

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.  
G06K 5/00 (2006.01)



## [12] 发明专利申请公布说明书

[21] 申请号 200680033683.4

[43] 公开日 2009 年 10 月 14 日

[11] 公开号 CN 101558414A

[22] 申请日 2006.7.14

[21] 申请号 200680033683.4

[30] 优先权

[32] 2005.7.15 [33] US [31] 60/700,049

[86] 国际申请 PCT/US2006/027309 2006.7.14

[87] 国际公布 WO2007/011695 英 2007.1.25

[85] 进入国家阶段日期 2008.3.13

[71] 申请人 革新货币公司

地址 美国佛罗里达州

[72] 发明人 詹森·裘德·豪格

帕特里克·格拉夫

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 王 玮

权利要求书 3 页 说明书 34 页 附图 18 页

[54] 发明名称

欺骗检测规则的用户选择系统及方法

[57] 摘要

一种建立欺骗检测规则体制的系统和方法，包括：第一交易卡，通过所述第一交易卡给予对货币资金的存取；数据库，用于将所述交易卡与一个或更多的欺骗检测规则相关联，所述欺骗检测规则管理由所述交易卡对所述货币资金的存取。该系统还包括被编程的计算系统，所述被编程的计算系统允许拥有所述交易卡的个人规定所述欺骗检测规则，所述欺骗检测规则管理由所述交易卡对所述货币资金的存取。

1.一种计算机化的方法，包括：

在数据库中，将交易卡与一个或更多的欺骗检测规则相关联，所述欺骗检测规则管理由所述交易卡对所述货币资金的存取；和

允许拥有所述交易卡的个人规定所述欺骗检测规则，所述欺骗检测规则管理由所述交易卡对所述货币资金的存取。

2.根据权利要求 1 所述的方法，其中允许所述个人规定欺骗检测规则，在所规定的欺骗检测规则中，所述交易卡在每个规定的时间段从所述货币资金支出大于规定的货币数目被看作是潜在的欺骗。

3.根据权利要求 1 所述的方法，其中在允许所述个人规定的欺骗检测规则中，所述交易卡针对单件商品或服务从所述货币资金支出大于规定的货币数目被看作是潜在的欺骗。

4.根据权利要求 1 所述的方法，其中在允许所述个人规定的欺骗检测规则中，用所述交易卡从所述货币资金购买规定级别的商品被看作是潜在的欺骗。

5.根据权利要求 1 所述的方法，其中在允许所述个人规定的欺骗检测规则中，所述交易卡在规定的时间段期间从所述货币资金的支出使花费的货币总量超过所述交易卡在所述时间段期间从所述货币资金花费的货币平均或中间数目大于规定量时被看作是潜在的欺骗。

6.根据权利要求 1 所述的方法，其中在允许所述个人规定的欺骗检测规则中，用所述交易卡在规定级别、类型、或种类的商家从所述货币资金的支出被看作是潜在的欺骗。

7.根据权利要求 1 所述的方法，其中在允许所述个人规定的欺骗检测规则中，针对规定的商品或服务用所述交易卡从所述货币资金的支出被看作是潜在的欺骗。

8.根据权利要求 1 所述的方法，其中在允许所述个人规定的欺骗检测规则中，在规定的地理区域内用所述交易卡从所述货币资金的支出被看作是潜在的欺骗。

9.根据权利要求 1 所述的方法，其中所述交易卡包括信用卡。

10.根据权利要求 1 所述的方法，其中所述交易卡包括借贷卡。

11.根据权利要求 1 所述的方法，其中所述交易卡包括储值卡。

12.根据权利要求 1 所述的方法，其中依据所述个人已经规定的所述欺骗检测规则，立即用所述欺骗检测规则管理对所述货币资金的存取。

13.根据权利要求 1 所述的方法，进一步包括：

通过所述交易卡接收存取所述货币资金的请求；

对照所述欺骗检测规则测试所述请求；

根据对照所述欺骗检测规则进行的所述测试，确定所述请求是潜在的欺骗；

在授权所述请求存取所述货币资金的之前，联系所述个人以确认所述请求。

14.根据权利要求 13 所述的方法，其中通过短消息业务（SMS）执行联系所述个人的所述行动。

15.根据权利要求 13 所述的方法，其中通过因特网消息执行联系所述个人的所述行动。

16.根据权利要求 13 所述的方法，其中通过电话呼叫执行联系所述个人的所述行动。

17.一种系统，包括：

第一交易卡，通过所述第一交易卡对货币资金进行存取；

数据库，用于将所述交易卡与一个或更多的欺骗检测规则相关联，所述欺骗检测规则管理由所述交易卡对所述货币资金的存取；和

被编程的计算系统，所述被编程的计算系统允许拥有所述交易卡的个人规定所述欺骗检测规则，所述欺骗检测规则管理由所述交易卡对所述货币资金的存取。

18.根据权利要求 17 所述的系统，其中对所述计算系统编程以允许所述个人规定欺骗检测规则，在所规定的欺骗检测规则中，所述交易卡在每个规定的时间段从所述货币资金支出大于规定的货币数目被看作是潜在的欺骗。

19.根据权利要求 17 所述的系统，其中对所述计算系统编程以允许所

---

述个人规定欺骗检测规则，在所规定的欺骗检测规则中，所述交易卡针对单件商品或服务从所述货币资金支出大于规定的货币数目被看作是潜在的欺骗。

20.根据权利要求 17 所述的系统，其中对所述计算系统编程以允许所述个人规定欺骗检测规则，在所规定的欺骗检测规则中，用所述交易卡从所述货币资金购买规定级别的商品被看作是潜在的欺骗。

21.根据权利要求 17 所述的系统，其中对所述计算系统编程以允许所述个人规定欺骗检测规则，在所规定的欺骗检测规则中，所述交易卡在规定的时间段期间从所述货币资金的支出使花费的货币总量超过所述交易卡在所述时间段期间从所述货币资金花费的货币平均或中间数目大于规定量时被看作是潜在的欺骗。

22.根据权利要求 17 所述的系统，其中对所述计算系统编程以允许所述个人规定欺骗检测规则，在所规定的欺骗检测规则中，用所述交易卡在规定级别的商家从所述货币资金的支出被看作是潜在的欺骗。

23.根据权利要求 17 所述的系统，其中对所述计算系统编程以允许所述个人规定欺骗检测规则，在所规定的欺骗检测规则中，针对规定的商品或服务用所述交易卡从所述货币资金的支出被看作是潜在的欺骗。

24.根据权利要求 17 所述的系统，其中对所述计算系统编程以允许所述个人规定欺骗检测规则，在所规定的欺骗检测规则中，在规定的地理区域内用所述交易卡从所述货币资金的支出被看作是潜在的欺骗。

25.根据权利要求 17 所述的系统，其中所述交易卡包括信用卡。

26.根据权利要求 17 所述的系统，其中所述交易卡包括借贷卡。

27.根据权利要求 17 所述的系统，其中所述交易卡包括储值卡。

## 欺骗检测规则的用户选择系统及方法

本申请是 2006 年 7 月 14 日，在美国之外的所有国家指定美国公司 Gratis Card, Inc 的名称为申请人，和在美国仅指定美国公民 Jason Jude Hogg 和 Patrick Graf 为申请人的 PCT 国际专利申请，并要求 2005 年 7 月 15 日提交的美国申请序列号为 60/700,049 的美国专利申请的优先权。

### 技术领域

本发明涉及财务和数据交易系统领域，更具体地讲，涉及通过开放网络执行财务和数据交易的系统和方法。

### 背景技术

图 1 示出了当前使用的典型信用卡交易。如图 1 中所示，处理过程以信用卡持有者 100 将他的信用卡提交给位于商业设施 102 内的 POS 机设备（销售点装置）（例如，收银机）的服务员开始，如操作 101 所示。作为响应，服务员一般通过连接到 POS 机设备的磁条阅读器“扫描”卡。从而将包括持卡人的姓名和信用卡号在内的持卡人信息从卡上的存储介质传送到 POS 机设备。

POS 机设备将持卡人信息与交易信息（包括销售总额和商家身份）组合在一起，并将组合的数据集发送到受让人或第三方处理器 104，如操作 103 所示。第三方处理器 104 通过将数据集发送到卡协会（例如，Visa, American Express, 等）的专用交易网 106 做出响应（操作 105），并通过交易网 106 将数据集路由到发卡银行 108，如操作 107 中所示。

在接收到数据集时，发卡银行 108 对照一组信贷规则检查提出的财务交易，并且核准或拒绝财务交易。如果核准，那么核准信息以相反的顺序（操作 109, 111, 和 113）通过同一路径到达商家位置 102 的 POS 机设备。然后，如操作 115 所示，发卡银行 108 通过类似的一组复杂数据交易，将等于销售价格的货币金额转送到商家的银行 110（一般是将处理器用作向

商家的银行 110 转送货币金额的媒介)。在开票周期期满时, 持卡人 100 将销售价格(加上利息和财务费用)支付给发卡银行 108(操作 117)。

上述方案显现出某些缺陷。例如, 由于利用专用网络在商家 102 与授权实体(在本例中, 是发卡银行 108)之间通信数据, 从而招致了这种网络的建立和维护的花费。这种开销最终要由商家 102 来负担。使用专用网的另一个缺点是, 由于基础设施和成本的限制, 只能从商家的 POS 机设备发送较小量的数据。这意味着, 例如, 不能在其月度结算表中给持卡人提供有关一个特定交易的详细信息。在某种情况下, 现有的信用卡技术的确提供了有关一个特定交易内容的临时信息内容。但是, 这种信息不是在与执行交易同时的时间点收集的。而是在交易执行之后收集的。由于在收集数据中出现的这种延迟, 现有的信用卡技术当前不能提供某些预付服务。

上述方案中也存在其他的缺陷。个人身份信息一般印刷或压印在信用卡上, 和编码在它的磁条上。这需要在批准信用卡申请人使用信用卡的时间点与申请人接收到信用卡的时间点之间的延迟(将申请人的个人信息在该间隔周期中印刷和编码在卡上)。此外, 由于信用卡使用的存储机构是磁条, 所以必须将磁条阅读器与 POS 机设备连接。这造成了额外的开销, 使得小企业不愿意接受这种信用卡。此外, 当前正在准备将射频识别(RFID)装置引入信用卡。这种创新也涉及大量的基础设施投资, 这又使得小企业不愿意接受这种信用卡。

## 发明内容

根据一个实施例, 一种计算机化的方法, 包括: 在所述数据库中, 将交易卡与一个或更多的欺骗检测规则相关联, 所述欺骗检测规则管理由所述交易卡对所述货币资金的存取。该方法还包括:

允许拥有所述交易卡的个人规定所述欺骗检测规则, 所述欺骗检测规则管理由所述交易卡对所述货币资金的存取。

根据另一个实施例, 一种系统, 包括: 第一交易卡, 通过所述第一交易卡给予对货币资金的存取; 和数据库, 用于将所述交易卡与一个或更多的欺骗检测规则相关联, 所述欺骗检测规则管理由所述交易卡对所述货币资金的存取。该系统还包括被编程的计算系统, 所述被编程的计算系统允

---

许拥有所述交易卡的个人规定所述欺骗检测规则，所述欺骗检测规则管理由所述交易卡对所述货币资金的存取。

#### 附图说明

图 1 示出了一个典型的信用卡交易；

图 2 示出了根据本发明的一个实施例的信用卡交易；

图 3 示出了一种可以在与核准与之相关的申请的时间点几乎同时地激活交易卡的方法；

图 4 示出了一个其中可以配置图 5 的内核的示例网络环境；

图 5 示出了可以配置在图 4 的示例网络实施例中的内核的示例实施例；

图 6 示出了从图 5 的内核通信到图 7 的软件系统的消息的示例实施例；

图 7 示出了一个可以通过由交易平台操作的一个或更多的服务器执行的软件系统的示例实施例；

图 8 示出了一个由图 7 的数据库实现的模型的示例实施例；

图 9 示出了一个从图 7 的软件系统通信到图 5 的内核的消息的示例实施例；

图 10 示出了一个从图 5 的内核通信到图 7 的软件系统的消息的示例实施例；

图 11 示出了一种为了将匿名的未转让卡分发给可能的申请人而奖励持卡人的方法的示例实施例；

图 12 示出了一种允许为了交易内的一个项目的价钱进行争议的方法的示例实施例；

图 13 示出了一种用于建立或改变控制子卡的使用的规则的方法的示例实施例；

图 14 示出了建立或改变使用者可选的欺诈检测规则的方法的示例实施例；

图 15 示出了一种建立或改变使用者可选算法的 PIN 修改规则的方法的示例实施例；

图 16 示出了一个允许商家之间交换货物的方案的示例实施例；

---

图 17 示出了个人对个人交换资金的示例实施例；和

图 18 示出了个人对个人交换资金的另一个示例实施例。

## 具体实施方式

以下参考附图详细说明这里提出的各个实施例，其中在所有视图中相同的参考号代表相同的部件和组件。参考各个实施例不能被认为是限制覆盖的技术主题的范围，技术主题的范围仅受附属的权利要求的限制。此外，本说明书中提出的任何示例是没有限制的，而仅仅提出了许多可能的实施例中的一些。

图 2 示出了一个根据本发明的一个实施例的财务交易，例如，信用卡交易、借贷卡交易、储值卡交易、预付卡交易、等等。如图 2 中所示，持卡人 200 通过将信用卡提交给 POS 机设备 202 或操作这种装置 202 的服务人员而启动交易（操作 201）。当然，交易可以在普通的在线交易过程中启动，例如，通过将持卡人信息输入到为在线贸易设计的网站中启动。仅仅是为了说明，将这里参考附图说明的交易描述为发生在服务人员手工操作的 POS 机设备（在商店）。此外，为了人们熟悉的称呼，这里可以将卡称为“信用卡”、“卡”、或“交易卡”。实际上，如下面要讨论的，卡可以作为信用卡、签帐卡、储值卡、和/或允许对诸如卫生保健数据、俱乐部成员数据之类的各种格式的数据存取的数据存取卡操作。

卡可以有如下的特征。卡本身可以包括一个基底（即，卡的基体），基底可以是聚合物的或任何适当材料的。可以将存储介质沉积在基底上，镶嵌在基底内，和/或印刷在基底上。存储介质可以是只读的，例如印刷在基底上的条形码，或可以是可读和可写的，例如磁存储介质（例如，磁条）。根据一些实施例，信用卡上可以同时具有条形码和磁条。根据一些实施例，将唯一地标识卡的卡号编码在磁条上或条形码上。此外，信用卡也可以包括其中存储有卡号的 RFID 装置。根据一个实施例，存储介质，无论是条形码、磁条、还是 RFID 装置，都不包含、编码、和/或存储有关持卡人的个人信息。根据一些实施例，卡上的存储介质仅包含、编码、和/或存储一个唯一地标识该卡的卡号。根据一些实施例，卡的存储介质不包含、编码、和/或存储个人身份号码（PIN）。

---

在接收到卡时，服务人员将卡提供到输入装置，例如，条形码阅读器，磁条阅读器，或 RFID 收发器。然后读取编码在信用卡的存储介质上的信息。接下来，提示持卡人提供个人身份号码（PIN），个人身份号码可以由持卡人或服务人员通过诸如小键盘、键盘、触摸屏显示器、和/或任何适于输入 PIN 的装置输入到 POS 机设备。将来自信用卡的数据，PIN，和来自 POS 机设备的交易信息用于填充多个数据信息包，数据信息包可以“包装”为一个构成核准提出的交易的请求的单一单元。各种不同信息包将在以下更详细地讨论。根据下面一般说明的方案给包装的单元加密，并且通过诸如因特网之类的开放网络发送到交易平台 204，如操作 203 中所示。

如这里更详细说明的，交易平台 204 可以与发卡银行保持一定程度的联合，以便能够核准或拒绝全部、大部分、或一些交易（例如，少于极限货币量的交易），而无需进一步通知发卡银行以获得核准决定。在获得核准或拒绝决定之后，核准/拒绝决定经过开放网（例如，因特网）返回到商家 202，如操作 205 中所示。

上述实施例显示了某些重要的优点，但这些优点并非是实践这里所述的各个实施例所必须的。例如，商家 202 与交易平台 204 之间的通信经过一个开放网发生，例如经过因特网。利用开放网，消除和/或减少了对于专用网元件和/或线路的需要，这意味着执行每个交易的成本降低。此外，由于经过诸如因特网之类的开放网的通信是免费的，所以如下面说明的，可以在商家 202 与交易平台 204 之间交换较大量的数据，这使能够开列更为详细的结算表。此外，诸如可资利用的信用、利息支付、和费用之类的银行定义的银行规则的管理是通过平台管理的，减少了对于信息协会 202 与各种发卡银行 206 之间的固定通信的需要，这是通过预定的系统合并/同步实施的，这也可能经过开放网实施，从而获得相同的效益。

也应当注意，在一些实施例中，信用卡不包含个人信息。更具体地讲，没有个人信息印刷、镶嵌、或呈现在卡的表面（例如，卡不包含持卡人的姓名），也没有个人信息编码、存储、或包含在卡上的存储介质中。这种安排使得能够几乎在瞬间将一个激活交易卡交付到想要成为持卡人的手中。例如，如图 3 中所示，未过户的匿名卡的供应可以在，例如，商店的 POS 机设备提供（操作 300）。用“匿名的”这个术语表示卡没有包

---

含、编码、和/或存储标识卡所属的个体的信息。也就是说，它的表面上不包含个体的姓名，也没有关于个体的姓名或标识有关个体的信息其他信息存储或编码在卡的存储介质中。卡的存储介质仅包含唯一地标识卡的卡号，而没有账号。

如操作 302 中所示，将一个匿名卡颁发给一个申请人。例如，这可以发生在一个顾客要进行货物或服务的购买的交易的时间点。假设，未过户匿名卡的来源保持在 POS 机设备，那里的服务人员可以询问顾客他或她是否要申请信用卡或开户预付/储值卡。如果顾客的回答是肯定的，那么服务人员可以给顾客提供一张卡。当然，想要成为申请人的人可以从任何来源，包括从朋友或其他持卡人，获得匿名卡（以后讨论）。

