[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04M 15/00
H04M 3/38 H04M 3/36

[12]发明专利申请公开说明书

[21]申请号 99804523.3

[43]公开日 2001年5月23日

[11]公开号 CN 1296694A

[22]申请日 1999.4.5 [21]申请号 99804523.3
[30]优先权
[32]1998.4.3 [33]US [31]60/080,006
[32]1999.4.1 [33]US [31]09/283,672
[86]国际申请 PCT/US99/07441 1999.4.5
[87]国际公布 WO99/52267 英 1999.10.14
[85]进入国家阶段日期 2000.9.26
[71]申请人 朗迅科技公司
地址 美国新泽西州

[72]发明人 杰拉尔德·D·鲍利尔
迈克尔·H·卡希尔
弗吉尼亚·K·费拉拉
黛安娜·兰伯

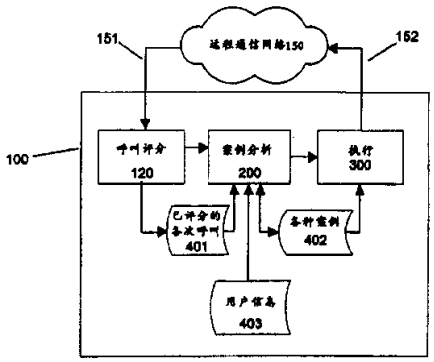
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 杨国旭

权利要求书5页 说明书17页 附图页数9页

[54]发明名称 在基于交易的网络中对欺诈行为的自动管理

[57]摘要

通过自动地产生用于管理欺诈行为的各项建议,以响应可疑的 欺诈活动,并且通过导出各项建议,作为欺诈活动的被选定的各种 属性的一个函数。更具体地说,一个可编程的规则引擎被用来自动 地产生各项建议,以便在逐次呼叫地对欺诈行为进行评分的基础上 产生各项建议,使得各项建议直接地对应于可疑的欺诈活动的类型 和数额。以远程通信欺诈为例,一个欺诈行为自动管理系统接收先 前已被评分的各项呼叫详细记录,以便识别可能的欺诈呼叫。根据 一个个别用户的已学习的行为以及一个欺诈作案者的已学习的行 为,欺诈评分方法对每一次呼叫的欺诈概率进行评估。评分方法还 提供针对该呼叫的呼叫详细记录中的各种要素对欺诈行为分数的贡 献的一种表示。一次案例分析被启动,并且根据欺诈行为分数将先 前已评分的各项呼叫详细记录划分为无害组与可疑组。根据已选定 的各变量以及针对其各次呼叫的评分来表征各个组。这些特征跟用 户信息组合在一起,以产生诸判决变量的一个集合。然后,应用一 组规则来确定各判决变量的当前集合是否符合可定义的各项条件。当符合一项条件时,就向该帐户提出与该条件有关的各项预防措 施。作为一个例子,可以经由在远程通信系统中的执行功能,自动 地实施所建议的各项预防措施。



ISSN1008-4274

00·03·25

权 利 要 求 书

1．一种用计算机实现的、在一个远程通信系统中用于管理欺诈行为的方法，包括下列步骤：

为了响应在远程通信网络中的可疑的欺诈活动，自动地产生一项或多项建议，其中各项建议都作为按照对欺诈行为的似然度而评分的各次呼叫的一个函数而被导出，并且其中各项建议对应于可疑的欺诈活动的各种属性。

2．根据权利要求1所述的用计算机实现的方法，其中，在一个逐次呼叫的基础上进行评分。

3．根据权利要求2所述的用计算机实现的方法，还包括下列各步骤：

接收各项呼叫详细记录，这些记录已经被评分，以便识别可能的欺诈活动，其中，一个已评分的呼叫详细记录提供多个预定的呼叫变量对欺诈行为分数的贡献的一种表示；以及

根据与欺诈行为分数的变化有关的预定的标准来启动一次案例分析。

4．根据权利要求3所述的用计算机实现的方法，其中启动一次案例分析的步骤包括下列各步骤：

a）根据欺诈行为分数，将多个已评分的详细记录划分为至少一个表示非可疑活动的第1组以及一个表示可疑活动的第2组；

b）根据预定的标准（各变量）以及在各组中针对个别的各次呼叫的欺诈行为分数来标识每一组；

c）根据步骤 b）以及用户信息，产生一个或多个判决变量；

d）将一条或多条规则应用于一个或多个判决变量，以确定是否满足一个预定的条件；以及

e) 当满足一个预定的条件时，建议作出符合于该条件的一项或多项已规定的对欺诈行为的响应。

5．根据权利要求 4 所述的用计算机实现的方法， 其中，一次个别呼叫的一个欺诈行为分数是对欺诈行为的似然度的一种表示，基于包括一个用户签名在内的一个用户的已学习的行为以及包括一个欺诈签名在内的欺诈呼叫活动的已学习的行为，来确定上述的似然度。

6．根据权利要求 5 所述的用计算机实现的方法，其中，一项或多项已规定的对欺诈行为的响应包括各项预防措施。

7．根据权利要求 6 所述的用计算机实现的方法，其中，预防措施之一包括实施基于执行的欺诈行为预防。

8．根据权利要求 1 所述的用计算机实现的方法，其中，各项建议还符合于合法活动的各种属性。

9．根据权利要求 8 所述的用计算机实现的方法，其中，各项建议还符合于跟一个案例有关的用户信息以及各种属性。

10．一种用计算机实现的、在一个发生各种交易的网络中用于管理欺诈行为的方法，包括下列步骤:

