

30. 根据任意前述权利要求的设备,其中如果识别请求交易的区域的数据与识别移动通信设备所在的区域的数据相匹配,则该交易被确定为是可信的。

31. 根据任意前述权利要求的设备,其中如果识别请求交易的区域的数据与识别移动通信设备所在的区域的数据不相匹配,则该交易被确定为不是可信的。

32. 根据权利要求30的设备,还包括用于在请求交易的用户的移动通信设备和该交易的业务提供方之间建立连接的装置。

33. 根据任意前述权利要求的设备,其中识别请求交易的区域的数据,以及特别是识别

该移动通信设备所在的区域的数据,是从金融业务提供方或者从用于执行该交易的装置接收的。

34. 根据任意前述权利要求的设备,还包括用于特别通过实时语音电话技术或者通过短消息业务(SMS)连接请求交易的人的移动设备和交易业务提供方的装置。

35. 根据任意前述权利要求的设备,还包括用于根据比较结果控制用于执行交易的装置的控制装置。

36. 一种用于取得关于所请求的金融交易的有效性的概率数据的设备,包括:

用于接收识别请求交易的区域的数据的装置;

用于从用于与请求交易的人相关的移动通信设备的位置寄存器(LR)数据确定识别该移动通信设备所在的区域的数据的装置;

用于比较识别请求交易的区域的数据与识别该移动通信设备所在的区域的数据的装置;以及

用于根据比较结果确定关于所请求交易的有效性的概率数据的装置。

37. 根据权利要求 36 的设备,还包括用于接收识别与请求交易的人相关的移动通信设备的数据的装置。

卡片误报预防

技术领域

[0001] 本发明涉及确定被请求交易的有效性和误报预防 (false-positive prevention), 例如实卡 (card present) 误报预防。特别的, 本发明涉及金融交易和实卡误报预防, 以及跨边界 (cross-border) 实卡误报预防。

背景技术

[0002] 当用户试图进行合法的金融交易, 而由于金融提供方 (例如向客户提供借记卡或信用卡的发行银行) 将该交易错误地识别为可能是欺诈导致该合法的金融交易被拒绝时, 会发生误报事件。该交易可以是跨边界实卡交易。跨边界交易可以是其中在与用户向金融提供方注册的区域所不同的区域中发生交易。也就是说, 跨边界实卡交易可能是用户利用他的信用卡或借记卡异地从 ATM (自动出纳机) 取现金, 或者用户利用他的信用卡或借记卡异地在消费终端 (PoS) 处购买商品。在这两种情况下, 卡必须实际出现在交易地点, 例如在 ATM 或 PoS。这与非实卡的交易是相反的, 其中非实卡交易存在卡的细节, 例如持卡人姓名、卡号、有效期以及安全信息。卡本身不需要出现在交易进行的地点。非实卡交易可能由于因特网或者邮件订单交易而发生。此外, 该交易可能是跨边界交易, 即是交易发生在不是发行该卡的持卡人发行银行的国家以外的国家的交易。

[0003] 跨边界实卡诈骗在不断增多, 现在已经占到 UK 发行卡的所有卡犯罪的 40%。例如芯片和 PIN (个人识别码) 的技术不能有效预防跨边界实卡诈骗, 因为当验证回复到卡的磁条时, 刮卡 (伪造卡) 就可以简单地在例如 US 的不支持芯片和 PIN 的国家中在 ATM 和 PoS 上使用。芯片和 PIN 技术允许利用借记卡或信用卡来支付。卡用户必须输入仅仅是持卡人才知道的 PIN 码, 而不是使用签名来验证支付。

[0004] 银行或其它金融业务提供方通常试图通过在实时授权处理中使用第三方软件风险引擎或者内部逻辑, 以试图确定交易是否可能是欺诈的, 来预防实卡诈骗。其它方式将拒绝所有跨边界交易, 除非持卡人已经提前将精确的行程路线 (实践证明可能仍然是不充分的) 提供给金融业务提供方。