接下来，将申请人的申请信息和唯一地标识卡的卡号提供给交易平台的服务器（以后详细讨论）（操作 304）。再假设在 POS 机设备将卡分发给顾客，服务人员可以将顾客的信息输入到 POS 机设备中，POS 机设备经过诸如因特网或电话网之类的网络将顾客的信息通信到交易平台的服务器。此外，可以通过交易平台的职员接收申请信息（例如，经过与申请人的电话呼叫），并由该职员输入到服务器中（或输入到与服务器通信的计算机中）。此外，可以将顾客引导到一个网页或建造以便允许输入申请信息的店内亭子间（例如，卡可以包含网页的网址）。申请人可以直接将他的或她的申请信息输入到网页中，由此将他的或她的申请信息通信到服务器。服务器一般可以用许多方式接收申请信息。

申请信息本身可以包括进行信用检查所需的信息，以便确定个体的信誉。例如，这种信息可以包括诸如申请人的姓名、地址、电话号码、和/或社会保险号码之类的标识信息，并且也可以包括雇佣信息，例如，行业的地点以及在这个行业地点工作的年数等等。申请信息可以构成服务器适当处理申请人的财务交易所需的一个最小信息集。根据一些实施例，服务器接入到一个可以存储有关申请人的各种信息的数据库。这种信息可以包括健康信息，紧急联系信息，家庭信息，等等（这些其他形式的信息要在下面讨论）。在接收到申请信息的时刻，交易平台的服务器可能不接收上述的其他形式的信息。因此，服务器利用申请信息填充上述数据库中的有关申请人的申请的一个或更多的表，并且也最小地填充有关申请人和其他

---

事务的其他表。如果申请最终获得批准，可以在以后的时间从申请人/持卡人收集其他类型的信息，和可以更充分地填写数据库的各种表。

在接收到申请信息之后，服务器将信息输入到数据库中，以将申请人的卡号与申请人的申请信息结合（操作 306）。然后，执行申请的评价（操作 308）。根据一些实施例，可以对申请人执行信用检查。申请信息可以包括足够的信息量以查询信用分数服务（例如：Fair Isaac Co.），从而获得个体的信用分数（例如：FICO 分数）。例如，信息协会的服务器可以经过因特网之类的网络与信用分数服务通信，以确定与个体有关的信用分数。如果信用分数超过一个特定阈值，那么批准申请，否则拒绝申请。根据其他实施例，将申请人的申请信息经过因特网之类的网络通信到一个或更多的发卡银行。每个发卡银行单独地使用申请信息来执行它们自己的分析，并独立地得出拒绝还是批准申请的决定。根据一些实施例，交易平台的服务器比较核准发卡银行提供的信贷条件，并且选择提供最佳信贷条件的发卡银行作为与卡号相结合的银行。根据其他实施例，每个发卡银行可以通信一个出价，例如，它愿意付给交易平台以获得该账户的货币金额，例如，交易平台可以选择提供最高出价的银行。根据其他实施例，可以有一个以上的银行与卡号结合，并且对于每次购买，允许申请人/未来的持卡人从多个银行中选择贷款扩展。

不管如何进行分析，如果评价指出申请被核准，那么服务器将信息输入到数据库中，将规则与申请人的卡结合，如操作 310 中所示。例如，可以将根据信用分数确定的花费限额与卡结合（或，发卡银行可以确定限额并且将限额通信到交易平台的银行），也可以将普通的反欺诈数据与卡结合，等等（操作 312）。然后，可以将卡激活（操作 314），这意味着可以用卡执行交易，例如，可以用于赊帐购买货物或服务（或，如下面讨论的，可以以另外的方式使用，例如，作为签帐卡，储值卡等办理购买）。为了便于执行交易，将分配给交易卡的 PIN 通信给核准的申请人。例如，可以将 PIN 经过短消息服务消息，经过无线或其他装置接收的电子邮件，经过 POS 机设备，等等，通信到持卡人。在与具有小于一个特定量的货币值的交易结合的基础上，这个 PIN 既可以是永久的 PIN，或可以是在一个特定时间周期中、特定的使用次数中有效的。

另一方面，如果操作 310 指示申请被拒绝，那么卡不被激活（316），这意味着卡不能用于执行交易。

操作 300-314 可以几乎瞬间地实施。例如，根据一些实施例，操作 300-314 可以在小于一分钟内进行，根据其他实施例，这些操作可以在小于 30, 15, 和/或 5 秒钟内进行。因此，例如，申请人可以在商店的 POS 机设备开始购买的同时申请卡，并且可以实际地使卡激活，从而申请人可以使用卡办理购买（和在其他商店办理其他购买，等等）。由于卡是匿名的，所以卡无需包含标识持卡人的印刷，而且卡的存储介质中也无需编码这种标识信息或 PIN。因此，在申请处理过程之后，没有等待在卡上印刷的周期，或等待在卡的存储介质中编码标识申请人的信息的周期。

如参考图 2 所述的，为了使用所述的交易卡办理购买，POS 机设备（例如，收银机）可以读取一个给定的卡，并且可以将信息经过开放网通信到交易平台的服务器。图 4 示出了一个其中可以容纳图 2 的 POS 机设备 202 的示例网络环境。如从图 4 可以看到的，一个给定的商店可以具有多个 POS 机设备 202 位于其中。每个 POS 机设备 202 可以耦合到一个局域网（LAN）400。仅为了说明的原因，将图 4 的 LAN 说明为一个以太网网络。LAN 400 可以是任何结构的和使用任何协议的。

各 POS 机设备 202 经过 LAN 400 与服务器 402 通信。服务器 402 保持着一个存储有关经过每个 POS 机设备 202 进行的所有交易的信息的数据 404。（如下面要讨论的，每个交易一般用一个交易标识符标识）。服务器 402 可以经过一个路由器 406 向/从一个诸如因特网之类的开放网络传送信息。

图 4 的网络环境是仅为图示说明提供的例子。还有许多其他环境，并且是熟悉本领域的人员知道的。图 5 示出了配置的交易内核，即，在 POS 机设备 202、服务器 402、二者的某种组合、和/或与 POS 机设备和/或服务器 402 通信的任何计算装置存储和执行的各种软件单元。在这里，图 5 的内核的讨论是以将它配置在图 4 的网络环境中的假设为前提的，但是如同任何一个熟悉本领域的人员所知道的，它的模块可以适用于任何网络环境。

转到图 5，POS 机设备 202 耦合到一个输入装置 500，例如，磁条

---

或条形码阅读器，或 RFID 收发器。在购买的交易中，利用磁条阅读器 500 阅读卡上的磁条。当然，如果卡的存储介质是条形码，那么可以将输入装置 500 实现为一个条形码扫描器。同样地，如果卡的存储介质是 RFID 芯片，那么可以将输入装置 500 实现为一个 RFID 收发器。当输入装置 500 阅读卡的存储介质时，将唯一地标识卡的卡号从中读出。输入装置 500 也可以包括持卡人能够用于输入个人身份号（PIN）的小键盘。PIN 代码和卡号从输入装置 500 通信到 POS 机设备 202。

POS 机设备 202 具有通用计算装置的结构。也就是说，POS 机设备 202 包括一般能够在普通计算机中见到的组件，即，它包括一个耦合到一级或多级存储软件和数据的存储器的处理器。处理器经过输入/输出（I/O）总线与包括诸如监视器之类的显示器在内的输入、输出、和通信装置通信，并且也能够与键盘、鼠标器或诸如触控板之类的指点装置、和/或扬声器等通信。各种外围装置也可以经过 I/O 总线与处理器通信，这些外围装置包括网络接口卡、硬盘驱动器、或其他海量数据存储器、诸如 CD ROM 驱动器或 DVD 驱动器（可以是可读和可写的）之类的可取出介质驱动器、无线接口、磁条阅读器、条形码阅读器、RFID 收发器、等等。应当知道，计算机目前使用着许多芯片组和体系结构。POS 机设备 202 广义地代表所有的这种芯片组和体系结构，并且这里所述的内核的各种实施例以及各种软件方法可以在所有这些芯片组和体系结构上执行。

PIN 代码和卡号提取器模块 502 可以驻留在 POS 机设备 202 的存储器中，或与之通信和/或构成网络的任何其他装置中，并且通过它的处理器执行。用“模块”表示软件的一个单元或部分，例如：函数、对象、函数和/对象集、和/或可以由 POS 机设备 202 的处理器执行的计算机指令集（例如机器码）。当然，模块提供的功能也可以由一个或多个专用集成电路（ASIC）的协同作用实现，或由一个或更多的 ASIC 以及存储在存储器中并由处理器执行的软件的模块的协同作用实现。一旦输入装置 500 将 PIN 代码和卡号通信到 POS 机设备 202，提取器模块 502 从输入装置 500 通信到 POS 机设备 202 的数据集读出卡号和 PIN 代码。如下面要讨论的，提取器模块 502 将 PIN 代码和卡号信息通信到根据一些实施例的、可能由服务器 402 存储和执行的其他软件模块。

POS 机设备 202 与服务器 402 管理的数据库 404 通信。提供了一个应用界面 (API) 504，以允许 POS 机设备 202 与数据库相互作用。根据一些实施例，数据库 404 是根据一个包括多个构造以存储有关已经在商店销售的项目的信息的表的模型组织的。数据库 404 也可以存储其他信息。例如，如果特定的商家操作许多商店，数据库 404 可以存储有关已经在商家的所有商店，或在一个区域内的商家的所有商店销售的项目的信息。此外，数据库 404 可以存储有关商品库存的信息、供应商信息、和其他操作特定生意中有用的信息。如同熟悉本领域的人员所知道的，像图 4 的网络结构一样，数据库 404 的模型对于每个商家都是不同的，并且可以对于每个商店都是不同的。

尽管数据库 404 使用的模型可以随每个商家改变，但是数据库通常都包括存储说明每项交易的详细情况的记录的表。在这里将这种表说明为“交易表” 506。一般组织一个交易表 506 以便用一个交易标识符 508 唯一地标识每项交易，即，交易标识符 508 可以是交易表 506 的主关键字。每个交易标识符 508 可以结合多个字段 510。提供这些字段 510 以存储有关包括在交易中的每一项的信息。例如，字段可以包括以下的一个或多个：

- (1) 包括在交易中的每一项的零售设备 (SKU) 号；(2) 包括在交易中的每一项的价格；(3) 包括在交易中的每一项的内部说明；(4) 包括在交易中的每一项的外部说明；(5) 包括在交易中的每一项的一般说明；(6) 包括在交易中的每一项的所属种类；(7) 与包括在交易中的每一项相关的销售税；(8) 交易发生的日期；(9) 交易发生的时间；(10) 指示发生交易的特定商店的标识符；(11) 指示发生交易的特定 POS 机设备的标识符；(12) 指示在交易日期和时间操作特定的 POS 机设备的雇员的标识符；(13) 用于处理特定交易的支付方法的指示，例如，现金信用卡，等等；(14) 交易的总价；(15) 交易类型的指示符，例如，购买、退款、退货、数据查询、等等；和/或(16) 说明交易的主体和/或环境的其他信息。刚才一般提到的种类的信息，即，交易的总价、日期、时间、和/或位置（例如，商家和城市/州的标识符）之外的信息，被称为“三级数据 (level three data)”。

在 POS 机设备 202 扫描了包括在交易中的每一项之后，可以选择支付

技术。POS 机设备 202 可以提供一个查询要经过交易卡执行的交易的类型的屏幕，例如，是要把卡用作信用卡、签账卡、和/或储值卡（如前面说明过的，交易卡在一种交易中可以被用作信用卡，在另一种交易中用作签账卡，在又一种交易中用作储值卡）。POS 机设备 202 利用 API 504 建立一个新的交易标识符 508，以唯一地标识它正在执行的交易。然后，可以将关于交易的交易类型和三级数据与交易标识符 508 结合地存储在交易表 506 中。根据一些实施例，PIN 和卡号提取器 502 也捕获交易类型，并且如下面讨论的，将交易类型数据传送到第二加密模块 522。

监视模块 512 与 API 504 相互作用，以观察交易表 506 内新的交易标识符 508 的建立。一旦观察到新的交易标识符 508 的建立，监视模块 512 呼叫数据提取模块 514 启动它的操作。

根据一些实施例，数据提取模块 514 与 API 504 相互作用，以提取包括交易标识符 512 的与新交易结合的三级数据。根据其他实施例，数据提取模块 514 与 API 504 相互作用，以提取小于三级数据的全部范围的数据。例如，数据提取模块 514 可以仅从数据库 404 获得交易标识符和交易的总价。仅为了说明的原因，本文件将数据提取模块 514 说明为从数据库 404 获得三级数据的全部范围内的数据。

为了允许数据提取模块 514 从数据库 404 获得数据，在安装图 5 中所示的内核时，给数据提取模块提供允许这种提取的信息。例如，可以根据交易表 506 的名称，和从中获得数据的各个字段 510 的名称改变数据提取模块 514 的代码和/或数据空间。

在数据提取模块 514 获得三级数据时，将它输入到存储器 516 的一个存储区中，以传送到第一加密模块 520。在第一加密模块 520 的传送之前，一个充分性模块 518 检查捕获的数据，并且与 PIN 和卡号提取器 502 相互作用，以保证：(1) 数据提取模块已经捕获到至少一个总价和一个交易标识符；和 (2) PIN 和卡号提取器 502 已经捕获到卡号和 PIN。如果上述数据没有被捕获的，那么指示错误，并且将内核的关于交易的操作停止。另一方面，如果捕获到上述数据，那么将存储在存储器 516 中的数据传送到第一加密单元 520。

第一加密单元 520 利用 PIN 和卡号提取器 502 捕获的 PIN 和卡号作为

密钥给三级数据和交易类型数据（如图 5 中所示的，从 PIN 和卡号提取器 502 接收的交易类型数据）加密，从而建立第一加密对象 600。图 6 中示出了第一加密对象 600。将第一加密对象 600 从第一加密模块 520 传送到第二加密模块 522。

第二加密模块 522 接收第一加密对象 600，并且附加上卡号，建立一个附加的数据集。（卡号是从 PIN 和卡号提取器 502 接收的，如图 5 中所示）。然后，将商家的口令用作密钥给附加的数据集加密，从而获得第二加密对象 602。图 6 中示出了第二加密对象 602。将第二加密对象 602 从第二加密模块 522 传送到第三加密模块 524。根据一些实施例，商家的口令是一个 64、128、256、512 位的值，或一个适合于在沿开放网发送时防止被无照商家将第二加密对象 602 解密的另外长度的值。商家口令一般是保密的，并且仅为商店和交易平台的一组选定的必要雇员所知。根据一些实施例，商家口令是在把内核安装在商店的服务器 402 上时输入到内核的代码和/或数据空间中的。

第三加密模块 524 接收第二加密对象 600 并且附加上商家标识符、商店标识符、和 POS 机设备标识符，从而建立起一个附加的数据集。商家标识符是一个唯一地标识商家的值（例如，一个指示交易发生在一个 Target 商店的值）。商店标识符是一个唯一地指示交易发生的特定商店的值（例如，一个指示交易发生在哪个 Target 商店的值）。POS 机设备标识符是一个唯一地指示交易发生的特定 POS 机设备 202 的值（例如，一个指示交易发生在哪个收银机的值）。商家标识符、商店标识符、和 POS 机设备标识符是经过 API 504 从数据库 404 得到的。根据一些实施例，在把图 5 的内核安装在商家的服务器 402 上时，将包含这种信息的数据库内的表和字段的名称输入到第三加密模块 524 中（例如，输入到第三加密模块 524 的代码和/或数据空间中），以便能够与 API 504 相互作用获得这种信息。第三加密模块 524 随后利用与交易平台结合的公用密钥给附加的数据集加密，产生传送对象 604。图 6 中示出了传送对象 604。根据一些实施例，公用密钥是一个 64、128、256、或 512 位值，或适合于在沿开放网发送时防止被无照商家解密的另外长度的值。将传送对象 604 与 SSL 模块 526 使用的 SSL 加密密钥一同传送到加密套接字协议层（SSL）模块 526。根据一些

---

实施例，上述 SSL 加密密钥是由一个随机数发生器产生的，而公用密钥可以直接硬编码到第三加密模块 524 中。

SSL 模块 526 接收传送数据对象 604，并使用 SSL 加密密钥给传送对象加密，产生加密传送对象 606。图 6 中示出了加密传送对象 606。尽管图 5 将 SSL 加密密钥显示为是由第三加密模块 524 中的随机数发生器产生的，但是，根据其他实施例，SSL 加密密钥可以由 SSL 模块 526 产生。

SSL 层 526 将加密传送对象传送到传输控制协议/网际协议（TCP/IP）模块 528，以通过开放网 408 通信到交易平台的服务器。（根据图 4 的示例网络环境，传送对象被作为通过路由器 406 路由的一个或多个信息包通信到开放网 408）。

图 7 示出了一个在交易平台的服务器上执行的软件系统的示例实施例。交易平台的服务器被构造为能够至少包括与通用计算装置相同的元件。也就是说，交易平台的服务器包括一般能够在通用计算机中看到的组件，即，包括耦合到存储软件和数据的一或更多级的存储器的处理器。处理器经过输入/输出（I/O）总线与包括诸如监视器之类的显示器在内的各种输入、输出、和通信装置通信，并且能够与键盘、鼠标器或诸如触控板之类的其他指点装置、和/或扬声器等通信。各种外围装置也可以经过 I/O 总线与处理器通信，外围装置包括网络接口卡、硬盘驱动器、或其他海量数据存储装置、诸如 CD ROM 或 DVD 驱动器之类的可取出介质驱动器（可以是可读和可写的）、无线接口、磁条阅读器、条形码阅读器、RFID 收发器、等等。应当知道，服务器当前使用许多芯片组和体系结构。在整个文件中，将交易平台的服务器说明为单独的，即，仿佛它是一个单独的机器。当然，服务器实际上可以是由多个协同操作执行这里所述的功能的服务器构成的。例如，两个或更多的服务器可以各自地执行这里所述的所有功能，并且在受到负载余额器的指派时，它们可以操作客户机程序（即，安装在各种地点的各种交易内核）。此外，两个或更多的服务器可以在第一服务器执行这里所述的操作的一个子集，并且可以与执行这里所述的操作的另一个子集的第二服务器通信的意义上协同操作。