为了响应在网络中的可疑的欺诈活动，自动地产生一项或多项建议，其中各项建议都作为按照对欺诈行为的似然度而评分的各次交易的一个函数而被导出，并且其中各项建议对应于可疑的欺诈活动的被选定的各种属性。

11．根据权利要求 10 所述的用计算机实现的方法，还包括下列

各步骤:

接收各项交易记录，这些记录已经被评分，以便识别可能的欺诈活动，其中一个已评分的交易记录提供多个预定的交易变量对欺诈行为分数的贡献的一种表示；以及

根据与欺诈行为分数的变化有关的预定的标准来启动一次案例分析。

12．根据权利要求 11 所述的用计算机实现的方法，其中启动一次案例分析的步骤包括下列各步骤:

a）根据欺诈行为分数，将多个已评分的交易记录划分为至少一个表示非可疑活动的第 1 组以及一个表示可疑活动的第 2 组;

b）根据预定的标准（各变量）以及在各组中针对个别的各次交易的欺诈行为分数来标识每一组;

c）根据步骤 b）以及用户信息，产生一个或多个判决变量;

d）将一条或多条规则应用于一个或多个判决变量，以确定是否满足一个预定的条件；以及

e）当满足一个预定的条件时，建议作出符合于该条件的一项或多项已规定的对欺诈行为的响应。

13．根据权利要求 12 所述的用计算机实现的方法，其中，一次个别交易的一个欺诈行为分数是对欺诈行为的似然度的一种表示，基于包括一个用户签名在内的一个用户的已学习的行为以及包括一个欺诈签名在内的欺诈呼叫活动的已学习的行为，来确定上述的似然度。

14．根据权利要求 13 所述的用计算机实现的方法，其中，一项或多项已规定的对欺诈行为的响应包括各项预防措施。

15．根据权利要求 14 所述的用计算机实现的方法，其中，预防

措施之一包括在网络中实现基于执行的欺诈行为预防。

16．根据权利要求10所述的用计算机实现的方法，其中，在一个逐次交易的基础上进行评分。

17．根据权利要求10所述的用计算机实现的方法，其中，各项建议还符合于合法交易活动的各种属性。

18．根据权利要求17所述的用计算机实现的方法，其中，各项建议还符合于用户信息。

19．根据权利要求18所述的用计算机实现的方法，其中，各项建议还符合于跟一个案例有关的各种属性。

20．一个用于管理在一个发生各种交易的网络中的欺诈行为的系统，包括：

用于导出一项或多项建议的装置，上述建议作为按照对欺诈行为的似然度进行评分的各次交易的一个函数，对在网络中的可疑的欺诈活动作出响应；以及

用于自动地产生一项或多项建议的装置。

其中，各项建议均对应于可疑的欺诈活动的被选定的各种属性。

21．一个用于管理在一个发生各种交易的远程通信网络中的欺诈行为的系统，包括：

至少一个存储装置，用于接收、存储和提供各项呼叫详细记录，这些记录已经被评分，以便识别可能的欺诈活动，其中，一个已评分的呼叫详细记录提供多个预定的呼叫变量对欺诈行为分数的贡献的一种表示；以及

一个计算机处理器，它被连接到至少一个存储装置，用以执行已编程的各项指令，同时自动地产生一项或多项建议，以便对在远程通信网络中的可疑的欺诈活动作出响应，其中各项建议作为已评分的各项呼叫详细记录的一个函数而被导出，并且其中各项建议均对应于可疑的欺诈活动的被选定的各种属性。

00.09.26

说　　明　　书

在基于交易的网络中对欺诈行为的自动管理

与相关申请书的交叉参照

本申请书要求 1998 年 4 月 3 日申请的美国临时申请系列号第 60/080,006 号的权益，后者已作为参考文献被收入本文。本申请书还涉及跟本申请书同时提交的美国申请书系列号第　　号（Baulier 4-2-2-5），后者也已作为参考文献被收入本文。

技术领域

本发明一般地涉及欺诈行为管理，并且，更专门地涉及在一个例如各种通信网络以及诸如此类的基于交易的网络中，用于管理欺诈行为的一种自动方案。

发明背景

对各种通信网络的欺诈性使用是一个占有令人吃惊的比例的问题。以使用通信网络为例，据估计，因欺诈而付出的代价每年为数十亿美元，并且还在增长中。给出了巨额的财务亏损之后，远程通信企业继续寻找各种方法，以减少欺诈行为出现的次数，与此同时，还要把对合法用户的服务的损害降低到最低限度。

虽然存在多种形式的远程通信欺诈行为，但是在今天的网络中，欺诈行为的两种最流行的类型或种类就是盗用服务欺诈和订购欺诈。例如，盗用服务欺诈可能涉及各种用户卡、各种蜂窝电话，或各种电话线路（例如，各种专用小交换机线路）的合法使用，而当一个从来不打算为一次服务付费的作案者装作一个新顾客时，就会发生订购欺诈。由于在帐户中没有任何合法的呼叫活动可以被用来作为区分欺诈活动的基础，所以后一种类型的欺诈已经变得特别难以检测和预防。无论在哪一种情况下，由这些类型的欺诈所带来