[0005] 风险引擎方法的主要问题是风险引擎在确定潜在的诈骗交易时非常不精确。这种风险引擎所产生的误报率极高, 典型地在 80% 和 90% 之间, 导致实际上并不方便, 加大了持卡人和银行等的成本。所谓误报率, 是指在拒绝交易的总量中错误拒绝交易的百分比。由于当前与确定误报相关的高数量和成本, 金融业务提供方通常不能拒绝它们所希望拒绝的所有交易, 这使得诈骗交易被授权。当预防的成本超过诈骗的成本时, 这也有所上升。对于金融业务提供方和客户的主要成本是误报交易解析处理所带来的。

[0006] 因此, 金融业务提供方通常将真正的交易错误地识别并拒绝为潜在的诈骗, 这是一个问题, 特别是当交易由合法持卡人在不是发行卡片的国家的海外国家进行时。

[0007] 结果, 因为金融业务提供方已经拒绝了交易, 它通常联系持卡人来确认该交易实际上是否是诈骗。这是通过诈骗中心操作员手动完成的 (非常昂贵), 或者是通过外拨业务电子完成的 (其中一些效率低而且昂贵)。然而在许多情况下, 因为金融业务提供方鼓吹这

种处理花费时间,因此持卡人直接(从海外)联系金融业务提供方试图解决这个问题。

[0008] 因为从海外致电给金融业务提供方的花费高得惊人,因此非常不令人满意。此外,在国家之间的时差问题也可能意味着如果是在卡片发行国家的工作时间以外,持卡人不能联系上金融业务提供方。

发明内容

[0009] 本发明定义于所附权利要求中的各个方面,其现在进行参考。

[0010] 根据本发明的一个方面,一种取得关于所请求金融交易的有效性的概率数据的方法,包括步骤:接收关于所请求交易的位置数据;接收识别与请求交易的个人相关的移动通信设备的数据;从用于移动通信设备的归属位置寄存器(HLR)数据确定移动通信设备的位置数据;比较关于交易的位置数据与来自移动通信设备的位置数据;以及根据比较的结果,确定关于所请求交易的有效性的概率数据。

[0011] 根据本发明的另一方面,一种取得关于所请求金融交易的有效性的概率数据的设备,包括:用于接收关于所请求交易的位置数据的装置;用于接收识别与请求交易的个人相关的移动通信设备的数据的装置;用于从用于移动通信设备的归属位置寄存器(HLR)数据确定移动通信设备的位置数据的装置;用于比较关于交易的位置数据与来自移动通信设备的位置数据的装置;以及用于根据比较的结果,确定关于所请求交易的有效性的概率数据的装置。

[0012] 本发明的优选实施例通过如下方式取得关于所请求金融交易的有效性的概率数据:接收关于所请求交易的位置数据;接收识别与请求交易的个人相关的移动通信设备的数据;从用于移动通信设备的归属位置寄存器(HLR)数据确定移动通信设备的位置数据;比较关于交易的位置数据与来自移动通信设备的位置数据;以及根据比较的结果,确定关于所请求交易的有效性的概率数据。

[0013] 这允许确定交易的合法性的概率,使得发行银行能够更好地确定是允许还是拒绝交易。这意味着更少的误报交易发生,向持卡人提供了改善的业务,并降低了发行银行的成本。

附图说明

[0014] 现在仅以示例的方式,参考相应附图描述本发明的实施例,其中:

[0015] 图1示出了本发明实施例的系统结构的示意图;以及

[0016] 图2示出了本发明主要执行步骤的流程图。

具体实施方式

[0017] 参考图1,一种误报预防系统包括服务器或者计算机101。如以下进一步详细描述,服务器或计算机101确定交易是否可能是诈骗。该系统可以进一步包括移动网络数据聚合器103;移动网络105、106,移动通信装置(未示出),银行107,以及客户109。此外,该系统还可以包括解析(resolution)系统111,尽管该特征不是必要的,因此在图1中以虚线示出。现在将描述本发明实施例执行的主要步骤。