仅为了说明的目的，参考一个信用交易提供图 7 的功能的说明。如这里所讨论的，在下面，同样的基础设施可以用于处理借方交易，储值交易，

---

数据存取交易，和它们的组合。

图 7 的软件系统包括一个接收一个或更多的信息包，构成加密传送对象 606 的组合有效负载，的 TCP/IP 模块 700。TCP/IP 模块 700 从一个或更多的信息包重构加密传送对象 606，并且将加密传送对象 606 传送到 SSL 模块 702。SSL 模块 702 利用 SSL 加密密钥给加密传送对象解密，产生传送数据对象 604。（如同熟悉本领域的人员知道的，SSL 模块借助启动安全 SSL 会议的协商存取 SSL 加密密钥）。然后将传送数据对象 604 传送到第一解密模块 704。

第一解密模块 704 经过 API 708 接入数据库 706。数据库 706 包括每个持卡人的财务数据，和其他数据，并且也将在下面更详细地讨论。根据一些实施例，第一解密模块 704 存取数据库 706，以获得交易平台的私有密钥，然后解密传送对象 604，产生第二加密对象 602 和附加的商家标识符，商店标识符，和注册标识符。根据其他实施例，第一解密模块 704 具有硬编码到其代码空间中的上述私有密钥，或从一个存储器的存储区存取私有密钥。在任何情况下，都要把第二加密对象 602 和附加的商家标识符、商店标识符、和注册标识符传送到第二解密模块 710。

第二解密模块 710 也经过 API 708 接入数据库 706。第二解密模块 710 利用从第一解密模块 704 传送到它的商家标识符获得商家的口令。例如，可以将商家标识符用作存取数据库 706 中的一个表的密钥，以发现商家的口令。因此，第二解密模块 710 可以存取一个将商家标识符与商家的口令相关联的表，并且可以将商家标识符用作获得商家的口令的密钥。然后，将商家的口令用于解密第二加密对象 602，产生附加了卡号、商家标识符、商店标识符、和注册标识符的第二加密对象 600。将第一加密对象 600 和上述附加的数据传送到第三解密模块 712。

第三解密模块 712 接收包括卡号在内的上述数据，并经过 API 708 存取数据库 706。第三解密模块 712 利用卡号从数据库 706 获得卡标识符和 PIN。可以将卡号用作密钥，以存取将卡号结合到卡标识符和直接或间接地结合到 PIN 的表。例如，可以将卡号用于存取将卡号结合于卡标识符和 PIN 代码标识符的表。然后，利用 PIN 代码标识符可以存取将 PIN 代码标识符与 PIN 相关联的表，以便获得 PIN。如熟悉本领域的人员所知道的，

可以用加密格式存储 PIN，以便使其不能被盗用。一旦从 PIN 存储在其中的表中检索到 PIN，假设请求任务具有请求这种解密的适当的存取级别，那么给 PIN 解密。一旦接收到 PIN，第三解密模块 712 解密第一加密对象 600，产生三级数据，以及卡号、商家标识符、商店标识符、和注册标识符。(当然，如参考图 5 讨论的，在一些情况下，第一加密对象 600 的有效负载可以仅包括总价和交易标识符)。

将上述数据传送到余额检验模块 714，余额检验模块 714 也像各解密模块 704、710、和 712 一样，经过 API 708 接入数据库 706。首先，余额检验模块 714 从数据库 706 获得与卡号相联系的当前余额和信贷限额。例如，余额检验模块 714 可以存取包含将卡详细信息与卡标识符相关联的表。然后，利用第三解密模块 712 得到的卡标识符作为密钥，寻找当前余额，并获得信贷限额外值。将当前余额和建议的交易的总价的总和与信贷限额比较。如果总和超过信贷限额，那么可以拒绝建议的交易（下面要进一步讨论）。否则，处理流前进到欺诈检验模块 716。

欺诈检验模块 716 经过 API 708 接入数据库 706。欺诈检验模块 716 从数据库得到与卡号相关联的欺诈指示规则。根据一些实施例，规则中的一些或全部可以由持卡人确定（这将在下面讨论）。此外，规则中的一些或全部可以是不用从持卡人输入而产生的系统规则。可以将建议的交易和最近的交易的参数与欺诈指示规则比较。如果欺诈指示规则中的检验是肯定的，那么可以联系持卡人。交易平台的雇员可以经过电话联系持卡人（应当注意，包括持卡人的电话号码在内的持卡人的联系信息存储在与主账户和卡标识符结合的表中，如图 8 中所示）。可以要求持卡人确认他的身份

（例如，可以要求回答电话的个体证实自己的身份，和可以询问与卡号相关联的 PIN），并且也可以要求确认交易是合法的。此外，可以经过短消息服务（SMS）模块 718 的操作联系持卡人。例如，SMS 模块 718 可以将 SMS 消息发送到持卡人的蜂窝电话（这个号码与卡号结合地存储在数据库 706 中），要求持卡人确认建议的交易应当被核准。为了使确认的交易能够被核准，持卡人必须做出肯定的回答，并且也必须输入他的 PIN 代码。SMS 模块 718 接收回答消息，并将它返回到欺诈检验模块 716。如果返回的消息指示建议的交易没有被核准，那么拒绝建议的交易（后面讨论），并且

---

将卡冻结（也在以后讨论）。如果返回的消息指示交易是合法的，并且也包含与卡相关联的 PIN，那么执行流前进到简表检验模块 720。

简表检验模块 720 在子（child）卡上操作。“子”卡是与父（parent）卡关联的同一主账户（参考图 8 讨论）相关联的卡。这种关联的效果是，父卡与任何数目所关联的子卡利用相同的资金，即，利用相同的信贷限额，利用相同的储值，利用相同的预付服务或货物的余额，和/或利用相同的支票存款账户或银行账户。与父卡关联的持卡人接收呈现与主账户关联的所有账户的交易的结算表，也就是说，父卡的持卡人接收到呈现经过父卡和任何子卡执行的交易的结算表。如下面要详细讨论的，父卡可以规定子卡的花费允许额度的规则。例如，假设父亲是持卡人的情况。父亲可以建立由他的儿子或女儿使用的子卡。子账户产生的账单积累到父亲的账户上的账单中。父亲可以对孩子的账户指定一些规则。例如，父亲可以将只允许子账户每个选定的时间单元到达选定水平的债务（例如，每月\$250）的规则与子账户结合。其他规则包括，但不限于：(1) 不允许购买某些 SKU 或某些 SKU 的种类（例如：不允许指示购买的项目是酒精的 SKU 的购买）；(2) 不允发生在某些商家、商家类型、和/或商家种类的购买；(3) 仅允许发生在某些商家、商家类型、和/或商家种类的购买。为此，根据一些实施例，数据库 706 存储着一个或更多的将存储在其中的各种商家标识符与商家类型和/或商家种类结合的表。简表检验模块 720 通过检索与卡号结合的规则（如果有的话）和对照规则测试建议的交易而操作。如果违犯了任何规则，那么如同参考欺诈检验模块 716 说明的那样，联系父卡的持卡人，以求允许交易。

例如，简表检验模块 720 可以通过存取将子卡的卡标识符与控制它的父卡相关联的表而操作。简表检验模块 720 可以检查该表，以确定其中是否有卡标识符（最初由第三解密单元 712 检索的）对应于父卡。如果在表中没有发现，那么该卡不是子卡，并且没有父卡指定的规则与之关联。作为选择，如果在表中发现了它，那么它是子卡，并且可以具有与之关联的规则。在这种情况下，上述表可以将子卡与可以用作另一个表的密钥的值结合，所述另一个表将上述的值与指向实现为卡选择的规则的可执行代码的指针结合。然后，如上所述，执行可执行代码以确定是否违反了任何规

则。

如果余额检验模块 714、欺诈检验模块 716、或简表检验模块 720 中的任何一个指示不应当允许交易，那么控制转到拒绝/冻结模块 722。拒绝/冻结模块 722 拒绝交易，并且将消息发送到 POS 机设备，指示建议的交易已经被拒绝(有关对于 POS 机设备的返回消息的结构的细节将在下面说明)。此外，如果欺诈检验模块 716 指示购买是欺骗性的，那么与卡关联的账户被冻结，也就是说不允许任何未来的交易，直到卡被重新激活。

如果余额检验模块 714、欺诈检验模块 716、和简表检验模块中的每个都指示应当允许交易，那么控制转到记录交易模块 724。记录交易模块把三个解密模块 704、710、和 712 恢复的，包括三级数据在内的数据输入到数据库 706 中。例如，将与商家分配的标识符不同的交易标识符分配给交易。由新分配的交易标识符标识的新记录建立在将有关交易的详细情况与新分配的交易标识符联系在一起的表中。然后，利用三个解密模块 704、710、和 712 恢复的、包括三级数据在内的数据填充新记录的各个字段。(商家的交易标识符也与新分配在的交易标识符结合地存储在上述表中，从而保存了交易平台的交易标识符与商家的交易标识符之间的联系。)

如上所述，交易的拒绝/核准被通知给位于商家的 POS 机设备。根据一些实施例，如图 9 中所示构造的消息经过 SSL 模块 702 和 TCP/IP 模块 700 发送到前面讨论过的在商家的服务器 402 上执行的内核。如在图 9 中看到的，消息包括建议的交易是被核准还是被拒绝的指示 900，商家的数据库分配的交易标识符 902，以及商家标识符、商店标识符、和注册标识符 904。

内核的 TCP/IP 模块 528 接收图 9 的消息(图 5)，并且传送到 SSL 模块 526，在 SSL 模块 526 将其解密。其有效负载传送到确认模块 530，确认模块 530 利用 API 504 使用有关核准或绝句的信息更新数据库 404。(建议的交易是被核准还是被拒绝的指示 900 与商家的交易标识符 902 相关联括在图 9 的消息中)。根据一些实施例，在把内核安装在商家的服务器 402 上时，改变确认模块 530 以包括用于这种信息的输入的适当表和字段名称(例如，改变确认模块 530 的代码和/或数据空间，以包括用于这种信息的输入的适当位置的表名称和字段名称)。然后，利用商家标识符、商店标

---

识符、和注册标识符确定如何将有关拒绝/核准的信息路由到适当的 POS 机设备 202，并且使用交易标识符拒绝/核准适当的交易。

如前面讨论中说明的，根据一些实施例，在与交易的执行同时的时间点，收集作为给定交易的主体的三级数据，传送到图 7 的软件系统，和存储在数据库 706 中。这提供了某些值得注意的，但是对于本发明的实践并不是必须的优点。例如，由于三级数据是在交易的执行过程中被捕获和输入到数据库 706 中的（与在交易执行之后相反），软件系统可以检查三级数据并将这些三级数据与各种规则比较，以确定应当核准还是拒绝建议的交易。如下要讨论的，持卡人可以选择，例如，如果一种特定的货物或货物的种类或种类是交易的主体，那么将建议的交易识别为可能是欺诈性的欺诈检测规则。显然，如果直到交易执行之后作为交易主体的货物的身份仍然短缺或没有被收集到，那么不能使用这种规则。也如下面讨论的，持卡人可以定制控制“子卡”开销的允许额度的规则。例如，持卡人可以规定，禁止子卡执行其中一种特定的货物或货物的种类是交易的主体的交易。如果直到交易执行之后，有关作为给定交易的主体的货物的身份仍然短缺或没有被收集到，那么也不能利用这种规则。最后，由于三级数据是在交易的同时收集和存储的，所以可以给持卡人提供有关利用与他的或她的卡结合任何卡购买的项目（包括，例如：经过子卡购买的项目）的身份和其卡号实施例这种交易的卡的身份的信息。这种信息可以实时地，或接近实时地提供，例如，经过网站或呼叫中心。

根据一些实施例，数据库 708 可以如同图 8 中所示那样组织。从图 8 可见，可以如此地组织数据库，使得卡号 800，即，一组编码/存储/包含在交易卡上的存储介质上的并且唯一地标识该卡的数据，与卡标识符 802 相结合。卡标识符 802 是一组唯一地与数据库 706 中的卡号 800 关联的数据（例如，整数）。卡标识符又与主账户号 804 相关联。

主账户号 804 是一组与可以经过交易卡存取的每个账户的所有账户信息 806 相关联的，并且也与可以经过卡存取的所有持卡人信息 808 相关联的数据。例如，主账户号与可以经过卡存取的每个账户的余额相结合。因此，它可以与贷方余额（在卡用作信用卡的时候），银行账户余额（当卡用作签帐卡的时候），和/或储值余额（当卡用作储值卡的时候，例如，赠

卷卡、预付货物和/或服务卡、等等)相结合。主账户号 804 也可以与通过可以由卡存取的每个账户执行的所有交易的所有细节，例如，三级数据，相结合。此外，主账户号 804 与控制卡的每个规则相结合，例如，与利息规则、逾期付款规则、欺诈检测规则、子账户开销规则等等，相结合。此外，主账户号 804 与有关能够通过卡存取的每个账户相关联的金融机构的信息结合，例如，与卡用作信用卡之后提供贷款限额的银行的信息结合。一般地讲，要求的和/或与作为信用卡、签帐卡、和/或储值卡的卡的容量结合的每个数据单元都直接或间接地与主账户号相结合。

上述安排提供了某些值得注意的优点，但对于本发明的实践并不是必要的。例如，假设与卡号 800 相关联的交易卡被盗窃，可以将具有另一个号卡，例如，具有卡号 810 的另一个卡与主账户号再关联（通过新的卡标识符 812）。在这样做时，所有账户信息 806 和持卡人信息 808 保持不变，并且没有这种信息被丢失。

图 8 的安排中存在着值得注意的、但并非是实践本发明所必须的另外的优点。如图 8 中所示，可以将一个以上的卡号 800 和 810 与同一个主账户号 804 相关联。结果是，持卡人可以选择拥有两个交易卡，例如，一个为个人使用，一个为业务使用。（尽管这个例子说明了与特定主账户号 804 相关联的两个卡号 800 和 810，但是可以有任何数量的卡号 800 和 810 与同一个主账户号 804 结合。）因此，单一的结算标或网页可以给持卡人提供一个分类帐目，显示，例如，每个卡的总消费，或甚至在逐个交易的基础上，提供每个卡的所有三级数据（例如，每个项目和与之结合的价格）。

根据一些实施例，交易可以不使用交易卡进行，而是可以经过诸如蜂窝电话和/或个人数字助理之类的无线装置进行。仅为了说明的目的，参考蜂窝电话说明下面的示例实施例。如前面说明过的，交易可以在 POS 机设备 202 启动，在 POS 机设备 202 服务人员扫描与购买的项目结合的条形码。在这点，服务人员问询持卡人的蜂窝电话号码（或获取蜂窝电话号码，例如，让持卡人呼叫获取持卡人的蜂窝电话号码并将它通信到 POS 机设备 202、商家服务器 402、或与 POS 机设备 202 和/或商家的服务器 402 通信的计算机系统的专用号码），并且将电话号码输入到 POS 机设备 202 中。

然后，POS 机设备 202 将三级数据输入到数据库 404 中，如前面参考

图 5 说明过的。这又造成监视模块 512 观察交易表 506 中新的交易标识符 508 的建立，从而产生一组除了以下事件之外的、前面所述的事件。指令第一加密模块 520 使用持卡人的蜂窝电话的电话号码给三级数据加密，产生第一加密对象 1000，如图 10 中所示。然后，第二加密模块 522 将蜂窝电话号码附加到第一加密对象（替代这里放置的卡号），并且如上所述，用商家口令给附加的数据集加密，产生第二加密数据集 1002。其余的内核功能与前面说明过的相同。

在交易平台的服务器，许多处理与前面参考图 7 说明过的处理相同，只是有以下例外。在传送第一加密对象和附加的数据时，第三解密模块 712 检测已经插入代替卡号的蜂窝电话号码（例如，这种检测可以凭借蜂窝电话号码和交易卡号是不同长度这样的事实来进行）。一旦检测到蜂窝电话号码已经插入代替了卡号，第三解密模块 712 使用蜂窝电话号码作为解密密钥对第一解密对象解密。然后，第三解密模块 712 调用具有蜂窝电话号码的 SMS 模块 728。SMS 模块 728 将 SMS 消息发送到提供到它的的电话号码。SMS 消息指示交易的总价和进行建议的交易的商店的名称。消息提示使用者确认或拒绝交易。如果使用者确认交易，那么他把他的 PIN 输入到电话中，并且 Java 程序（applet）和/或其他形式的可执行代码将 PIN 与使用者的卡号捆绑在一起（事先改变 Java 程序和/或其他形式的可执行代码以将卡号包括在它的代码或数据空间中），产生指示建议的交易被确认的回答，并且其中包括使用者的卡号和与其结合的 PIN。根据一些实施例，确认或拒绝交易的回答消息是经过由装置建立的无线因特网连接通信的，并且是经过 SSL 协议加密的。将回答消息返回到第三解密单元 712。如果回答消息拒绝交易，那么交易被拒绝，如前面参考图 7 说明的。另一方面，如果回答消息核准交易，那么如前面说明过的，第三解密模块 712 存取数据库 706，以根据卡号检索使用者的 PIN。如果检索的 PIN 与输入到蜂窝电话中并且经过 SMS 模块 728 传送到第三解密模块 712 的 PIN 匹配，那么处理如同前面参考图 7 说明过的那样继续进行（即，如常执行余额检验，欺诈检验，和简表检验）。