的损失都是一个重要问题。

许多公司在它们的产品中夸耀自己具有超级的欺诈行为管理，然而，事实是同时考虑到服务提供商和顾客的运营和经济利益的一种综合性的欺诈管理系统并不存在。例如，大多数系统的一个共同的缺点就是，只有在一个帐户上已经出现大量的欺诈活动之后才能把欺诈行为检测出来。而且，在今天的各种系统中，所实施的许多欺诈行为预防措施对合法的顾客来说也很有破坏作用。其结果是，顾客们为了寻找一个更加安全的系统而更换服务提供商，形成一种顾客“打转转”的现象。

一般来说，现有各种系统的短处已经是很明显的，表现在为检测欺诈行为以及对它作出响应所需的时间上。例如，无论对服务提供商或者顾客来说，基于顾客从每月的帐单中给出反馈信息的欺诈行为检测不是一种可接受的方案。基于“阈值”技术的欺诈行为自动检测系统在对欺诈行为进行实时或接近实时的管理方面也不是特别有帮助的。例如，阈值方法典型地涉及按一定时间（例如，几天、几星期、几个月）积累话务量，建立各用户的轮廓图（例如，各种呼叫模式），并且使用各种阈值来识别欺诈行为。由于各合法用户也可能产生超出各种阈值的使用，以及在检测和预防之前可能出现的欺诈次数很多，使得这些系统不被认为特别有效（参见例如，美国专利第 5, 706, 338 号，“实时通信欺诈行为监测系统”以及美国专利第 5, 627, 886 号，“使用实时网络监测方法的用于检测欺诈性的网络使用模式的系统与方法”）。

虽然通过使用诸如神经网络、统计分析、基于存储的推理、各种遗传算法，以及其他数据挖掘技术等项技术可以使检测欺诈行为的速度有所改进，但是光改进对欺诈行为的检测并不能完全地解决这个问题。特别是，在一种检测欺诈行为的尝试中，即使纳入了这些技术的各种系统可以在接近实时的基础上接收和处理个别的呼叫数据，但是这些系统仍然不能在一个实时或接近实时的基础上对已检测出来的欺诈行为作出响应。在一个实例中，系统可能向在一个

网络监测或运营中心里面的一名调查人员产生一次报警。然而，这些报警一般地将不会被立即审查或处置，由此导致在对欺诈行为作出响应方面出现一个不容忽视的潜伏期。由于这些系统在对已检测出来的欺诈行为作出响应方面的迟滞性质，所以在产生报警之后，各服务提供商和各顾客仍然要遭受为数相当可观的财务损失。而且，基于不精确的检测的自动预防措施将导致对各合法用户的服务的损害。

本发明的概要

根据本发明的原理，通过自动地产生用于管理欺诈行为的各项建议，以响应可疑的欺诈活动，以便从实质上减少在一个通信网络中因欺诈行为而产生的损失，并且通过导出各项建议，作为欺诈活动、合法活动，以及用户背景信息的一个函数。更具体地说，一个可编程的规则引擎被用来自动地产生各项建议，以便在逐次呼叫评分的基础上对欺诈活动作出响应，使得各项建议直接地对应于可疑的欺诈活动的类型和数额。通过自动地产生更精确的对欺诈行为的响应，使得根据本发明原理的欺诈行为管理跟现有的安排相比，在符合运营、财务以及顾客满意等方面的要求上是更加有效的，在现有的安排中，一个案例可能要经过排队等候，直到一名调查人员对它进行分析并且确定要采取何种动作，这些动作典型地关闭或者挂起一个顾客的帐号，直到欺诈活动被调查清楚为止。根据本发明原理的欺诈行为自动管理在减少因欺诈行为而导致的损失以及在调查可疑的欺诈行为中需要占用较少的资源方面导致明显的成本降低。而且，调查时间得以缩短，从而改进了对可疑的欺诈行为的响应时间。

在一个用于管理远程通信欺诈的说明性的实施例中，一个欺诈行为自动管理系统接收先前已被评分的呼叫详细记录以识别可能的欺诈呼叫。根据一个个别用户的已学习的行为以及一个欺诈作案者的已学习的行为，欺诈计分方法对每一次呼叫的欺诈概率进行评

估。重要的是，计分方法还提供针对该呼叫的呼叫详细记录中的各种要素对欺诈分数的贡献的一种指示。一次案例分析被启动，并且根据欺诈分数将先前已评分的呼叫详细记录区分为无害组与可疑组。根据已选定的各变量以及针对其各次呼叫的评分来表征各个组。这些特征跟用户信息组合在一起以产生诸判决变量的一个集合。然后，应用一组规则来确定各判决变量的当前集合是否符合可定义的各项条件。当符合一项条件时，就向该帐户提出与该条件有关的各项预防措施。作为一个例子，可以经由在远程通信系统中的执行功能，自动地实施所建议的各项预防措施。

根据本发明的另一方面，基于逐次呼叫评分的欺诈行为自动管理有助于实现一种连续的更新特征。例如，随着各次新的呼叫被评分以及被添加到一个案例当中去，正在使用的案例可以被重新评估。而且，随着各项新建议的产生，可以对一个案例进行更新。