[0018] 参考图2,在步骤201,用户首先在用于进行或执行交易的装置处开始交易。用于

执行交易的装置可以是 ATM 或者 PoS。如果该交易是在 ATM 请求的,该用户将卡插入 ATM,并输入他的 PIN 码。可选地,如果该交易是在 PoS 上执行的,那么该用户可以将卡交给零售商,该零售商将卡插入读卡器进行处理。如果该卡是芯片和 PIN 卡,该用户可选地可以输入 PIN。其它验证方案,例如签名,也是可以替代或者除 PIN 之外还要使用的。无论如何,该卡包括与个人或者用户相关的数据,允许用户的账户被识别。通常,这个信息是采用十进制数字序列的形式。

[0019] 在步骤 203,ATM 或者 PoS 接着联系金融业务提供方(发卡方)107,并且开始发卡银行或者金融业务提供方 107 验证处理。此时,在步骤 205,金融业务提供方接收交易请求。ATM 或者 PoS 发送信息,使得推断出持卡人的身份。该信息可以包括卡号,并且可以由传统方式发送,或者利用技术人员已知的无线装置发送。该信息还可以采用技术人员已知的任意合适的加密形式发送。

[0020] 一旦银行或者金融业务提供方 107 接收到该交易请求,可以可选地执行附加处理来确定(利用软件风险引擎或者内部逻辑)该交易是否可能是诈骗,例如如果该交易是大额的。然而,如果金融业务提供方 107 确定该交易可能是真实的,那么在步骤 217,它可以直接进行到授权处理,在步骤 219 允许该交易。如果金融业务提供方确定该交易可能是诈骗,那么将请求传送给服务器 101。

[0021] 然而,如果金融业务提供方没有执行这个附加处理,那么它将交易信息直接传送给服务器 101。

[0022] 在一个实施例中,服务器 101 可以位于金融业务提供方的组织机构中。然而,优选实施例具有一种服务器 101,它与金融业务提供方是物理分离的,且该交易信息(例如卡号或 / 和姓名或 / 和交易额)利用无线或者传统的有线技术发送给服务器 101。

[0023] 在一个实施例中,在步骤 207,服务器 101 接着提取包含在交易信息中的国家代码信息。

[0024] 在可选实施例中,金融业务提供方从交易信息中提取国家代码信息。该金融业务提供方还可以将参考号分配给该交易。这有一个优点就是不必将潜在的敏感的金融信息,例如卡号,发送给服务器 101。

[0025] 金融业务提供方接着在客户数据库或者查找表中搜索识别移动通信设备的信息,如表 1 所示。

[0026]

持卡人姓名	卡号	电话号码
Smith A 先生	5432 1234 5678 9998	00 44 7981 123 789
Smith A 先生	5432 1234 5678 9999	00 44 7981 123 789
Jones N 先生	5432 1234 0123 4567	00 44 7981 567 831

[0027] 表 1:发卡银行中的部分查找表

[0028] 这是通过使用持卡人识别信息(例如卡号)来搜索查找表而进行的。该查找表具有每个持卡人的持卡人识别信息,还有使得持卡人的移动通信设备能够被确定的信息。每

个用户的持卡人识别信息与至少一条使得持卡人的通信设备能够被确定的信息相关。如果该移动通信设备是便携式电话,那么该信息可以是与执行交易的用户相关的便携式电话的(唯一)电话号码。此外,每个持卡人在查找表中可以具有不止一个条目,因为他们可能在该金融业务提供方有不止一张卡。

[0029] 金融业务提供方接着将识别移动通信设备的信息以及所提取的关于该交易的国家代码(即位置)发送给服务器 101。优选的,还可以发送交易参考号。这可以由金融业务提供方分配给该交易的任意号码。该信息可以加密形式发送。

[0030] 服务器 101 从发行银行接收识别客户 109 的移动通信设备的信息(移动电话号码),接着从商业可用数据库执行 HLR 查找。HLR 数据库是每个移动网络提供方所持有的,并且包括有关提供方的永久订户的信息。信息中包括当前指定给订户的网络国家代码,供漫游的客户使用。考虑到用户位置的变化,该 HLR 数据库是频繁更新的。