上述的效果是，持卡人可以通过简单地将他的蜂窝电话号码提供给 POS 机设备 202 的服务人员而处理购买交易。在服务人员扫描进购买的项

---

目之后，持卡人接收到要求持卡人确认总价的正确性的 SMS。持卡人通过肯定地回答 SMS 和输入他的 PIN 而确认。

根据一些实施例，持卡人可以使用诸如蜂窝电话之类的无线装置来办理从没有安排与图 5 的内核相互作用的有线 POS 机设备的卖主购买货物或服务。用 Java 程序给无线装置编程，以允许输入交易的总货币之和、商家标识符、和与持卡人的交易卡关联的 PIN 号码。根据一些实施例，Java 程序是在安装时进过配置的，以能够存取持卡人的卡号。然后，Java 程序将卡号、商家标识符、交易总量、和说明交易的类型的交易类型数据单元组合到首先使用 PIN 作为加密密钥加密，然后用 SSL 加密的数据包中。在图 7 的软件系统，数据包首先被 SSL 模块 702 解密，然后用第三解密模块 712 解密。然后，处理如前面说明过的那样进行。

如上所述，图 5 的内核和图 7 的软件系统可以协同操作，以执行各种各样的交易，并且可以通过改变图 6 的加密传送对象中携带的数据完成这些种类的交易。例如，上述基础设施可以协同操作，以执行“私人俱乐部购买 (private club purchase)”。私人俱乐部购买是一种在需要成员资格的商家进行的购买（例如，Sam's Club 和电影出租商店，等等）。例如，考虑一个个人希望从电影出租商店租一部电影的情况。为了进行购买，这个商店一般要求出示会员卡。会员卡一般包含编码了与会员账户结合的号码的存储介质（条形码，磁条，等等）。考虑到这里的基础设施，这种会员卡已经过时了。

作为一个初始步骤，持卡人可以将他的会员账户号（或其他与之关联的标识号码，例如，编码在他的会员卡的存储介质上的号码）与他的主账户关联。在租电影时，持卡人出示这里所述的用于购买电影租赁和提供他的会员账户的类型的交易卡。雇员可以如前面所述的那样“扫描”该卡，开始前面说明过的事件。但是，在这种情况下，将交易类型数据设置到一个值，以指示私人俱乐部购买正在进行。（三级数据带有说明被出租的电影的标题，等等）。因此，将具有标识电影出租商的商家标识符、标识特定商店的商店标识符、标识特定的 POS 机设备的 POS 机设备标识符、交易卡的卡号、刚刚说明过的三级数据、和刚刚说明过的交易类型数据的加密传送对象通信到图 7 的软件系统。

一旦接收到加密的传送对象，系统如前面说明过的那样开始行动，只是有以下的不同：该系统存取数据库 706 中的一个将私人俱乐部号码（或其他与之关联的号码）与主账户和卡标识符关联的表。该系统获得上述会员号码，并且在图 9 的回答信息包中返回该号码以及其中所示的元素。因此，给 POS 机设备提供了有关财务交易的核准/拒绝信息，并且也提供了持卡人的会员号码。因此，不需用两个卡来完成私人俱乐部交易。

上述基础设施也可以用于进行数据获取交易。数据获取交易是一种使用卡获得与卡的标识符以及与主账户关联的信息的交易。这种检索的信息可以是简单的。例如，检索的信息可以提供一个个人是否的确是一个组织的成员（例如，一个个人是否是某个健康俱乐部的成员）的指示。作为选择，信息可以是复杂的，例如，指示持卡人的健康信息。在数据获取交易的环境下，基础设施如同前面所述的那样操作，只是具有以下的不同，下面参考持卡人用他的卡向卫生保健机构（医院，诊所，等等）提供卫生保健信息的过程来说明这些不同。

作为最初的事情，持卡人在数据库 706 中建立一组标识可以检索哪些种类的数据的规则。例如，规则说明可以通过用它们各自的商家标识符标识的各种机构从卡检索的卫生保健数据的种类。

在卫生保健设施，“扫描”卡以读取其上的存储介质，并且发生前面所述的一系列事件。但是，在这种情况下，持卡人可能已失去意识，从而输入的 PIN 可以是“911”，或一些其他预定的 PIN。将交易类型数据设置到一个指示数据获取交易正在进行的值。（三级数据可以是空或可以用空数据填充，例如，商店标识符和销售点标识符这样的数据，但是，在一些情况下，要填写这些字段以便使得能够将回答消息路由到卫生保健设施内的适当交易执行装置）。因此，具有标识卫生保健设施的商家标识符、卡号、和刚才说明的交易类型数据的加密传送对象被通信到图 7 的软件系统。（在某些情况下，可以填写商店标识符和销售点标识符。）

一旦接收到加密传送对象，系统如同前面所述的那样操作，只是具有以下的不同。一旦识别出商家标识符对应于某个卫生保健设施并且交易类型数据对应于数据获取交易，将第三解密模块旁路，因为三级数据是空。然后，软件系统存取数据库 706 以获得控制存取与商家标识符结合的数据

的规则。例如，数据库 706 可以包含将每个商家标识符、主账户、和卡标识符与回答数据获取交易而返回的持卡人数据相联系的表。然后，软件系统执行规则，将允许返回的数据返回到被给出了这些规则的卫生保健设施。因此，这里所述的交易卡可以用于将任何种类信息提供到任何种类的组织。

为了允许上述交易，图 7 的前端模块可以提供持卡人可以登录到其中的网站。网站可以提供一个或更多的构造以允许持卡人将任何数据与他的卡结合的网页，所述任何数据包括：卫生保健数据、保险数据、俱乐部成员数据、或包括使用者规定的数据在内的任何其他数据。网站也可以提供一个或更多的构造以允许持卡人结合控制存取这些数据的规则的网页，例如，在逐个商家（逐个实体）的基础上。

参考图 2-10 说明的系统的一些特征是显著的，但是对于本发明的实践并不是必须的。例如，从图 2 可以看到，交易系统不包括任何交换执行部分，从而消除了与之有关的系统组件和财务支出。例如，与图 1 的系统比较，可以看到图 2 的系统不需要专用的网络线路或元件。因此，从交易的执行处理中消除了负责这种网络线路和元件的建立和维护的交换执行部分。因此，消除了商家通常为了提供他们的交换服务而负担的成本。但是，根据一些实施例，可以使用最小数量的网络线路和/或元件。

交易平台保持的数据库包括具有用于包含信贷限额、欺诈规则、和通常是在逐个银行或逐个协会的基础上强加的其他规则的字段的表。图 7 的软件系统包括允许持卡人和发卡银行存取数据库的前端 726。发卡银行可以经过前端模块 726 建立与给定卡号关联的规则，例如，信贷限额规则、欺诈检测规则、等等。发卡银行建立的规则与规则应用到的卡号相关联地存储在数据库 706 中。因此，交易平台的服务器不需要为了每个建议的交易而与发卡银行的信息系统通信以便拒绝或核准交易。作为替代，交易平台的服务器可以在一个周期中独立地核准一个或更多的交易之后，周期性地更新发卡银行的信息系统（例如，在每日的基础上）。

一个也是显著的，但对于本发明的实践并非是必须的特征是，数据库 706 可以包含将卡标识符与银行标识符相联系的表。银行标识符指示对应于给定的卡的金融机构的身份。通过简单地改变上述表中的银行标识符，

---

可以改变与一个给定卡相关联的银行。因此，持卡人可以有效地将他的余额从一个银行转到另一个银行，而不必改变信用卡（交易平台简单地改变银行标识符）。

同样地，数据库 706 可以包括将卡类型标识符与卡标识符结合的表。卡类型标识符标识卡支持的财务交易的种类。也就是说，卡类型标识符指示卡是信用卡还是签账卡、储值卡、卫生保健管理卡、其他形式的卡、或上述卡中的一些或全部的组合。因此，例如，一个单一的交易卡在一种情况下可以用作信用卡，在另一种情况下可以用作签账卡。提到的另一个方式是，数据库模型提供了一种机构，通过这种机构将存储在卡的存储介质上并且输入到数据库 706 中的卡号与卡标识符结合；卡标识符又与标识卡支持的交易或通过卡存取的信息的种类的卡类型标识符相关联；卡类型标识符和卡标识符协同操作，联系到一组组织和填充以允许卡能够起到信用卡、签账卡、储值卡、健康信息卡、等等的作用的表。

例如，如上所述，数据库包括一组包含着足以允许卡起到信用卡作用的信息表。除了其他信息之外，这些表还包括有关卡的信贷限额的信息，与卡有关的利息规则，与卡有关的滞纳金规则，与卡有关的发卡银行的身份，允许与发卡银行的信息系统联系的地址信息（例如，IP 地址，端口信息，物理地址，等等），和类似信息。通过使用卡标识符，可以将这些表中的数据与给定的卡相关联，即，在这些表中可以将卡标识符用作密钥。

第二组表允许卡起到签账卡的作用。除了其他信息之外，这些表还包括，有关与卡关联的账户的支票存款账户号和路由号码的信息，支票存款账户的余额、以及诸如此类的信息。也能通过卡标识符的使用将这些表中的数据与给定的卡相关联，即，可以将卡标识符在这些表中用作密钥。

第三组表允许卡起到储值卡的作用。储值卡是一种提供对预付货物或服务的存取的卡（例如，预付电话呼叫卡，赠券卡，等等）。除了其他信息之外，这些表包括有关可用余额的信息，可以花费余额的商店，有关余额花费的任何限制的规则，以及诸如此类的信息。也能通过卡标识符的使用将这些表中的数据与给定卡相关联，即，可以将卡标识符在这些表中用作密钥。

再一组表允许卡起到健康记录存取空的作用。健康记录存取卡是一种

允许存取存储在诸如图 7 的数据库 706 之中的健康信息的卡。除了其他信息之外，这些表还包括有关持卡人持有的健康保险、持卡人持有的牙齿保险、持卡人的生命统计、持卡人服用的药物、持卡人的过敏性、持卡人接受过的外科手术的信息，有关持卡人的医生和其他卫生保健提供者的信息，个人健康记录，电子医疗记录，支付裁决，共同支付计算和结算，以及诸如此类的信息。也可以通过卡标识符的使用将这些表中的数据与给定的卡相关联，即，可以将卡标识符在这些表中作为密钥使用。

如参考图 3 讨论的，前面已经说明过了申请人持有的激活交易卡的快速销售方案。图 11 提供了一种方法，通过这种方法当前的持卡人可以代表交易平台分发交易卡，并且可以为这样做而接受奖励。希望作为交易卡的分发人的持卡人可以请求一批匿名的未转让交易卡。作为回答，交易平台给持卡人提供一批未转让的匿名卡（操作 1100）。如操作 1102 中所示，持卡人将匿名卡分发给他相信会成为持卡人的人（例如，朋友、同事，等等）。在分发之前或分发之后，在数据库 706 中将分发的卡与持卡人相关联（操作 1104）。例如，可以填写一张表以将每个分发的匿名卡的卡号与对应于卡递送到的持卡人的卡标识符结合。表也可以被填写为包括标识持卡人对其分发了未转让的卡的人（即，预期的申请人）的信息。例如，操作 1104 可以通过持卡人在前端模块 726 提供的网站进行。

在操作 1104 之后，申请过程如参考图 3 所述的那样进行。但是，如操作 1106 中所示，如果假设申请人的身份信息与操作 1104 中持卡人提供的身份信息匹配，而使得持卡人为其提供了匿名卡的人获得批准，那么把奖励点添加到分发持卡人的账户中（这防止了持卡人请求大量的未转让交易卡并且将它们中的许多留在，例如，购物中心，以期为了任何由此而来的申请而获得奖励）。除此之外，或作为奖励点的替代，可以将货币金额奖励给持卡人的账户。操作 1102 中执行的结合操作允许交易平台的服务器识别增加奖励点的适当卡。一旦申请人的卡被核准，交易平台的软件系统可以检查将未转让的卡号与接收并分发卡的持卡人的卡标识符相联系的表，以便确定刚刚核准的卡的卡号是否与这个持卡人的卡标识符结合。如果它被结合，那么获得对应的卡标识符。接下来，可以存取将卡标识符与主账户相关联的表，以获得分发卡的持卡人的主账户。然后，存取将奖

---

励点余额与主账户号相联系的表，并且更新奖励点余额以反映增加的奖励点。

根据一些实施例，即使持卡人对其提供了卡的人被拒绝，也要给分发持卡人的账户提供点（操作 1108）。根据一些实施例，奖励点可以在商家指定这种用途的项目上花费，或可以用于一般的奖励程序。如果对持卡人的账户奖励货币金额，那么货币金额可以花费在任何货物或服务上。

如参考图 6 讨论的，交易系统的一些实施例考虑到了说明给定交易的三级数据的通信。例如，假设持卡人进行了总额为\$15 的肥皂、苏打水、和纸巾的购买的交易，从图 5 的内核通信到图 7 的软件系统的信息包括将交易标识为包括\$8 价钱的肥皂、\$4 价钱的苏打水、和\$3 价钱的纸巾的\$15 总价的信息。图 7 的软件系统接收该信息，并且，如上所述，建立标识\$15 交易的交易标识符。将每个购买的项目（和与之结合的价钱）与交易标识符结合。因此，根据一些实施例，数据库 706 包含特定的商家、商店、注册、每个购买的项目、每个购买的项目的价钱、和交易的总价。这种三级数据的保存使得能够获得某些此前不可能的功能。

三级数据保存允许的功能的一个例子涉及到增强争议的解决。如果信用卡持有人检查他的或她的结算表，并相信某个特定费用太高，那么这个持卡人可以争议这个费用。继续前面的例子，假设持卡人接收到的结算表显示交易的总价是\$25，而不是\$15，那么持卡人要联系他的信用卡公司，并且陈述交易应当是总价\$15,而不是\$25。结果，整个\$25 交易将被标识为有争议的，尽管事实是只有\$25 中的\$10 存在争议，即，持卡人承认他欠款\$15，而不相信他欠款\$25。在一些情况下，必须争议整个交易，因为传统的信用卡公司不接收有关交易的内容的详细信息，而在另一些情况下，是由于传统信用卡公司使用的软件系统没有考虑到与特定项目相关的价钱的争议。响应争议，发卡银行从持卡人的余额中取消该\$25 交易（直到争议解决），并且不将用于该交易的任何资金转移到商家的银行，甚至不转移持卡人承认他的确欠的\$15。因此，商家不能接收到双方都承认欠商家的\$15，直到争议的\$10 金额得以解决。

根据图 12 的方法，与在逐个交易的基础上相反，可以在逐个项目的基础上记录争议。如图 12 中所示，可以从持查人获得关于有争议的项目

的信息（操作 1200）。例如，持卡人可以呼叫交易平台的雇员，并且说明有争议的项目。例如，持卡人可以说明日期、商家、和争议的项目。一般地讲，持卡人可以引用任何量的三级数据来唯一地标识有争议的项目。雇员利用提供的级别信息存取数据库，直到识别出特定的交易及其有争议的项目。（识别与作为交易主体的特定项目相关联的特定价钱的过程可以经过前端模块 726 提供的网站执行。例如，在登录之后，持卡人可以选择一个选项，对交易内的项目提出争议。然后，网站可以提供一系列的字段，以使持卡人能够标识要争议的特定项目。例如，网站可以提供允许持卡人看到特定时间周期内的所有交易的第一字段，例如，在给定日子发生的所有交易。作为回答，可以给使用者提供一组交易总汇表，例如，由日期、商家、和总量标识的交易列表。一个特定总汇表的选择造成显示出作为交易的主体的每个项目和与之结合的价钱的列表。为了争议某个特定价钱，持卡人可以选选该项目进行争议，并且可以在与之相关联的字段中输入争议的说明。）返回到该例子，借此经过与雇员的电话交谈输入了争议，找到有争议的项目是其组成部分的交易的交易标识符（操作 1202）。接下来，在一个或更多的表内建立记录，以便争议与标识的交易的标识的项目结合的价钱（操作 1204）。例如，记录可以争议与某个项目相关联的价钱，因为结算表反映出的项目的购买价格是与持卡人相信的真实价钱不同的价钱。该记录也可以争议与某个项目相关联的价钱，因为持卡人根本就否认购买了该项目。说明争议的记录可以包括说明有争议的项目，和持卡人争议与某个给定项目结合的价钱的理由的数据字段。把与有争议的项目结合的价钱从与卡结合的余额中删除（操作 1206），直到争议解决的时候。一旦争议解决（超过了本说明的范围，但是熟悉本领域的人员是知道的），可以将适当的货币金额加回到与卡相关联的余额中。最后，如操作 1208 中所示，可以将对于操作 1204 中建立的记录的介绍输入到解决了的争议的表中。

由三级数据的收集产生的另一个功能是可以完成的帐单结算表的详细程度。根据一些实施例，可以将三级数据中的一些或全部包括在帐单结算表中。根据一些实施例，持卡人可以选择一定量的三级数据呈现在与他的卡结合的结算表中。例如，前端 726（图 7）可以提供允许持卡人选择

呈现在他的结算表上的细目的级别的网站。网站可以允许，例如，持卡人指示把所有可用三级数据都显示出来。在这种情况下，结算表显示出为提供在结算表中的每个交易收集的所有三级数据。网站也可以允许使用者仅选择呈现某些类型的三级数据，例如，仅呈现货物/服务的说明，或货物/服务的分类，或货物/服务的 SKU，等等。因此，结算表可以为每个交易呈现：构成每个交易的每个货物/服务的说明，构成每个交易的每个货物/服务的分类，构成每个交易的每个货物/服务的 SKU，等等。当然，网站也可以允许使用者选择不将三级数据呈现在他的结算表中，在这种情况下，结算表提供典型的交易信息（交易的商家、日期、总量）。

图 13 示出了建立一个或更多的控制子卡的规则的方法。如上所述，子卡对应于作为父卡的分账户的账户。父卡的持卡人可以为子卡建立一个或更多的规则，例如，通过登录到图 7 的软件系统的前端模块 726 提供的网站（操作 1300）。例如，根据一些实施例，网站提供用于输入登录到网站的持卡人的卡号的字段。网站还提供用于输入对应于卡号的口令和/或 PIN 的字段。持卡人输入他的卡号、口令和/或 PIN 以登录。因此，图 7 的软件系统将网站的特定使用者标识为对应于特定的卡号。作为选择，网站可以提供用于输入与持卡人结合的使用者名称的字段，和另一个用于输入口令的字段。一旦在这些字段中输入了数据，登录过程开始执行。