附图的简要说明

通过结合诸附图来考虑以下的详细说明，就能获得对本发明的一个更全面的理解，在附图中，相同的各部分对应于相同的各参考号码：

图 1 是一份简化的方框图，说明在一个远程通信网络中用于管理欺诈行为的本发明的一个实施例；

图 2 是根据本发明的原理可以被使用的用户信息的一份示例性的列表；

图 3 是一份简化的方框图，说明在根据本发明的一个实施例中，呼叫评分是如何实现的；

图 4 是根据本发明的一个实施例的案例分析过程的一份简化的流程图；

图 5A 是一份简化的方框图，说明在图 4 所示的实施例中，用于归纳案例详细记录的步骤；

图 5B 是根据本发明的原理可以被使用的已评分的各呼叫变量的

一份示例性的列表；

图 6 是根据本发明的原理可以被使用的各判决变量的一份示例性的列表；

图 7 是根据本发明的一个实施例，用于产生各项建议、以响应可疑的欺诈活动的过程的一份简化的流程图；以及

图 8 是根据本发明的原理，可能被实施的各项预防措施的一份示例性的列表。

本发明的详细说明

虽然本文所描述的说明性的诸实施例特别地适合于管理在一个远程通信网络中的欺诈行为，并且将在这份示例性的文本中被描述，但是专业人士将从本文的讲授内容中了解到，本发明的各项原理也可以应用于其他非远程通信的基于交易的各种网络之中。例如，本发明的各项原理可以应用于支持各种在线信用卡交易、各种基于因特网的交易以及诸如此类的各种网络之中。其结果是，在一个远程通信实例中的“呼叫”和“呼叫详细记录”可以分别地等同于在一个非远程通信实例中的“交易”和“交易记录”，等等。相应地本文中所示出和描述的诸实施例仅仅是为了用于说明，并且没有限制的意义。

图 1 表示在一个典型的远程通信网络中用于管理欺诈行为的本发明的一个说明性的实施例。更具体地说，系统 100 被这样构成，它响应于在一个远程通信网络 150 中的可疑的欺诈活动，执行各种功能和操作。如图所示，系统 100 包括呼叫评分功能 120，实例分析功能 200，以及执行功能 300。为了激活这些功能，系统 100 存储的数据包括，但不局限于，已评分的呼叫详细记录 401，已存储的各案例 402，以及用户帐号信息 403。人们将会懂得，在一个说明性的实施例中，通过使用计算机硬件以及被编程用来实行这些功能和操作的软件来实现系统 100，它们中的每一项都将在下文中作更详细的描述。

众所周知，一个远程通信网络，例如网络 150，为在该网络中被处理的每一次呼叫产生各项呼叫详细记录。根据本发明的原理，这些呼叫详细记录经由路径 151 被送往处于系统 100 之中的呼叫评分功能 120，使得每一次呼叫都被评分，以便确定该次特定的呼叫对欺诈行为的似然度。如图所示，所得到的已评分的呼叫详细记录被存储到方框 401 供以后使用，同时也被送到案例分析功能 200，以便进行处理。正如在本文中所使用的那样，“案例”这个词被用来表示一个可能的欺诈案例，它可能出现在一份已付款的帐单、一份始发的线路／设备帐单、针对该呼叫的一份终到线路／设备帐单等等之上。

如图所示，案例分析功能 200 接收已评分的呼叫详细记录以及用户帐号信息（方框 403），其实例可能包括帐单的类型（商业，住宿），顾客的信用额度，顾客的信用限制，以往的帐单处理指示器，帐户建立日期，等等。作为案例分析的一个结果，如图所示，案例的各项详细记录被存储在方框 402 之中。此外，为了响应于在一个帐户上的可疑的欺诈行为，自动地产生各项建议，所建议的对欺诈行为的各项响应可以包括，例如，对应于可疑的欺诈活动的类型和数额的特定的预防措施。如图 1 的实例所示，来自案例分析功能 200 的所建议的对欺诈行为的响应可以包括，可以经由执行功能 300 实现的各项响应，上述执行功能经由路径 152 被连接到网络 150。可以使用众所周知的各种技术，令网络 150 以一种特定的方式去响应一次特定的呼叫活动，例如，阻止该呼叫，令该呼叫不能进入这个帐户，等等。

图 1 就呼叫评分以及案例分析进一步地说明本发明的叠代和自适应等各个方面。更具体地说，一个正在使用的案例（例如，已存储在方框 402 之中）可以作为新的呼叫而被重新评估，并且作为新的呼叫而被评分以及被添加到该案例中去。随着各项新的建议作为案例分析的结果而产生，一个案例也可以被更新。例如，各呼叫详细记录经由路径 151 被送往呼叫评分功能 120。如方框 401 所示，新

评分的各次呼叫可以连同已存储的先前的已评分的各次呼叫一起被送到案例分析功能200。再有，案例分析功能200对已评分的呼叫数据连同用户信息（方框403）一起进行分析。图2中的表格表示可以用于案例分析的用户帐号信息的某些例子的一份列表。然而，这些例子仅是说明性的，并且没有任何限制意义。

回到图1，案例分析功能200也可以取出一个有效的案例（例如，先前存储在方框402里面的）以便针对新评分的各次呼叫以及用户信息（方框403）作进一步的分析。由案例分析功能200产生的各项新的建议也可以被添加到正在使用的案例中去。如图所示，各项执行措施（方框300）可以作为由案例分析功能200所产生的新建议的一个结果而实施，或者作为跟一个先前存储的案例（方框402）有关的先前产生的各项建议的一个结果而实施。这样一来，根据本发明的原理的欺诈行为自动管理允许连续的更新。

参看图3，现在对图1的呼叫评分功能120进行更加详细的说明。如上所述。呼叫评分功能120针对在远程通信网络150中发生的各次呼叫提供欺诈行为评分信息，使之能产生用于响应可疑的欺诈活动的适当的建议。