[0031] 在步骤 209,服务器 101 通过向移动网络数据聚合器 103 打开一个或多个通信信道来执行 HLR 查找。网络数据聚合器持有在移动网络提供方注册的移动通信设备的 HLR 信息。网络数据聚合器可以具有不止一个移动网络业务提供方 105、106 的 HLR 数据。这有一个优点就是无需单独查询每个业务提供方,来获得在不同业务提供方注册的移动通信设备的 HLR 数据。

[0032] 在步骤 211,利用使得持卡人的通信设备能够被确定的信息(即,移动电话号码),网络数据聚合器 103 能够在订户的移动网络的归属位置寄存器(HLR)中提取每个永久订户所特有的移动国家代码(MCC)指示符。与识别移动通信设备的信息(电话号码)相关的 MCC 代码接着被发送到服务器 101。

[0033] 服务器 101 接着将在(跨边界)ATM 或者 PoS 交易中包含的接收到的国家指示符与接收到的移动国家代码(MCC)指示符进行比较。

[0034] 在步骤 213,计算交易合法的几率。有许多可以执行该计算的方式。其中检测合法交易的最简单方式是,所提取的交易发生地的国家代码是否与确定的 MCC 指示符相匹配。例如,具有与澳大利亚相关的所提取的国家代码的交易很大概率上是合法的,如果所确定的 MCC 指示符也是关于澳大利亚的话。这种情况下,该交易可能是合法的,因为合法持卡人很有可能是位于与其移动通信设备相同的或者相近的位置。对于合法的交易,执行该交易的合法持卡人可能是将其自己的移动通信设备带在身边。此时,该交易的位置将实际上与用户的移动通信设备的位置相同。

[0035] 可以利用技术人员已知的技术来确定移动通信设备的 HLR 数据,例如利用移动 GSM(全球移动系统)网络或者利用第三代移动网络。这允许移动通信设备的位置确定精确到至少 50 米。

[0036] 在一个实施例中,该系统可以被配置为仅当由此确定的移动通信设备的位置在交易发生位置的预定距离(例如 50 或 100 米)之内时,该交易才被确定为真实的。

[0037] 在可选实施例中,该系统被配置为仅当移动通信设备被确定为在与交易发生的地点在相同的城市或者省份或者国家时,该交易才被确定为真实的。该实施例是非常有用的,因为常有卡用户在进行交易时将移动设备放在家中或者旅店中。

[0038] 在某些情况下,尽管交易正在由合法用户执行,交易国家代码也不能匹配 MCC 指示符。如果该交易是在接近国家边界的位置发生,例如法国和德国的边界,就会发生这种情

况。这种情况下,如果 MCC 指示符被确定为接近边界,即使该交易国家代码与 MCC 指示符不匹配,倘若该交易是发生在利用 MCC 确定的国家代码的邻接(即,在预定距离之内)国家中,该交易也被允许。

[0039] 在步骤 213,该系统还可以确定交易是诈骗的概率,而不是只是确定该交易是否是真实的(1)或者诈骗的(0)。这种情况下,0 和 1 之间的数字可以被指定给该交易。

[0040] 在一个实施例中,当交易的位置和用户的移动通信设备之间的距离较大时,交易是诈骗的概率就较大。

[0041] 在步骤 215,交易请求随着确定的概率值而更新,例如 0.9(意味着该交易是真实的概率有 90%)或者整数,例如 1 或者 0(意味着确定该交易具有 100%的概率是真实的或者诈骗的)。该概率接着被传送到银行或者金融业务提供方 101,作为交易信息的一部分,在步骤 217,银行或者金融业务提供方根据所确定的概率允许或者拒绝该交易。如果该交易被允许,那么其在步骤 219 完成。