一旦登录，向持卡人提供与他的账户有关的选项的菜单。例如，可以向持卡人提供一个菜单，以允许持卡人审查他的包括其余额在内的结算表的实时显示，审查有关又是与他的卡号联系的任何账户的最近的交易，审查和/或输入诸如医疗信息、保险信息之类的与他的卡号联系的信息，设置个人化的欺诈规则以控制他的卡号，设置规则以不时地自动改变他的 PIN，和/或设置控制对应于他的父卡的子账户的规则。如操作 1302 中所示，持卡人选择一个选项，以设置控制子账户的规则。响应这个选择，如操作 1304 中所示，网站显示与操作 1300 中输入的父卡号对应于的子卡号的列表。例如，图 7 的软件系统检查数据库 706 中直接或间接将子卡号与父卡号相关联的特定表。与操作 1300 过程中输入的父卡号结合的所有子卡号被标识和显示出来。根据一些实施例，与子卡结合的持卡人的姓名也被显示出来。然后，父卡持卡人从列表中选择一个卡号（操作 1306）。

接下来，网站提供用于定制可以应用到子卡的规则的字段。例如，网站可以提供允许父亲将一个规则与子账户相关联的字段，以允许子账户在每个选择的时间单元负债选定水平的债务（例如，每月\$250）。其他规则包括，但不限于：(1) 不允许购买某些 SKU，或 SKU 的级别或种类；（例如：不允许指示购买的项目是酒类的 SKU 的购买）；(2) 不允许发生在某些商家、商家类型、和/或商家种类的购买；和/或 (3) 仅允许发生在某些商家的购买。持卡人选择应用到子卡的规则，并输入有关的规则数据（例如，如果持卡人希望限制子卡到每月\$250 的限额，那么将“250”输入到花费限额字段中，和把“月”输入到时间单位字段中，例如，可以从频率下拉菜单中选择）（操作 1310）。最后，如操作 1312 中所示，把在操作 1310 过程中选择的规则与子卡相关联。

如参考图 13 说明的，持卡人可以选择要指派给他的卡和/或子卡的欺诈触发器。如同建立子卡的规则的情况一样，欺诈触发器可以，例如，通过登录到图 7 的软件系统的前端模块 726 提供的网站建立（操作 1400，图 14）。如刚刚说明过的，根据一些实施例，网站提供用于输入登录到网站的持卡人的卡号的字段。网站也提供用于输入对应于卡号的使用者姓名、口令、和/或 PIN 的字段。持卡人输入他的卡号、口令和/或 PIN 以登录。从而，图 7 的软件系统将网站的特定使用者标识为对应于某个特定卡号。

如参考图 13 讨论的，在登录之后，使用者选择允许定制欺诈触发器的选项。然后，网站通过给持卡人提供可以应用到卡的各种种类的欺诈触发器做出回答（操作 1402）。例如，如方框 1404 中所示，网站可以给持卡人提供一组允许数据的输入的字段，以指定下列情况：(1) 每单元时间可以花费的最大货币数，超过限额的任何花销被假设为欺骗性的，例如，一天超过\$5000 的花销被假定为欺骗性的；(2) 每单笔交易的最大购买价格，超过最大购买价格的任何花销被假定是欺骗性的，例如，超过\$5000 的任何花销被假设为欺骗性的；(3) 被假设为欺骗性的特定级别的产品，例如，包括具有指示打算购买珠宝类产品的 SKU 的三级数据的交易被假设为欺骗性的；(4) 花销超过给定百分比的增长，例如，图 7 的软件系统可以跟踪过去 N 天 (N=30, 60, 90, 等等) 中一个特定持卡人的花费，并且可以计算每天的中等或平均花费量，一天中的花费超过平均和/或中等花销某

一个选定百分比被假设为是欺骗性的；（5）可以指定商家的种类，例如，在珠宝店的任何购买被假设为欺骗性的；（6）可以指定特定的商家，例如，具有对应于某个选定商家的商家标识符的任何交易被假设为欺骗性的；（7）可以指定特定的货物或服务，例如，包括具有对应于某个选定货物和/或服务的 SKU 的三级数据的任何交易被假设为欺骗性的；（8）可以指定地理范围，例如，具有指示商店位于某个给定区域（州、国家、大陆、等等）的三级数据的任何交易被假设为欺骗性的。

持卡人可以将数据输入到任何对应于他希望应用到卡的欺诈规则的字段中（操作 1406）。例如，为了建立超过\$5000 的花费将被认为是欺骗性的，持卡人可以将“5000”输入到标签为“最大可允许花费（元）”的字段中。最后，如操作 1408 中所示，图 7 的软件系统将选择的规则与操作 1400 过程中输入的卡号结合。

也如参考图 13 说明的，持卡人可以选择修改与他的卡相关联的 PIN 的方案。如参考图 13 和 14 说明的，持卡人可以通过登录到网站开始 PIN 修改方案的选择（操作 1500）。借此，图 7 的软件系统将网站的特定使用者标识为对应于特定的卡号。

如参考图 13 和 14 所述的，在登录之后，使用者选择一个选项，以允许与他的卡相关联的 PIN 的自动修改。然后，网站通过向持卡人提供可以应用到卡的各种修改方案作出回答（操作 1502）。例如，如方框 1504 中所示，网站可以给持卡人提供一组允许数据的输入的字段，以指定：（1）每个选择的时间单元递增 PIN 的选定的量，例如，每个星期给 PIN 递增 5 的量；（2）每个选择的时间单元递减 PIN 的选定的量，例如，每个星期给 PIN 递减 5 的量；（3）一组选定的 PIN，它们中的每个在选定的时间周期中是有效的，例如，选定的一组 5 个 PIN，组中第一 PIN 在一个星期中有效，组中的第二 PIN 在下一个星期中有效，等等；（4）在每个时间单元对 PIN 执行循环右移操作的选项，例如，在一个星期之后 PIN 4305 成为 5430，在下一个星期之后 PIN 成为 0543，等等；（5）在每个时间单元对 PIN 执行循环左移操作的选项，例如，在一个星期之后 PIN 4305 成为 3054，在下一个星期之后成为 0543，等等；（6）PIN 有效的时间周期的选择，在这个时间过去之后，随机选择一个新的 PIN，例如，每个星期随机选择一个

新的 PIN（持卡人可以登录到网站以便获悉新的 PIN，或可以呼叫一个电话号码并经过交互式声音识别获悉新的 PIN 号码，和/或将 PIN 邮寄给他，例如）；（7）在一个选定的时间周期过去之后用选定的量乘 PIN，例如，每天将 PIN 乘以 2；（8）个选定的时间周期过去之后用选定的量除 PIN，例如，每天将 PIN 除以 2；和/或（9）选择要附加到或预先附加到根据包括上述算法在内的任何算法改变的 PIN 的动态部分的 PIN 的静态部分，例如，一个静态部分 12345，将一个动态部分 99 附加到它，产生一个 1234599 的 PIN，如果选择通过递增 1 改变动态部分，它可以改变成为 12345100。在对 PIN 执行数学运算的情况下，例如，将 PIN 乘以选定的量 N，应该理解，可以将产生的量进行截短或其他操作，以达到适当的数字数量的数。但是应当注意，根据一些实施例，PIN 不是规定的长度，而可以是预定范围内任何长度的，例如，在 4 到 56 个数字之间。此外，在对 PIN 进行数学运算的情况下，例如，将 PIN 除以选定的量 N，应当理解，可以将得到的量四舍五入到最接近的数，或进行其他操作，以获得整数量。

持卡人可以将数据输入到对应于他希望应用到卡的 PIN 修改方案的任何字段（操作 1506）。例如，为了建立每个星期使与他的卡结合的 PIN 递增 5，持卡人可以将“5”输入到标签为“PIN 递增的量”的字段中，并且将“每星期”输入到标签为“递增 PIN 的周期”的字段中。最后，如操作 1508 中所示，图 7 的软件系统将选择的规则与操作 1500 过程中输入的卡号结合。

根据另一个实施例，图 7 的软件系统可以支持仅用一次的 PIN 的选择。例如，持卡人可以选择总是与他的卡号相关联的 PIN（如上所述，利用前端模块 726 提供的网站）。除此之外，持卡人可以选择只能使用一次的 PIN（如上所述，也是通过使用前端模块 726 提供的网站）。在执行交易的情况下，当图 7 的软件系统接收到如图 6 中所示的加密传送对象时，第三解密模块 712 可以最初尝试利用“普通”PIN 为它解密，如参考图 7 所述的那样。假设解密失败，那么第三解密模块 712 尝试用与卡号结合的“一次性”PIN 解密。如果成功，那么如上所述地进行交易，并且禁止该一次性 PIN 将来使用。一次性 PIN 可以在持卡人对把他的“普通”PIN 提供给商家犹豫不决的情况下使用，例如，当持卡人可能正在使用某个不熟悉的电

子商务网站时，或当他相信他的 PIN 的输入可能被看到时。由于该 PIN 仅能使用一次，所以 PIN 的输入是否被网站看到或获得都没有关系。

根据本发明的另一个实施例，如参考图 16A 和 16B 说明的，上述交易方案可以用于允许货物在商家之间的退货。例如，图 16A 示出了典型的在线购买安排，借此，持卡人 1600 从在线商家 1602 订购了某个项目。持卡人 1600 从在线商家 1602 接收到该项目（操作 1601）。作为回答，发卡银行 1604 将项目价格发送到在线商家的银行（操作 1603）。然后，在开票周期到期时，持卡人 1600 将等于项目价格的货币金额支付给银行 1604（操作 1605）。

图 16B 示出了货物的商家间退货安排的例子。经由图 16B 的安排，持卡人 1600 将该项目退还到一个具体的（brick-and-mortar）商家 1606（操作 1607）。在退货时，持卡人 1600 将他的收据提供给该具体的商家 1606，该具体的商家利用上面的信息向交易平台指出，要在该具体的商店 1606 处理特定的持卡人从某个特定商家购买的特定货物的退货。利用上述信息，交易平台存取一个规则数据库，以确定要从该具体的商家转移到在线商家的货币金额。然后，交易平台的服务器启动从该具体的商家的银行到在线商家的银行的、等于确定的货币金额的资金的转移（操作 1609）。上述基于规则的金额可以是预先由各个商家谈妥的，并且可以是要交换的特定货物，或要交换的货物级别的函数，并且可以额外地是商家间交换中涉及的两个特定商家的函数。

然后，在线商家 1602 将等于项目的价格的货币金额转移到发卡银行 1604（操作 1611），发卡银行 1604 将等于该项目的价格的货币金额归还到持卡人的账户（操作 1613）。因此，持卡人 1600 能够自由地与一个商家（例如，在线商家 1602）进行购买，并且将货物退货给第二个商家（例如，该 brick-and-mortar 商家 1606）。由于在特定货物或货物级别的交换的事件中，把要从一个商家转移另一个商家的一致同意的金额存储在与交易平台有关系的数据库中，从而使得这种退货安排成为可能。

图 17 示出了持卡人之间的资金无线交换的方案。方案涉及到在蜂窝电话内的处理器上运行的 Java 程序。Java 程序包括提示模块 1700，该提示模块 1700 要求持卡人输入如下：（1）他或她希望转移到另一个持卡人

的货币量；(2) 持卡人的 PIN 代码；和 (3) 接受方的蜂窝电话号码。将上述数据集合成一个数据集，并且通过加密单元 1702 加密，加密单元 1702 可以根据上述原理操作。然后，经过图 7 的 SSL 因特网连接交易平台，通信该加密的数据集。

在前端，提取启动交易的电话号码，并且用于查询将持卡人电话号码与 PIN 代码结合的数据库 1704。因此将对应 PIN 代码返回到模块 1706，并且提供到解密模块 1708，解密模块 1708 利用 PIN 代码作为解密密钥。

然后，检验对应于 PIN 的账户中的资金的可用性。根据一个实施例，可以将 PIN 或电话号码用于存取将卡身份号码联系到 PIN 或电话号码的数据库 1710。然后，将检索到的卡身份代码发送到资金检验模块 1712，资金检验模块 1712 确定与 PIN/电话号码对应的账户是否具有足够的资金以允许建议的交换。如果是这样，那么执行交换，并且通过模块 1714 将 SMS 发送到接受方的电话号码，将资金交换的信息通知他或她。

也可以经过从前端模块 726 提供的网站，在线进行资金的个人对个人的交换，进行的过程一般与参考图 17 说明的相同。

图 18 示出了上述个人对个人交易的示例实施例。如图 18 中所示，交易平台 1800 通过两个银行 1802 和 1804 中的每一个提供对货币资金（信贷限额，借方余额账户，支票存款账户，储蓄账户，储值账户，和/或预付账户）的存取。原则上，平台 1800 可以通过任何数量的银行提供对资金的存取。为了说明，参考从信用卡的转移说明资金的个人到个人转移。可以执行从任何类型的账户到任何类型的账户的个人到个人的资金转移。也仅是为了说明，假设交易平台处理八个当事人，他们中的每一个都拥有具有信用卡功能的交易卡。四个持卡人通过银行 1802 存取信贷额度，而其他四个持卡人通过银行 1804 存取信贷额度。因此，如图 18 中所示，每个发卡银行 1802 和 1804 为每个持卡人保持一个账户。一个这样的账户用参考号 1806 标识，而另一个这样的账户用参考号 1808 标识。

假设与信用账户 1806 结合的持卡人希望将资金转移到与账户 1808 结合的当事人，这使得与账户 1808 结合的当事人可以立即使用这个资金。交易平台将账户 1810 和 1812 保持在每个银行 1802 和 1804。在银行 1802 具有账户的所有持卡人具有存储在账户 1810 中的他们的预付账户的资金，

---

而在银行 1804 具有账户的所有持卡人具有存储在账户 1812 中的他们的预付账户的资金。平台保持着跟踪保存在预付账户 1810 和 1812 中的每个持卡人的资金份额的数据库 706。从信用账户 1806 到与信用账户 1808 结合的持卡人的转移资金被从信用账户 1806 转移到预付账户 1812，并且立即更新数据库 1706 以：(1)反映账户 1812 增加了被转移的货币金额；和(2)反映与信用账户 1808 结合的持卡人具有增加了被转移的货币金额的预付账户的份额。因此，与货币账户 1808 结合的持卡人可以立即从预付账户 1812 提取他的份额，例如，可以通过将这种购买处理为预付交易来进行货物或服务的购买，这意味着从该预付账户 1812 提取了资金，并且立即更新数据库 706 以反映这种交易。作为选择，与信用账户 1808 结合的持卡人可以规定将接收的资金转移到他的信用账户 1808，或任何其他账户。然后，例如，在数据库 706 和银行 1804 的计算机系统同步时，在这天结束时，完成这种转移，以便反映货币金额被从预付账户 1812 提取，并且存到信用账户 1808 中。

以上说明的各个实施例仅是通过举例说明的方式提供的，并且不应当被解释为对本发明的限制。熟悉本领域的人员应当知道，可以对本发明进行各种修改和改变，而不必遵循这里举例和说明的示例实施例和应用，并且不脱离后面权利要求中提出的本发明的真正精神和范围。