更具体地说，可以按照在图3所示的示例性实施例中所进一步地说明的方法，来实现呼叫评分功能120。一般来说，评分基于用户行为分析，在其中，代表一个用户的呼叫模式的一个签名（存储在方框1202之中）以及代表一种欺诈呼叫模式的一个欺诈签名（存储在方框1211之中）被用来确定一次特定的呼叫跟欺诈行为的似然度。然后将已评分的呼叫信息存储起来（方框401），供以后取出使用，并且用于叠代和连续更新过程之中，还准备用于案例分析（200），这将在下文中作更详细的说明。

如图所示，从网络150将各呼叫详细记录送往呼叫评分功能120。如方框1201所示，可以使用来自尚未被证实或者被怀疑是欺诈行为的各次呼叫的已评分的各呼叫详细记录，对一个用户的签名进行初始化。例如，当一个用户初次发出一次或多次呼叫时，就可

能出现初始化。正如在方框 1201 中进一步地表示的那样，使用来自尚未被证实或者被怀疑是欺诈行为的相继的各次呼叫的新评分的各呼叫详细记录，就能对来自方框 1202 的已存储的用户签名进行更新。就其本身来说，一个用户的签名可以在一段时间内适应于该用户的行为。

必须指出，用户签名的初始化也可以基于合法的呼叫行为的预先定义的各种属性，可以由历史上的多次呼叫记录以及诸如此类来加以定义。这样一来，由于一个合法用户的签名，即使在呼叫活动的早期阶段，也能跟合法的各主呼者的预期的（或者预告的）行为对得上。就其本身来说，例如，在一个新帐号上的任何直接的欺诈呼叫行为都将不会为用户签名的初始化提供唯一的基础。

还应当指出，一个用户签名可以监测一个用户的呼叫行为的许多方面，包括但不局限于：呼叫频率，每星期定时于星期几，每一天定时于几点钟，呼叫时长，付费方法，地理位置，等等。其结果是，可以从典型地包含在呼叫详细记录中的信息来导出一个签名，例如：始发号码；终到号码；已记帐的次数；开始时间和日期；始发位置；载频选择；呼叫等待指示器；呼叫转移指示器；三方呼叫／转移指示器；话务员帮助请求；以及网络安全失效指示器，仅举这几个为例。被用来建立以及更新一个用户签名的特定要素取决于网络的类型（例如，电话线路，无线电，用户卡，非远程通信，等等），被使用的特定评分方法，以及为专业人士所熟知的其他因素。

一般来说，每一次呼叫都将根据该呼叫与从方框 1202 中取出的用户签名相比较的结果，以及跟从方框 1211 取出的一个欺诈签名相比较的结果来进行评分。借助于实例，可以根据来自已确认的或可疑的欺诈呼叫的已评分的呼叫详细记录，对各种欺诈的签名进行初始化和更新（方框 1210）。在一个简化的实例中，若各呼叫详细记录表示对已知的行为的一次可疑的偏离，则产生一个高的欺诈行为分数，若各呼叫详细记录表示对考虑中的用户帐号来说是高度典型的行为，则产生一个低的欺诈行为分数。除了提供一个总的欺诈行

为分数作为从呼叫评分功能 120 的输出以外，该呼叫的各种要素对欺诈行为分数的贡献也应当被包括在内，在下文中将结合案例分析对其用途作更详细的说明。例如，可以包括下列各要素的贡献，以供后续的案例分析：一星期中的星期几；一天中的几点钟；时长；介于相继的两次呼叫之间的时间间隔；目的地；呼叫等待的使用；呼叫转移的使用；三方呼叫的使用；话务员服务的使用；始发点；漫游服务的使用（仅限于无线电）；呼叫过程中的越区切换次数（仅限于无线电）；网络安全报警的出现；载频选择；以及国际全面服务的使用。再有，这份列表仅是说明性的，并且在任何方面都没有限制意义。

由于呼叫评分是在一种顾客专用以及逐次呼叫的基础上进行的，所以有可能得到一个更精确的欺诈行为分数，它更能说明跟欺诈行为的似然度，同时降低虚警的次数（即，“假阳性”）。而且，为了在一个逐次呼叫的基础上精确地进行呼叫评分，专业人士都懂得，使用一个实时处理平台来执行上述各项功能。将是一种合适的实施方法。一种这样的示例性的实时处理平台就是朗讯技术公司的注册商标为 QTM 的实时交易处理平台，在作者 J. Baulier 等发表于《贝尔实验室技术杂志》1997 年 11 月 24 日的一篇论文“太阳升：一种实时事件处理框架”中，对此作了说明，该文作为参考文献已被收入本文。

专业人士都清楚，许多不同的呼叫评分技术都适于用来实现上述的呼叫评分功能 120 的各项功能。具体地说，基于统计分析、概率评分、基于存储器的推理、数据挖掘、神经网络以及其他方法学的呼叫评分技术都是已知的，并且被指望结合本文所描述的说明性的诸实施例来加以应用。在 Fawcett 等发表于《数据挖掘与知识发现》杂志 1997 年第 1 期 291－316 页的论文“自适应的欺诈行为检测”以及 1998 年 10 月 6 日授权的美国专利第 5, 819, 226 号“使用预测模型进行欺诈行为检测”等文献中，都叙述了这些方法和技术的某些示例，以上两篇已作为参考文献被收入本文。