[0042] 采用这种方式,本发明的实施例减少了误报交易的影响。

[0043] 减少误报的影响的结果是通过使更多的怀疑交易被拒绝而潜在增加了对实报(诈骗交易)的检测。所谓实报,是指由于被识别为潜在的诈骗而被拒绝的诈骗交易。本发明的实施例因此达到最大有效性,要求持卡人在异地携带并激活(尽管无需随身携带)他们移动通信设备(移动电话),还要求发行银行在它们的持卡人数据库中记录准确的移动电话信息。这种趋势在增长,因为跨边界误报的影响在增长,并且被银行积极地鼓励。支付清算服务协会(APACS)建议持卡人确保他们的卡公司具有最新的联系细节,包括移动号码,特别是海外旅行时。

[0044] 在其它实施例中,在步骤 221 提供一种自动解析处理,然而这是可选的。这考虑到通过具有低合法性概率(潜在的诈骗交易)而拒绝的任意交易的即刻和自动解析。该自动解析处理预测该拒绝是实报(诈骗交易)或者误报(合法交易)。根据结果,自动解析处理直接连接持卡人和银行或者金融业务提供方(即,诈骗部门),来解决诈骗卡的问题以及任意之前的诈骗交易。可替代的,它可以更新持卡人的信息,并请求持卡人再次提交被拒绝的交易。因为解析处理可能是在交易被拒绝时立即进行的,它流水线处理,向持卡人提供更好的客户体验并提供机会使持卡人能重试该交易,如果是误报,同时仍然是临近原始被拒绝的交易。

[0045] 本发明的实施例使用 HLR 信息结合实卡金融交易数据来预测合法性概率。利用 HLR 数据库来确定订户的国家位置,在成本、时间性和保密性方面都比例如维度/经度跟踪技术具有优势。本发明的实施例允许更多的实报跨边界实卡金融交易被识别,同时还降低了误报交易的数量。

[0046] 本发明的实施例还允许利用 HLR 信息识别无效的移动电话号码(不再使用的那些),由此避免了处理错误。这还允许了这些号码被识别,并使金融业务提供方请求来自持卡人的新的电话号码。本发明的实施例可以运行为主业务或者在内部运行。尽管本发明的实施例已经参考金融卡进行了描述,但事实上不需要在交易发生时实际出现任何卡。例如,用户可以使用生物信息,例如指纹或者视网膜扫描,作为其账户的唯一标识符,同时还给出授权信息。该授权信息可以是附加的 PIN 或者可以是生物信息本身。

[0047] 在其它实施例中,用户可以被提供有代码或/和 pin 码的唯一组合来输入到 ATM。

这允许其金融业务提供方从 ATM 向用户提供现金,而无需物理卡。取出的现金接着从利用唯一码所识别的用户账户中借贷。

[0048] 将理解,本发明可以应用于确定试图在 ATM 或 PoS 或任意其它执行交易的装置进行任意交易的有效性或者可信性。该交易可以是金融交易。此外,本发明的实施例可以采用硬件或软件执行。实施例可以在 ATM 或者 PoS 或者执行交易的其它装置上实施,尽管优选是在集中计算机或者服务器 101 处实施该系统。除了使用归属位置寄存器数据库信息之外,该系统 101 可以使用访问者位置寄存器数据库信息。这些数据库可以被称为位置寄存器 (LR) 数据库。

[0049] 在一个实施例中,关于请求金融交易的位置的位置数据可以包括识别请求交易的区域的数据。例如,本发明的实施例可以使用 ATM 国家代码指示符或者 PoS 国家代码指示符。这些金融交易国家指示符可以标记为例如“UK”或者“44”,并用于识别特定的区域,但是没有包括足够的信息来确定区域的所在或者甚至 ATM 或 PoS 在该区域中位于或定位在何处。