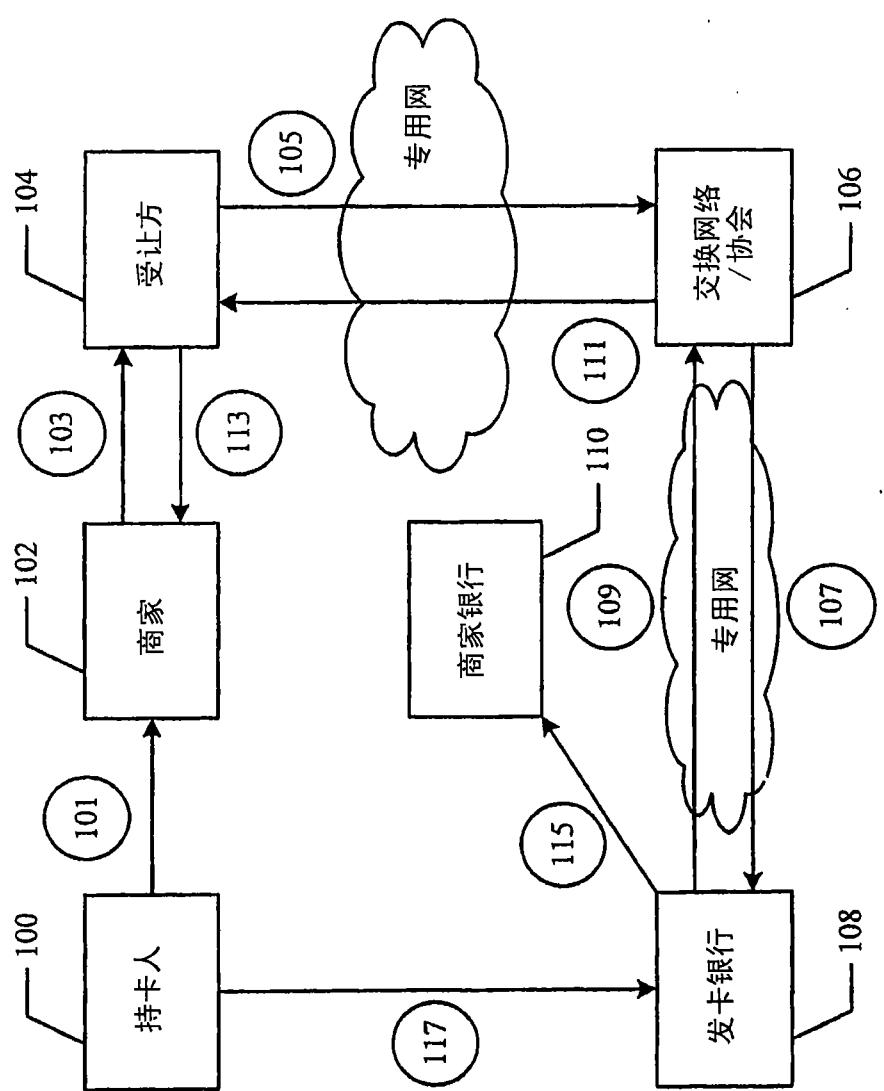


图 1

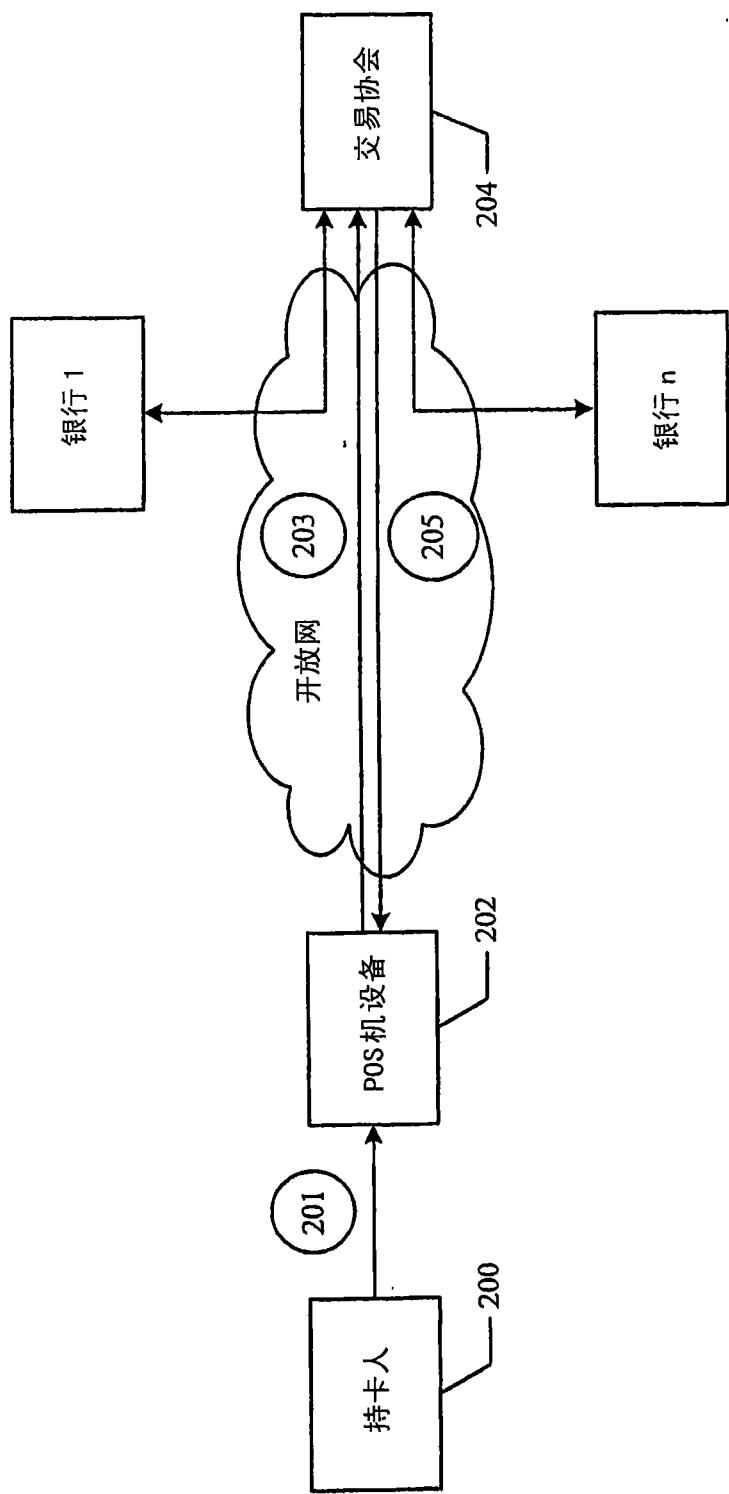


图 2

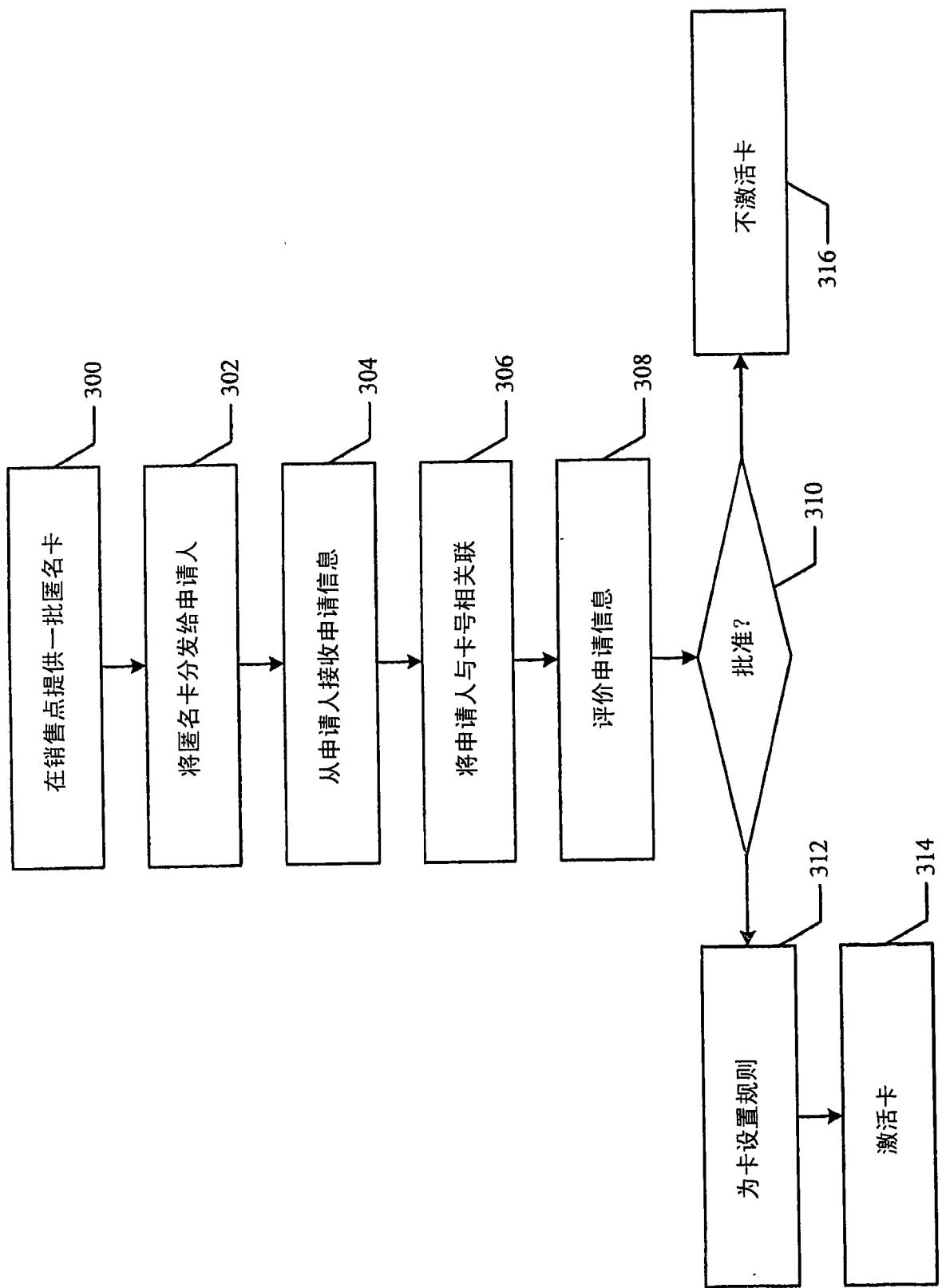


图 3

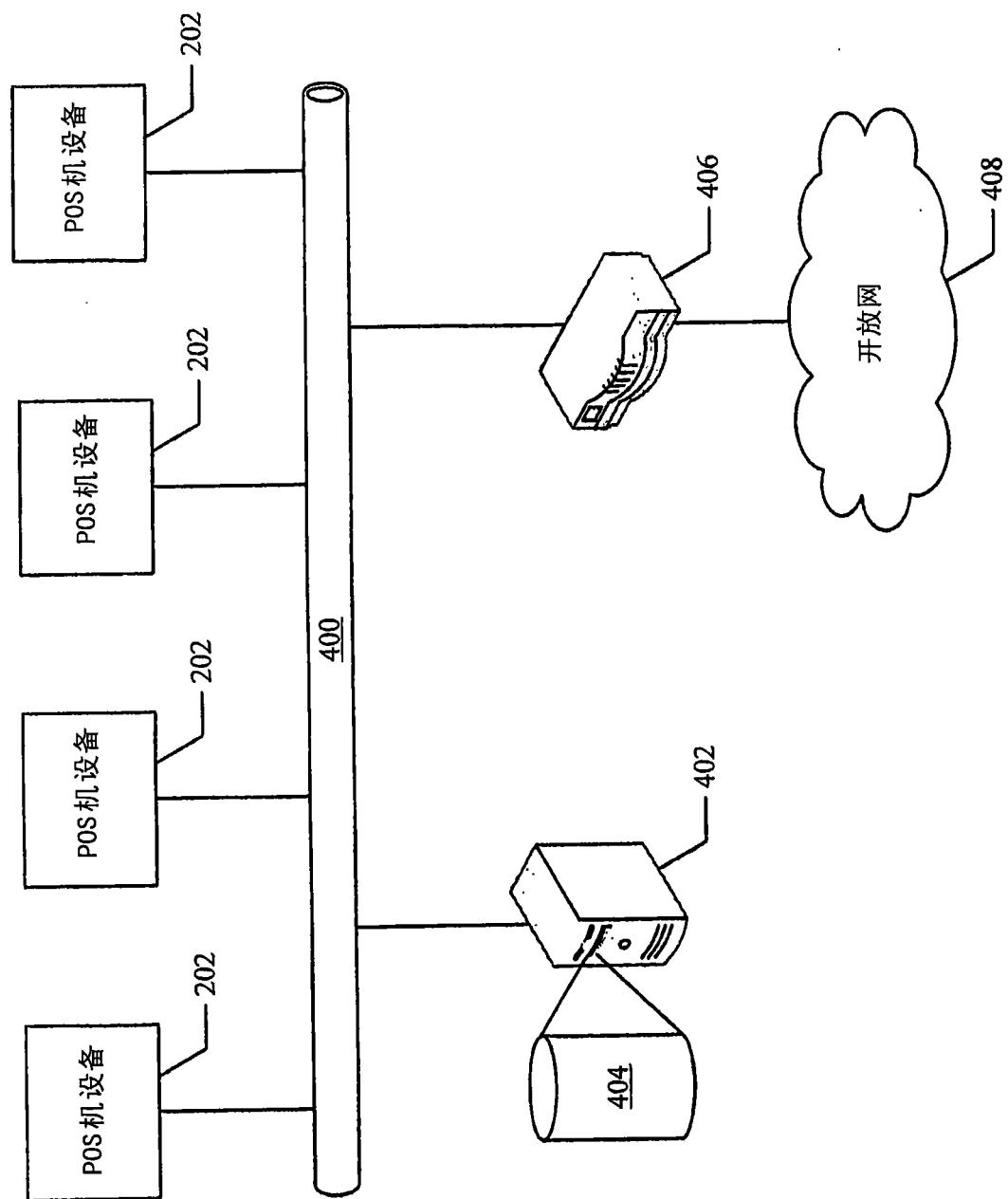


图 4

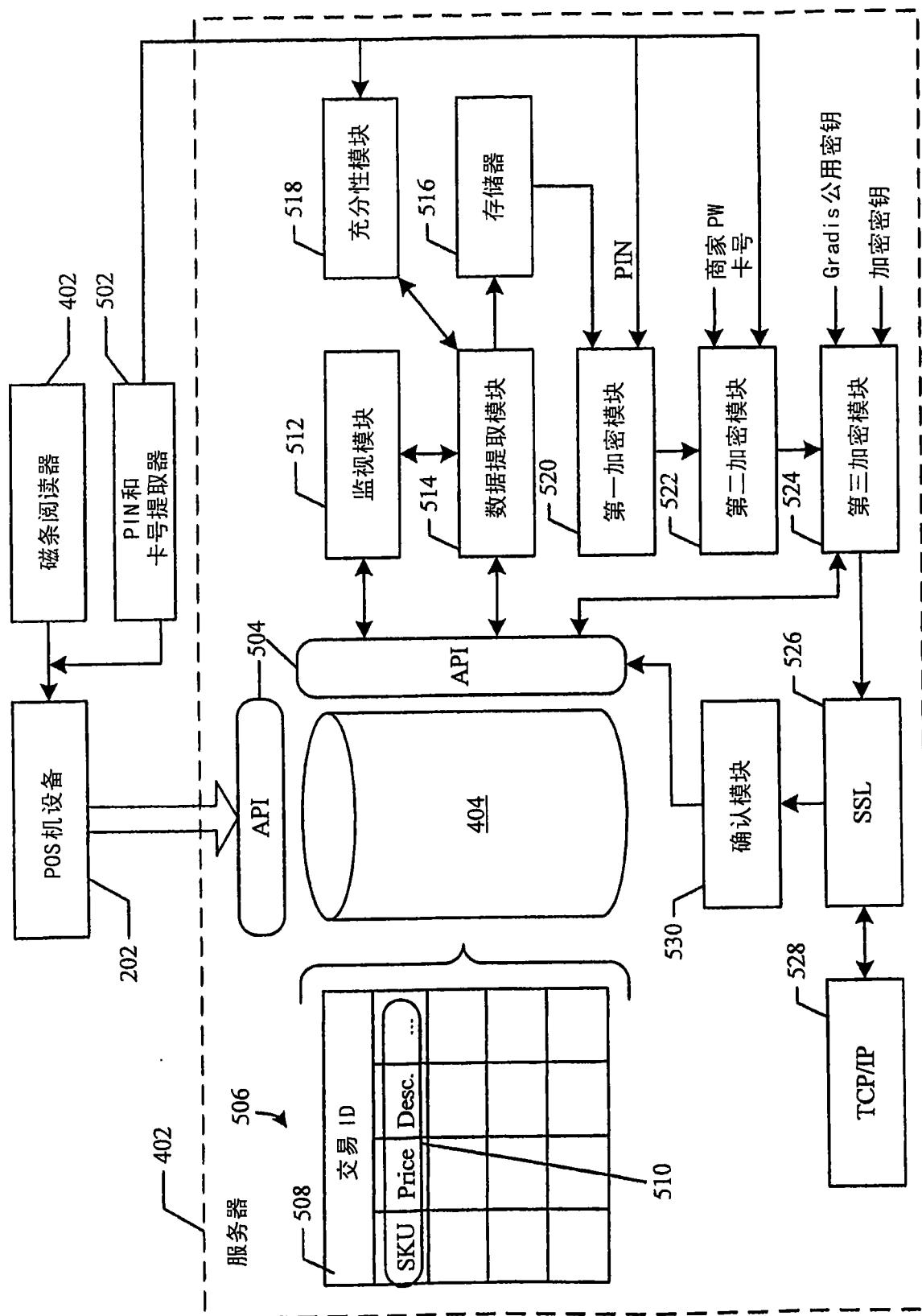


图 5

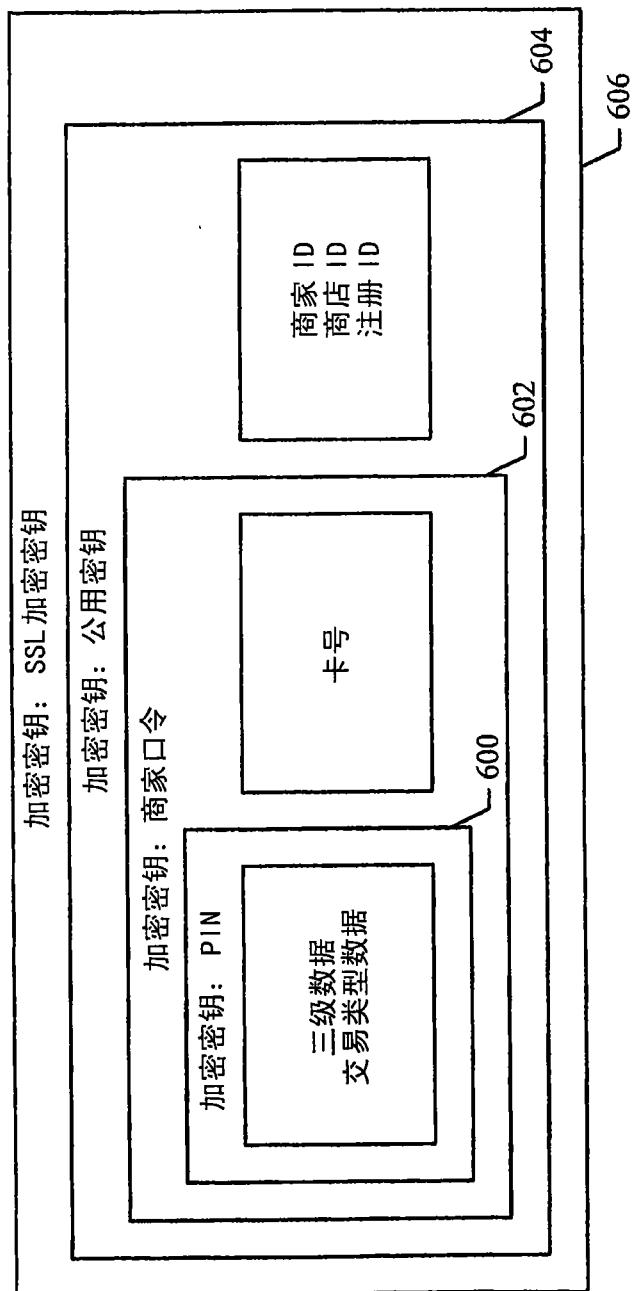


图 6