图 4 表示图 1 的案例分析功能 200 的一个说明性的实施例。如步骤 201 所示，对跟一个先前已评分的呼叫有关的各项详细记录进行观察，以确定该呼叫是否开辟了一个新的欺诈案例，或者将该呼叫添加到一个现有的案例中去。特别是，观察由呼叫评分功能 120 针对一次特定的呼叫所产生的欺诈行为分数以及其他预定的变量，例如特定的诸要素对欺诈行为分数的贡献，以确定从欺诈的角度来看，该呼叫是不是“感兴趣的”。由于任意数目的不同理由，可以使一次呼叫成为“感兴趣的”。这些理由包括，但不局限于：一个欺诈行为分数超出一个预定的（例如，可配置的）数值；在规定次数的呼叫中，一个欺诈行为分数表明它达到了一定数量的分数变化的顶点；在时间上跟一次先前的呼叫发生重叠的表示（即，一次“冲突”）；给出介于两次呼叫之间的时间间隔，表示在两次呼叫之间在始发点上的变化，这对一个用户来说是办不到的（即，一次“速度违规”）；或者是一个现有案例的一个成员。

若一次已评分的呼叫被确定为感兴趣的，则在步骤 202 进行一次检查，看看在有关的帐户上是否存在一个现有的案例。若找不到案例，则通过下列各步骤生成一个新案例：1）

在步骤 203，取出在用户帐号中的背景信息，上述用户帐号被存储在系统之中（见图 1 中的方框 403）；2） 在步骤 204，取出针对该帐号的已评分的呼叫详细记录；以及 3） 在步骤 205，将已评分的呼叫详细记录加以归纳。为了在步骤 205 中对已评分的呼叫详细记录进行归纳，必须首先对各呼叫详细记录进行分类，然后必须根据预定的诸变量来表征每一类。如图 5A 所示，各呼叫详细记录首先被分类为多个分组或集合，例如，集合 1、集合 2 到集合 N，它们可以被分类为，例如，无害的，可疑的以及不确定的各种集合。初始分类基于欺诈行为分数，其中，根据其欺诈行为分数与已建立的用以定义各类的数值或阈值进行比较的结果，将每一份呼叫详细记录放入各集合当中的一个。通过考虑其他的诸要素，仅举数例，例如始发位置以及所拨的电话号码，可以作出这种分类的自动调整。例

如，若在无害集合中的大多数呼叫详细记录都含有一个给定的高度典型的始发位置或所拨的电话号码，则一种可能的调整就是将在其他集合中具有相同属性的所有呼叫记录都转移到无害集合中去。然后，通过将处于每一个集合之中的呼叫汇总变量列成表格来表征各个集合。特别是，可以为该案例同时也为在一个案例之中的个别集合（例如，无害的、可疑的、不确定的）导出多个呼叫汇总变量。图 5B 中的表格表示可用于案例分析的呼叫汇总变量的一个示例性的列表。如表中所示，变量 410（"FirstAlertAt" 以及 "CaseScore"）代表属于所有案例的变量。例如，当针对该案例的第一个高分数呼叫（例如，可疑的欺诈）出现时，"FirstAlertAt"（首次报警发生在）将被用来提供此刻的一个时间数值，不管该呼叫最初被放入到哪一个特定类之中。可以根据在该案例中个别的各呼叫分数，使用 "CaseScore"（案例计数）来提供一个总的案例分数，同样不管它处于该案例中的哪一类里面。

在这个说明性的实例中，示于图 5B 的其余的各变量都可应用于该案例里面的一个特定的集合，例如，无害的、可疑的，以及不确定的集合。在该表的描述字段中，提供了关于每一种呼叫汇总变量的说明。如该表格所示，依赖于集合的呼叫汇总变量可以被表征为两种类型的变量。第 1 类呼叫汇总变量 420，从 "Number of Calls "（呼叫次数）到 "Hot Number Count"（热线号码计数），全都属于一种求和类型的运算，在其中，针对该呼叫的一个特定要素，保持一个计数或百分比。以呼叫汇总变量 421（"Hot Number Count"）为例，这个数值将表示在一个给定的集合中呼叫的总次数，在该集合中，被呼号码是一个预定的（以及可选择的、可编辑的，等等）"热线号码" 列表中的一个成员。专业人士都充分地理解 "热线号码" 的意义和用途。

剩下的呼叫汇总变量 430，从 "Day Score Dist"（日分数分布）到 "International Score Dist"（国际分数分布），全都属于一个特定的要素或诸要素对该集合之中的欺诈行为分数的贡献分布，例

如，呼叫汇总变量 431（“Hour Score Dist”[小时分数分布]）表示在该集合中“Hour of the day”（一天中的几点钟）发出的呼叫对欺诈行为分数的影响或贡献。应当指出，在图 5B 的表中所列出的呼叫汇总变量仅是说明性的，并且在任何方面都没有限制意义。

可以选择其他的呼叫汇总变量去表征一个集合，这依赖于几种因素，例如网络类型、交易类型，等等。

再次参看图 4，在步骤 202，若找到一个现成的案例，则随后在步骤 206 取出该案例，并且该案例的汇总，例如，来自图 5B 的各呼叫汇总变量，被来自当前呼叫的信息所更新。基于一个新生成的汇总（步骤 203－205）或者一个已更新的汇总（步骤 206－207），该系统计算各判决变量的一个集合，如步骤 208 所示。更具体地说，用各判决变量来确定是否已经满足一定的条件，在此基础上，产生用于响应在网络中的可疑的欺诈活动的各项建议。在图 6 的表格中示出了各判决变量的一个示例性的列表，根据本发明的原理，这些判决变量可以用于案例分析。