[0050] 此外,移动通信设备的位置数据可以包括识别移动通信设备所在区域的数据。

[0051] 例如,本发明的实施例可以使用移动国家代码 (MCC) 指示符,例如“UK”或者“44”。服务器 101 可从归属位置寄存器数据提取移动国家代码指示符。服务器 101 可以利用识别与请求交易的个人相关的移动通信设备的数据,从多个移动设备的 LR 数据提取移动国家代码指示符。对应于请求该交易的用户的移动设备的 LR 数据可随后被搜索,来提取国家代码指示符。例如,在 LR 数据库中搜索字段“MCC”将显示一个匹配,与该匹配相关的数据值是 MCC 值或者指示符。识别移动通信设备的数据可以是移动电话号码或者其它订户信息,例如国际移动订户身份 (IMSI)。

[0052] 识别移动通信设备所在区域的数据可以是一种标记,例如“UK”或者“44”,并用于识别该设备所在的特定区域,但是没有包括足够的信息来确定区域的所在或者甚至该设备在该区域中位于或定位在何处。

[0053] 利用识别区域的数据而不是位置数据本身的优点在于,服务器 101 并不知晓移动通信设备的位置,使得用户的隐私被保护。服务器 101 仅知晓表示特定区域的标识符的值是多少。例如,如果用户的移动通信设备位于 UK 中,识别该移动设备所在区域的数据可以是数字例如“44”。该信息不允许确定移动通信的位置。

[0054] 此外,利用识别区域的数据而不是位置数据本身的优点还在于,服务器 101 或者计算机并不知晓用户试图进行交易的 ATM 或者 PoS 的定位或位置。这对于用户的隐私方面也是有利的。

[0055] 此外,识别请求金融交易的区域的指示符或者数据不是唯一的。也就是说,特定地理区域中的所有 ATM 或者 PoS 都被指定特定的国家指示符,例如“44”。

[0056] 此外,识别与请求交易的用户相关的移动通信设备所在的区域的指示符或数据也不是唯一的。也就是说,指定给特定电话的移动电话国家指示符不是唯一的,特定区域或国家中的多个移动电话共享相同的代码。

[0057] 具有并不唯一的指示符的优点在于,简化了比较识别请求金融交易的区域的数据与识别移动通信设备所在的区域的数据的步骤。

[0058] 这是因为不必确定 ATM 或者 PoS 距离移动通信设备的距离,例如利用移动设备的

位置 (x1,y1,z1) 和 ATM 或者 PoS 的位置 (x2,y2,z2)。所需的就是将 ATM 或者 PoS 所在区域的数据或者标识符与移动通信设备所在的区域的数据或标识符相比较。因此这简化了并提高了系统的响应时间。对于加强用户隐私方面也是有利的。

[0059] 如果 ATM 或者 POS 所在的区域标识符与移动通信设备所在的区域标识符相匹配,那么交易可以被验证或者确定为可信的。

[0060] 在某些国家,还可以提供移动设备所在的区域的其它标识符。例如,对于美国的交易,识别移动设备所在的区域的数据还可以包括城市或州标识符。该标识符也可以位于 HLR 数据中。然而,这些城市或州标识符也不是唯一的,因为多个移动设备可以被指定相同的城市或州标识符。此外,城市或州标识符可能不包括足够的信息来使得能够确定城市或州所覆盖的区域的位置或者确实确定移动设备在城市或州中的位置。

[0061] 如前所述,本发明实施例可以从移动网络聚合器接收 HLR 数据。此外,该交易可以是实卡交易或者非实卡交易或者跨边界交易。移动通信设备的位置数据可以从不止一个网络聚合器接收。LR 数据可以包括来自不止一个移动网络业务提供方的数据。此外,可以实时或者后授权 (post authorization) 地确定所请求交易的合法性的概率。

[0062] 此外,如果所确定的合法性概率低于预定值,本发明的实施例可以拒绝交易。概率数据还可以被用来识别误报交易。该交易数据和识别移动通信设备的数据可以从金融业务提供方接收。该方法还可包括例如通过电话自动联系请求交易的人的步骤。

[0063] 本发明的实施例还可以包括根据比较结果控制执行交易的装置的步骤。这个步骤可以替代根据比较结果验证交易的步骤。

[0064] 例如,如果识别请求交易的区域的数据与识别移动通信设备的区域的数据相匹配,ATM 或者 PoS 或者其它执行交易的装置可以被控制,使得现金被分配或者使得 PoS 执行交易。