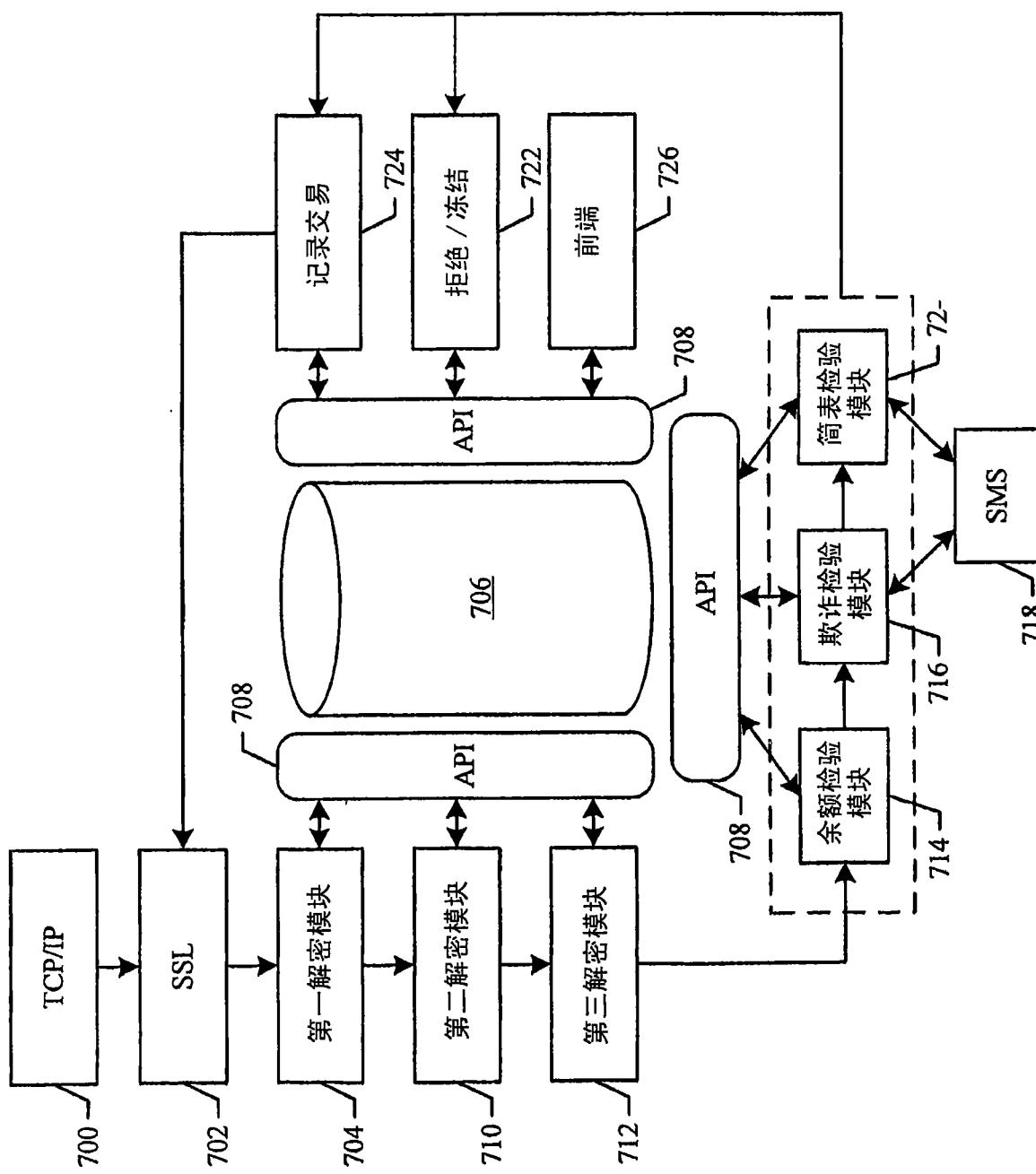


图 7

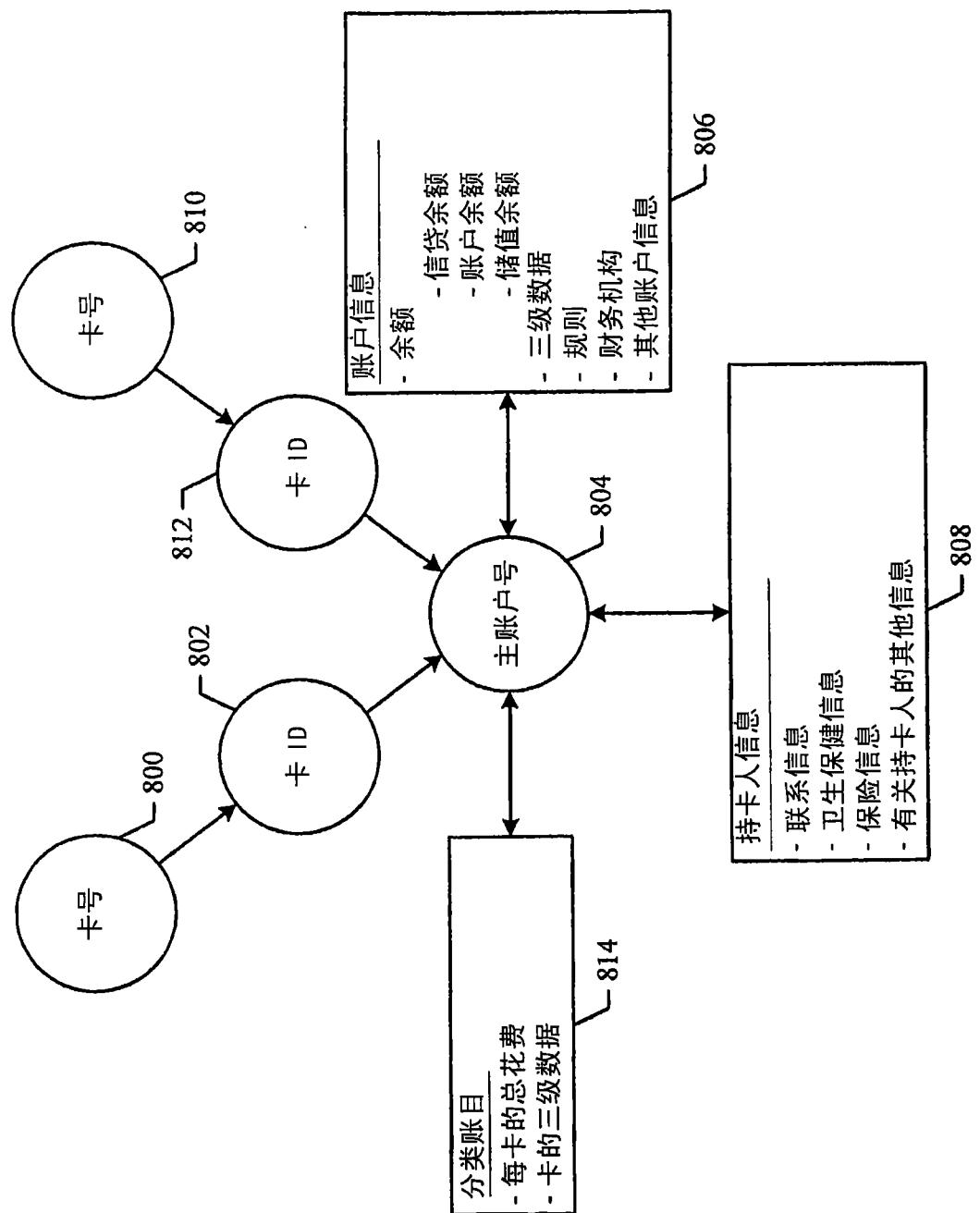


图 8

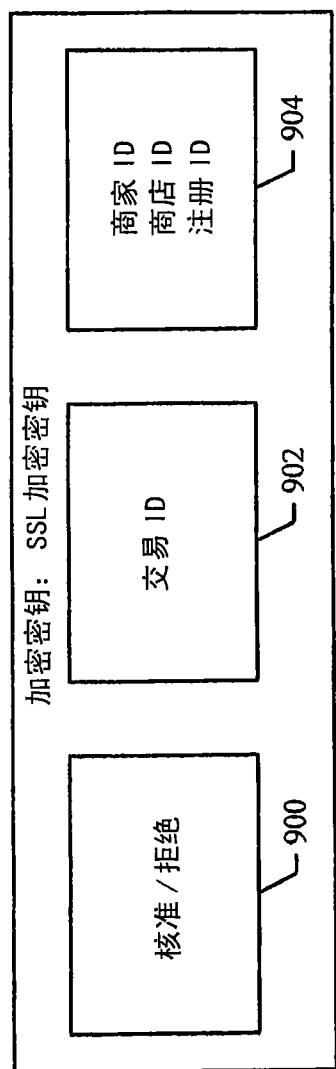


图 9

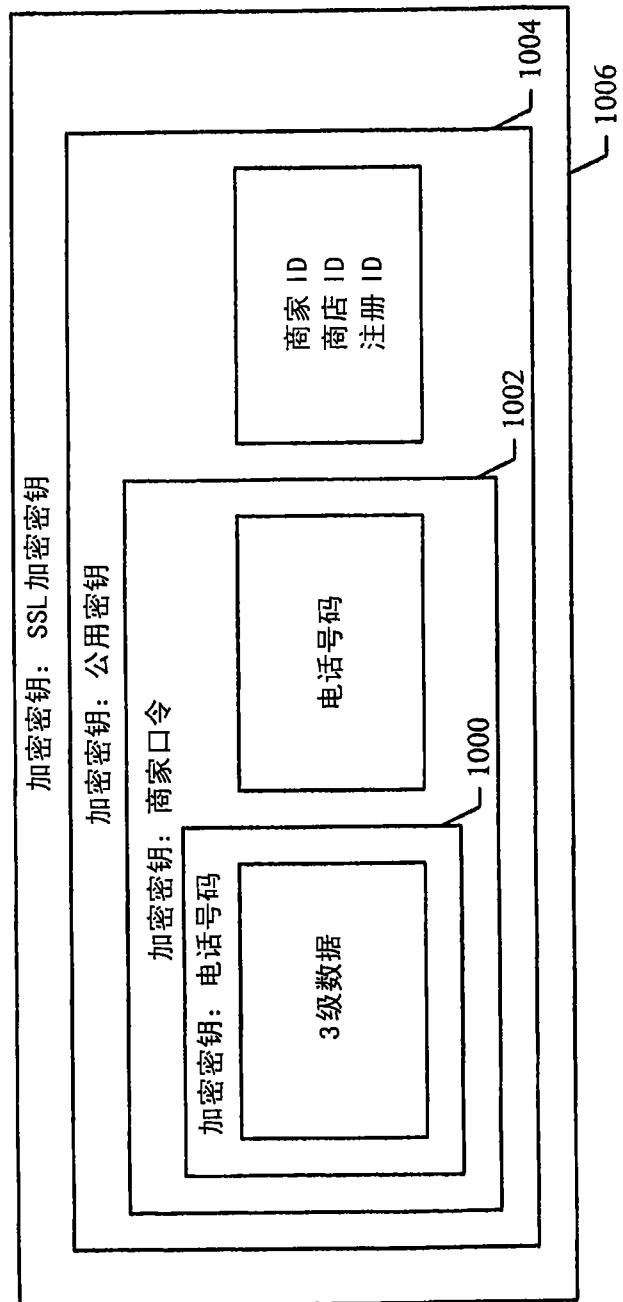


图 10

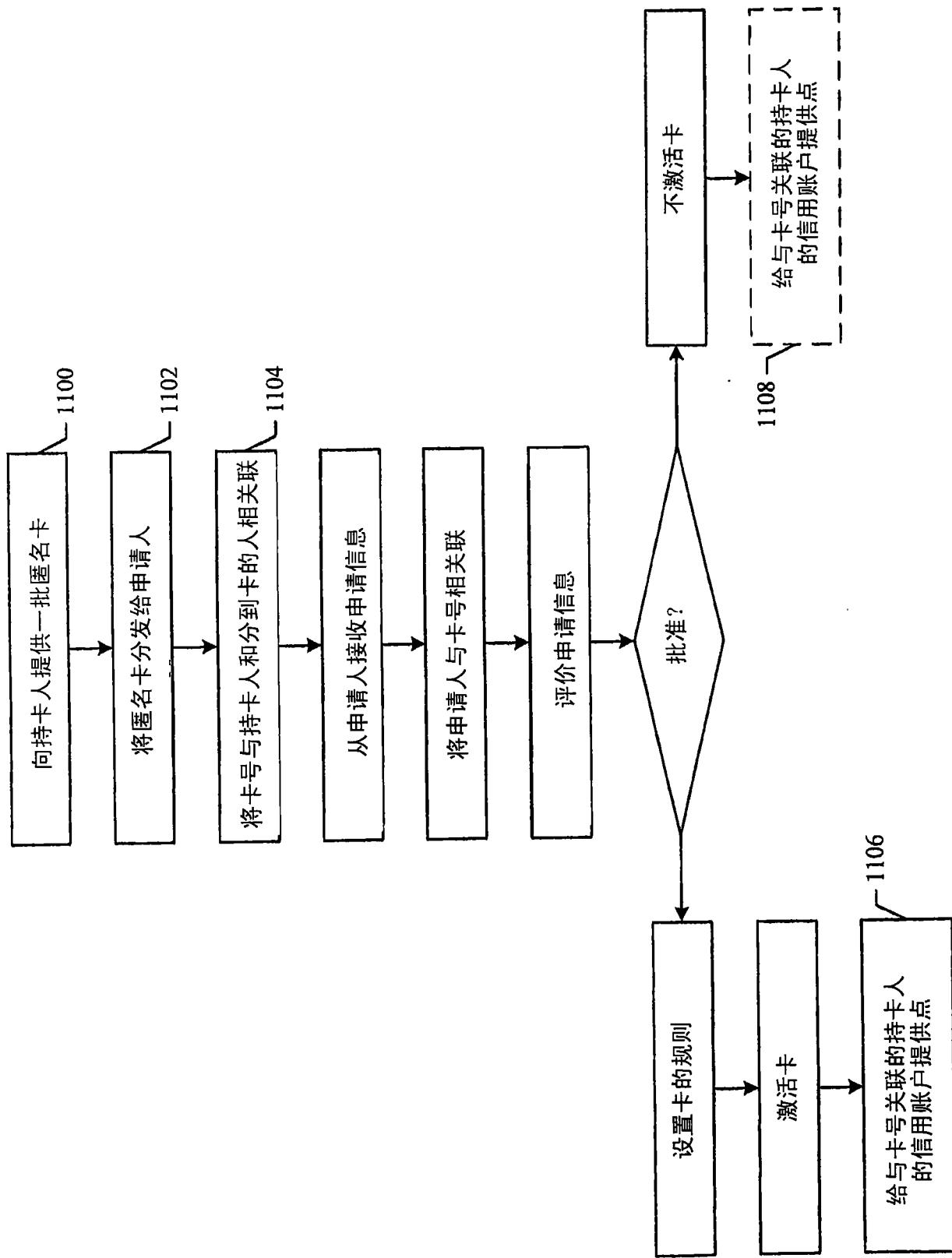


图 11

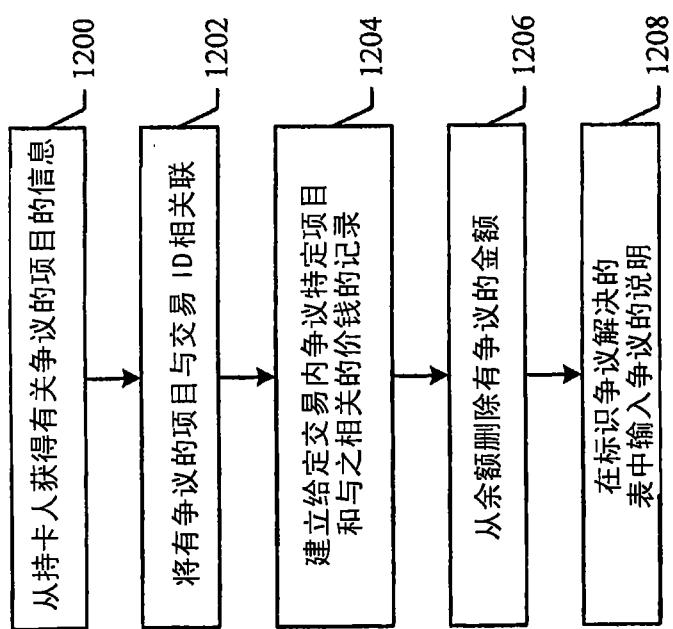


图 12

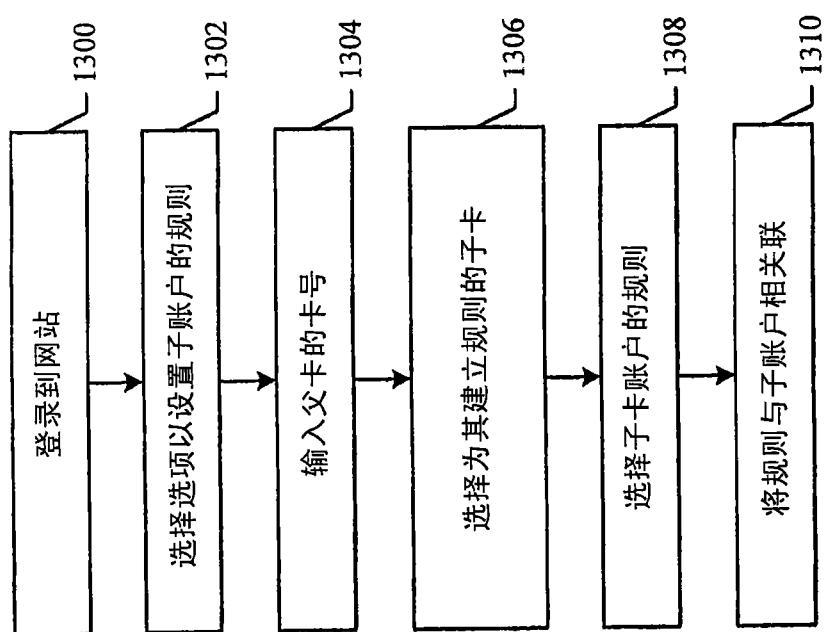