如图 6 所示，判决变量 440 被描述为来自图 5B 的任何呼叫汇总变量，或者一个或多个呼叫汇总变量的任何操作，例如比值、数学运算，等等。例如，任何一个呼叫汇总变量 410、420 或 430 都可以个别地构成一个判决变量，用以确定响应于欺诈行为的一项适当的建议。适当的判决变量的另一个实例就是按照某种预定的方式，将两个或多个呼叫汇总变量组合在一起，例如在该集合中，使用呼叫转移的呼叫次数（“CF Count”）对呼叫总次数（“Number of Calls”）的比值。可用的判决变量的选择还是依赖于网络类型、交易类型，以及被确定为可用的其他各项因素。附加的判决变量 450 也可以被用来提供附加的信息，在分析欺诈活动以确定适当的建议的过程中，这些信息是有帮助的。例如，可以使用在图 6 的表格中所描述的“AccountAge”（帐户年龄）、”PreviousFalseAlarms”（先前的虚警次数）、“AccountType”（帐户类型）、“CreditRating”（信用额度），以及“AlertCounts”（报警次数）等变量。应当指

出，在图 6 的表中所列出的各判决变量仅是说明性的，并且在任何方面都没有限制意义。其他的各判决变量对专业人士来说是显而易见的，它们分别给出特定的网络类型、交易特征，等等。

再次参看图 4，在步骤 209，该系统接着产生一项或多项建议，以响应可能在一个帐户中出现的欺诈行为。图 7 表示根据本发明的原理，在产生各项建议的过程中所涉及的各步骤的一个示例性的实施例。

简要地考察有关的术语对于理解图 7 所示的各步骤是有帮助的。正如本文所描述的那样，一项规则被定义为包括一项“条件”以及一项或多项“措施”的一份列表。一项“条件”可以是一个布尔表达式，它支持在各判决变量（在图 6 中被定义）以及各预定的数值或各常数中进行比较。在一种最简单的形式中，布尔表达式可以使用标准的布尔运算符，例如与、或、非以及运算优先顺序。一个单独的“措施”标识一项动作（例如，封锁服务或封锁市场），与该动作有关的各项参数（例如，在封锁服务实例中的呼叫转移，或者在封锁市场实例中的市场 25），以及一个用来表示该措施是否需要自动执行的标志。一般来说，可以由该系统的用户（例如，服务提供商）对各项规则进行修改，这取决于该网络所给出的对欺诈行为的管理要求。

参看图 6 中的步骤 2091，系统取出各种规则的一个列表，并且根据一种层次结构来处理每一条规则，这种层次结构可以是简单的，例如从头到尾，或者按照某些预定的图表。然后，使用为该条件而指定的可用的判决变量（图 6）来测试用于该规则的条件（例如，**CFcount / numcallsinset > 0 . 25**）。在步骤 2092 中对此作了说明。若该规则的条件得到满足，则在步骤 2093 取出跟这条特定规则有关的一项措施。如步骤 2094 所示，若先前没有这样的规则 [该规则调用与在已取出的措施（从步骤 2093）中所标识的动作相同的动作（例如，封锁各项服务）]，则在步骤 2095，将已取出的措施添加到所需的各项措施的列表中去。若该动作已经被一项先前的规则所要求，

则该措施被忽略。这样一来，在有冲突的案例中，在各项规则之间建立起优先顺序。下一个步骤就是确定是否还有更多的措施跟该规则有关，如步骤2096所示。若有，则为在该规则中的所有措施重复执行步骤2093－2095。若没有其他措施跟该特定的规则(在步骤2091中被取出）有关，则在步骤2097，系统检查是否有其他可用的规则。若有附加的规则，则在步骤2091－2096中重复上述过程。一旦没有更多可用的规则，则系统返回到图4中的步骤210。

再次参看步骤2092，若不满足该规则的条件，则在步骤2097，系统检查是否还有更多的规则，并且，若有，则从步骤2091开始，将该过程重复执行一遍。若没有更多的规则，则按照下文所述的方法，执行与图4中的步骤210以及后续的各步骤有关的动作。

作为在图7所示的各步骤中所进行的处理的结果，自动地产生出一项或多项被建议的措施，以响应可疑的欺诈行为。图8示出了在所建议的措施中某些动作的实例。例如，一项被建议的措施可能是封锁所有的帐户活动（在这里，该动作是“封锁帐户”），或者仅封锁国际拨号（在这里，该动作是“封锁拨号”并且相关的参数是“国际”），或者封锁一种特定类型的服务，例如，呼叫转移。应当指出，图8中的被建议的各项动作的这份列表仅是说明性的，并且在任何方面都没有限制意义。

重要的是，必须指出，作为逐次呼叫的评分、基于评分的各项适当的规则的应用、适当的呼叫汇总变量以及判决变量的选择等的一项功能，就是可以自动地产生适当的建议。就其本身来说，自动地产生的各项建议对应于逐次呼叫评分过程，使得各项建议更精确地对准在帐户中出现的欺诈行为的特定类型。例如，大多数欺诈行为检测和预防系统仅能检测欺诈行为的出现，并且仅具有变化着的精度水平。一旦检测到欺诈行为，这些系统典型地都将该案例转入人工调查。各项预防措施，如果它们都存在的话，并不全都适用于可疑的欺诈行为的类型。与此相反，根据本发明原理的欺诈行为管理系统不仅能检测欺诈行为，而且能收集关于该欺诈行为的特定的