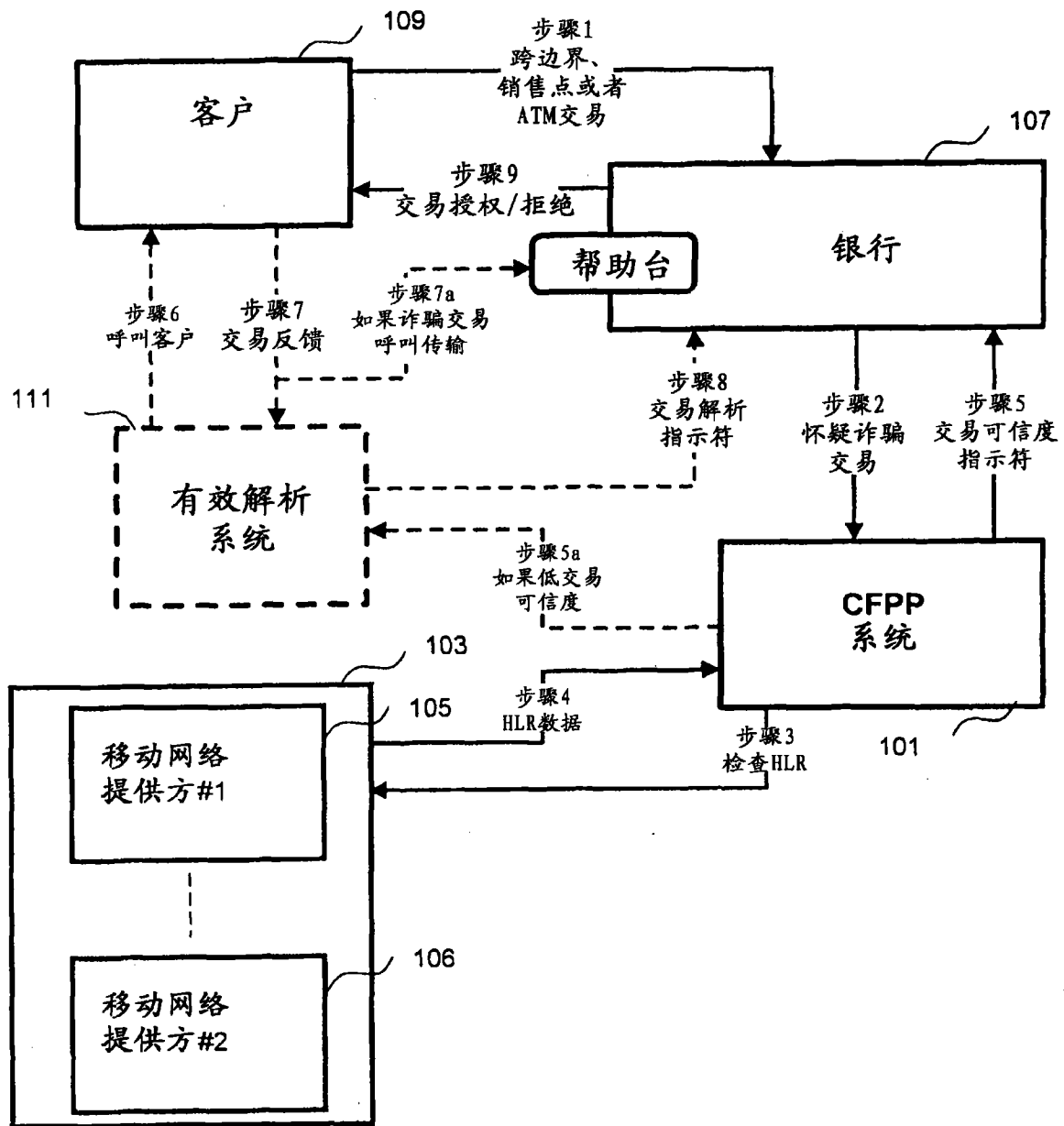


图 1