图 13

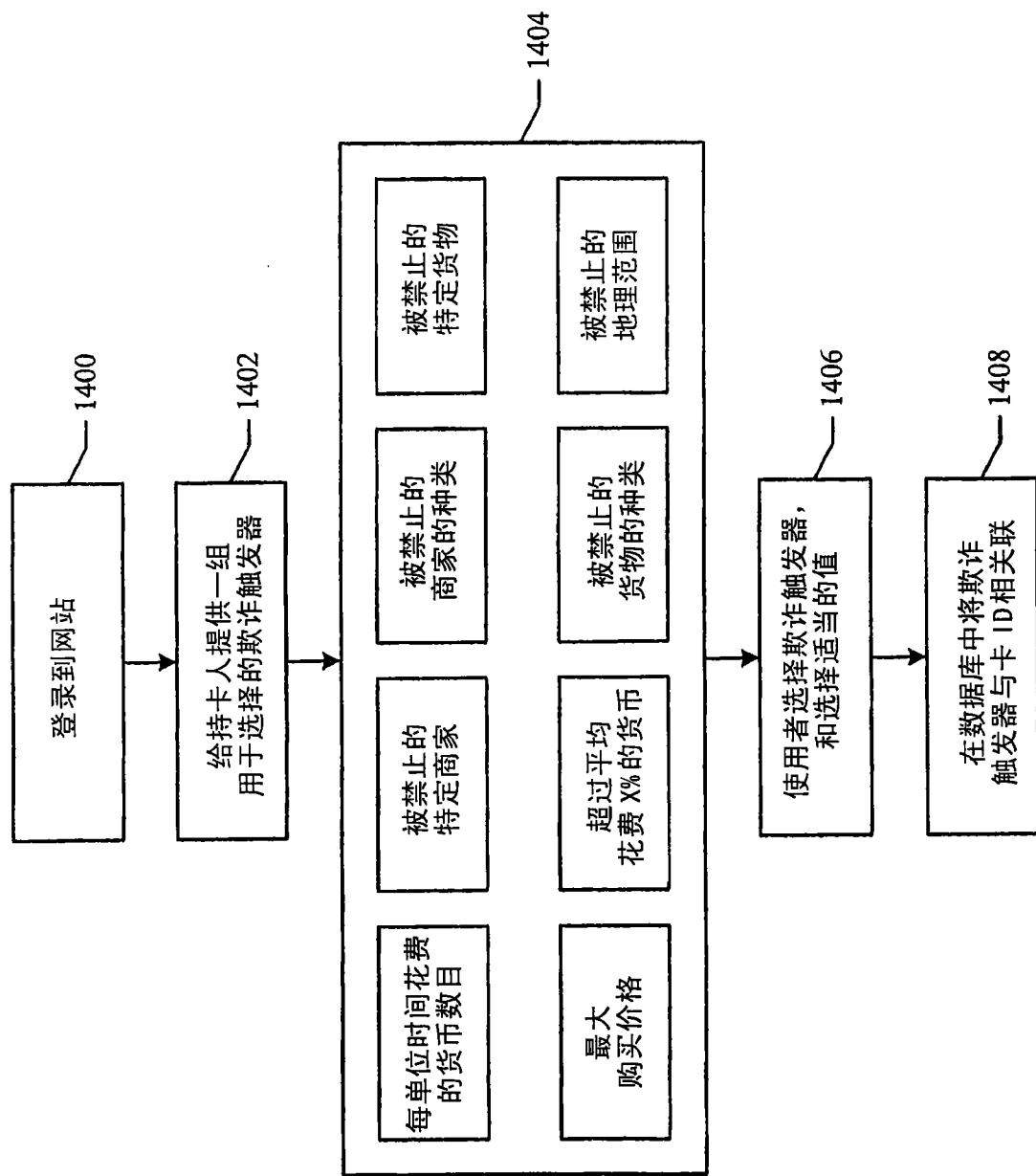
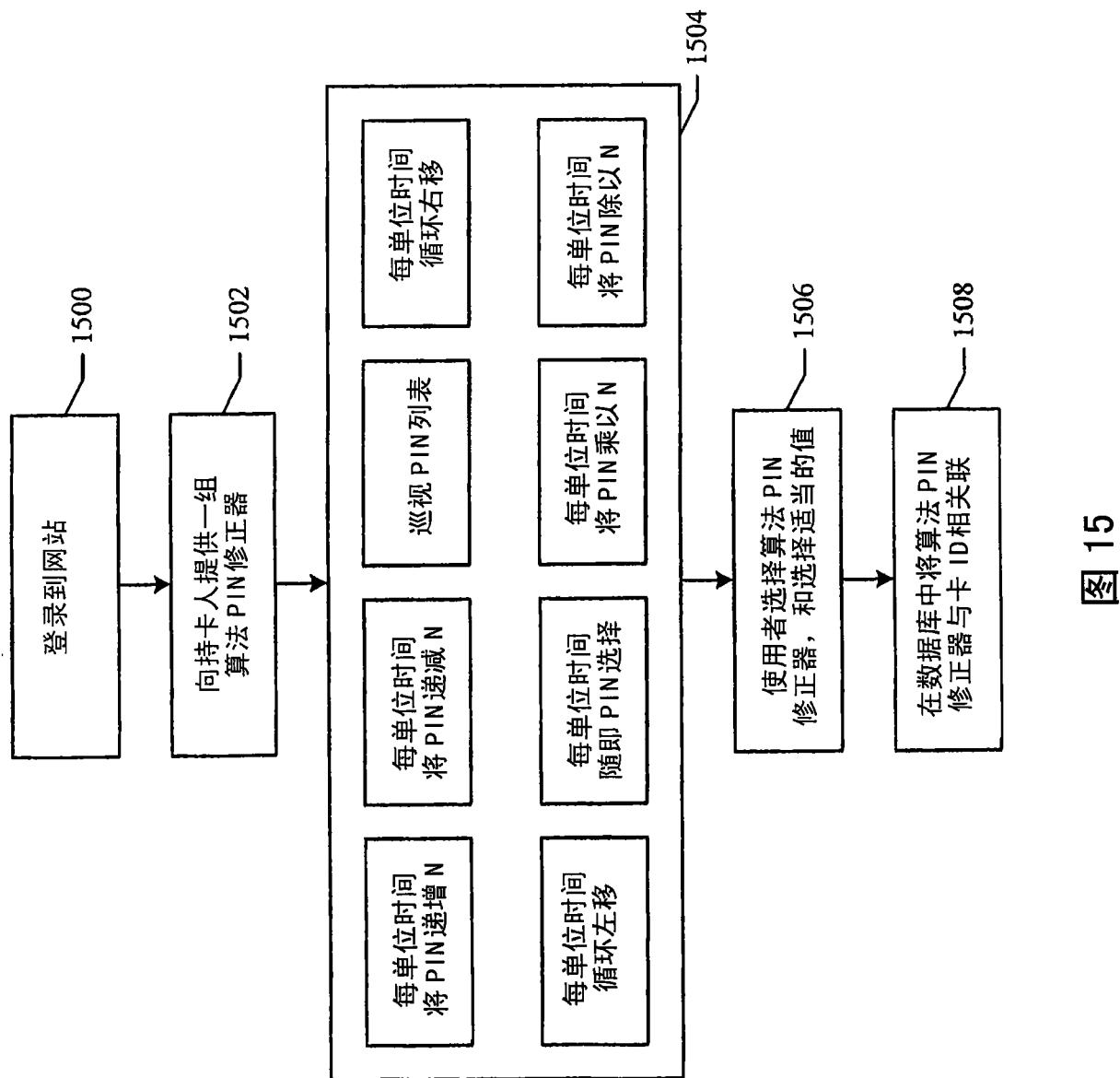


图 14



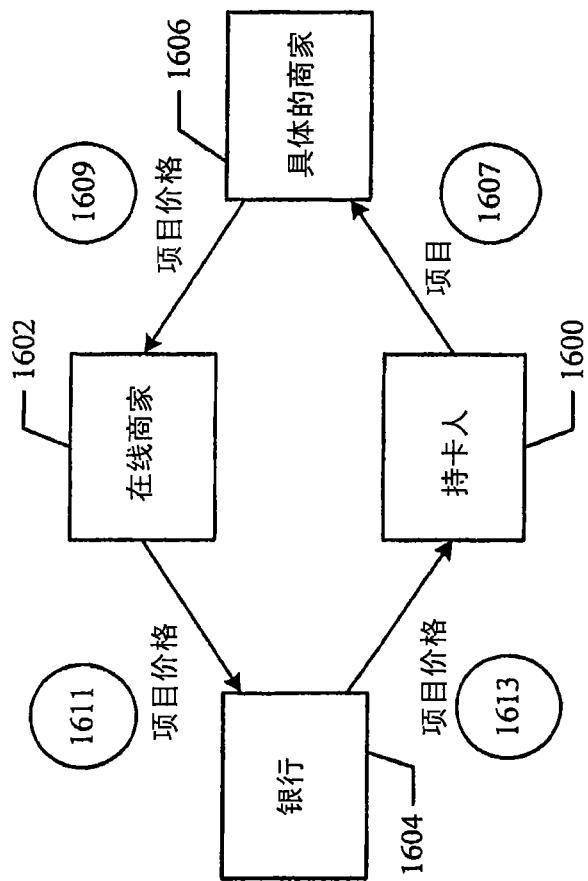


图 16 B

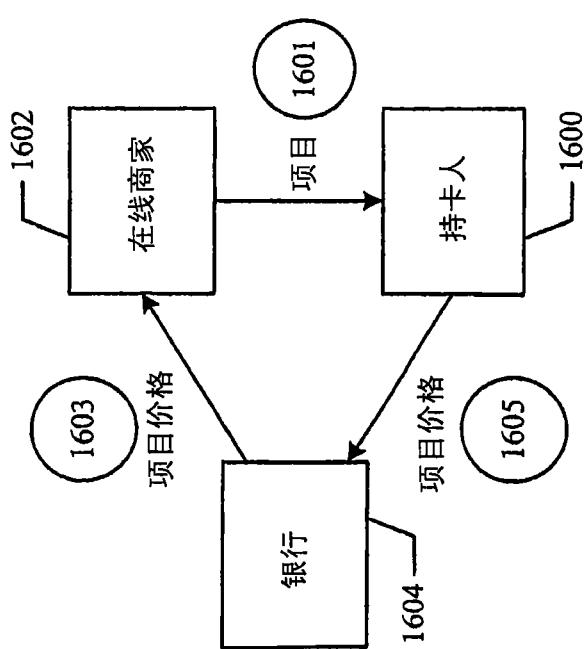


图 16 A

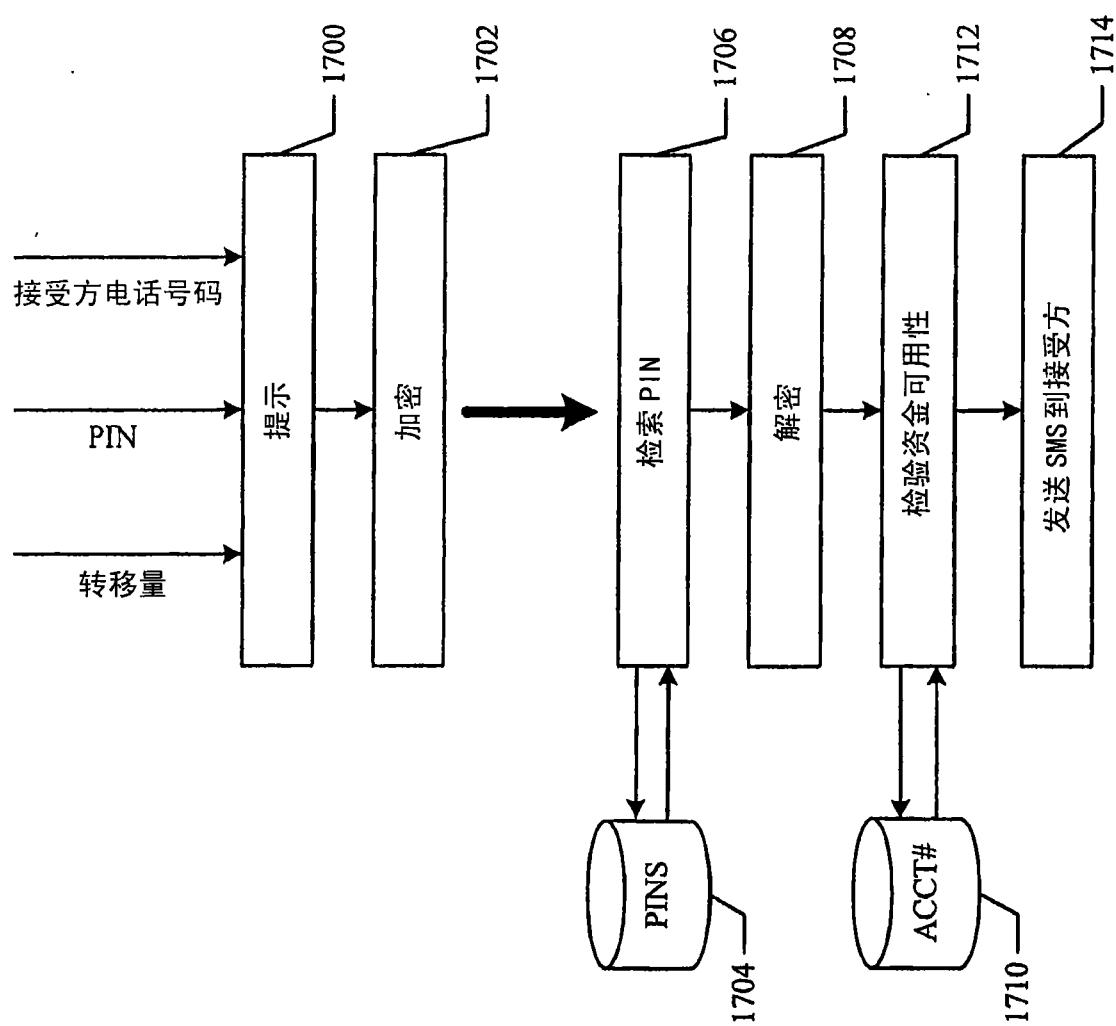


图 17

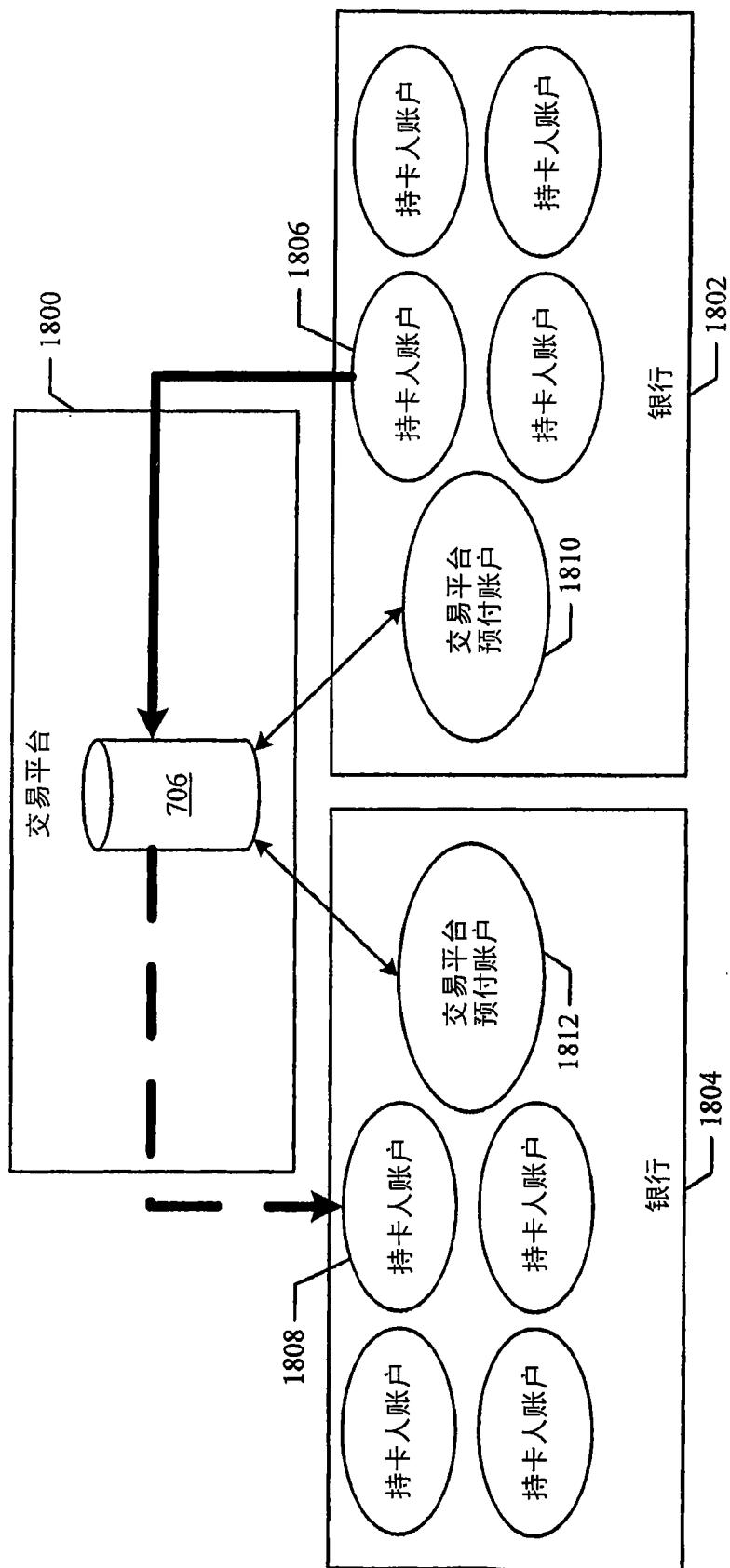


图 18