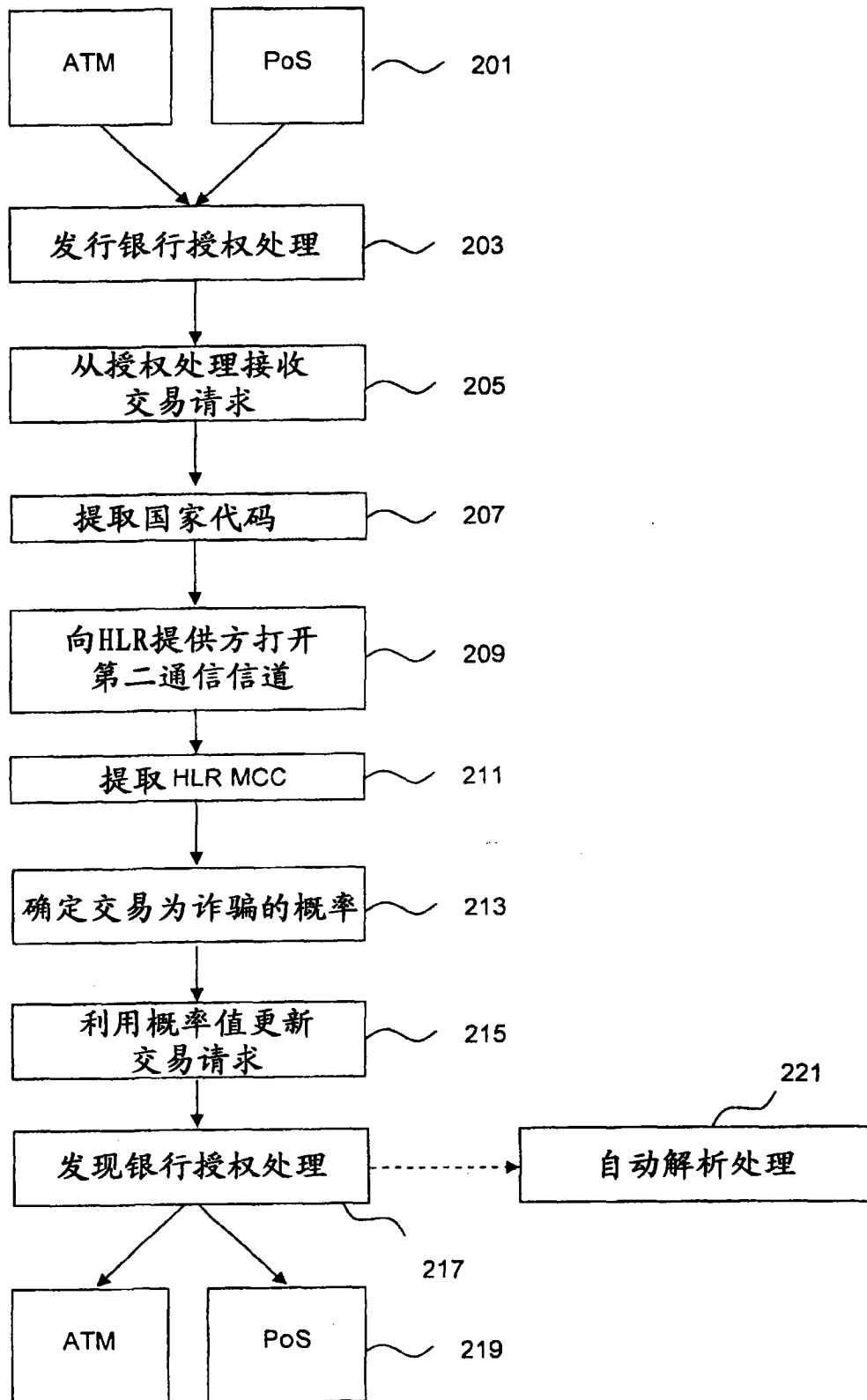


图 2