特征的信息。其结果是，所建议的对欺诈行为的响应适用于正在发生的欺诈行为的特定类型。

作为一个实例，若案例分析确定对一个高欺诈行为分数的最重要的贡献涉及呼叫转移的使用，则一个适当的被建议的对欺诈行为的响应可能是关闭该帐户的呼叫转移服务，而不是关闭该帐户的所有服务。这样一来，欺诈行为导致的损失得以最小化或消除，同时保持对该合法用户的服务。而且，通过使用在该网络之中的执行特性，就能自动地执行关闭呼叫转移的一项建议。

回到图 4，在步骤 210，将在步骤 209 中产生的建议或诸建议跟先前针对该案例给出的诸建议进行比较。若从步骤 209 产生的各项建议不是新的，则针对该特定呼叫的呼叫分析过程结束。若各项建议是新的，则在步骤 211，用各项新建议来更新该案例。若各项新建议中的任何一项属于如同在步骤 212 中所确定的准备自动执行的类型，则相应地采取各种适当的实施动作。例如，如前所述，可以经由在远程通信网络中的执行功能 300（图 1）自动地实施所建议的各种动作。

总的来说，根据本发明原理的各项建议的自动产生在一个可编程的基于规则的引擎（例如，各项规则可以被重新编程）上被描述。此外，记住这一点是重要的，即，以上在图 1－8 的文字说明中所描述的各处理步骤，在该网络中都可以在一个逐次呼叫的基础上加以实现。因而，基于规则的引擎是一个自适应系统，它被用来在网络中在一个逐次呼叫的基础上，显示各案例的一段历史、判决标准以及各项最终结果。就其本身来说，根据本发明原理的欺诈行为管理系统和方法向各服务提供商提供了一种欺诈行为管理系统，它除了检测之外，还能根据用户定义的政策、用户的各种行为，以及诸如此类来加以定制。

正如本文所描述的那样，可以采取各种方法以及用于实行这些方法的各种装置的形式来实施本发明。还可以采取被写入到有形介质之中的程序代码的形式来实施本发明，上述介质例如软磁盘、只

读光盘、硬盘，或者其他可用机器读出的存储介质，其中，当用一部机器，例如一部计算机，来安装和执行该程序代码时，这部机器就成为用于实施本发明的一个装置。还可以采取程序代码的形式来实施本发明，例如，不管是存储在一种存储介质之中，被一部机器所安装和／或执行，还是经由某些传输介质，例如通过电线或电缆，通过光纤，或者经由电磁辐射，来进行传输，其中，当用一部机器，例如一部计算机，来安装和执行该程序代码时，这部机器就成为用于实施本发明的一个装置。当在一个通用处理器上实施时，各程序代码段与该处理器相结合，就提供一部独特的装置，其工作类似于各种专用逻辑电路。

还应当指出，以上仅说明了本发明的原理，还要懂得，专业人士将能设计出各种不同的安排，虽然在本文中没有明显地描述或示出，但是这些安排体现了本发明的原理，并且被包括在它的精神实质和范围之内。而且，在本文中所列举的所有实例和条件语言主要地是为了专门地仅用于讲授的目的，以帮助读者了解本发明的原理以及由（各）发明人为了促进此项技术而提出的概念，并且被解释为不局限于如此专门地列举的各实例以及各项条件。而且，在本文中，用以讲述本发明的各项原理、各个方面以及各实施例的所有陈述，以及其中的各特例，旨在用来涵盖其结构上的和概念上的等效物。此外，还打算将这些等效物包括当前已知的等效物以及将来开发出来的等效物，即，不管结构如何，能执行相同功能而开发的任何要素。

因此，例如，专业人士将懂得，本文的各方框图表示能体现本发明的各项原理的说明性的电路的概念性的视图。类似地，还应当懂得，任何流程图、信号流图、状态转移图、伪代码，以及诸如此类均表示各种过程，这些过程基本上可以在计算机可读介质中被表现，并且由一个计算机或处理器来执行，不管这样的计算机或处理器是否明显地被示出。

在附图中所示的各项要素的功能可以通过使用专用硬件或者通

过能够执行软件的硬件并结合适当的软件来提供。当由一个处理器来提供时，可以由一个单独的专用处理器、由一个单独的共享处理器、或者由多个个别的处理器（其中的某些可以共享）来提供。而且，一个“处理器”或“控制器”不应当被解释为唯一地能执行软件的硬件，它同时可以不加限制地隐含数字信号处理器（DSP）硬件，用于存储软件的只读存储器（ROM）、随机访问存储器（RAM），以及非易失性存储器。还可以包括其他常规的和／或定制的硬件。类似地，在附图中的任何交换机都仅是概念性的。正如从文字说明中更明确地理解的那样，可以通过程序逻辑、通过专用逻辑、通过程序控制与专用逻辑的交互作用，或者甚至用手工方法来实现它们的功能，特定的技术可以由实施者进行选择。

在本文所附的权利要求书中，作为用于实行一项指定的功能而表达的任何要素都打算涵盖用以实现该功能的任何方式，包括，例如，a）实现该功能的各电路元件的一种组合，或 b）任何形式的软件，因此，包括固件、微代码或者诸如此类，它们与适当的电路相组合，用以执行该软件以实现该功能。由这样的权利要求书所定义的本发明具备这样一个事实，即，由各种已列举的装置所提供的各项功能，按照权利要求书所要求的方式被组合和集中在一起。各申请人认为，凡是能够提供这些功能的任何装置都是本文所示的装置的等效物。

说 明 书 附 图

图1

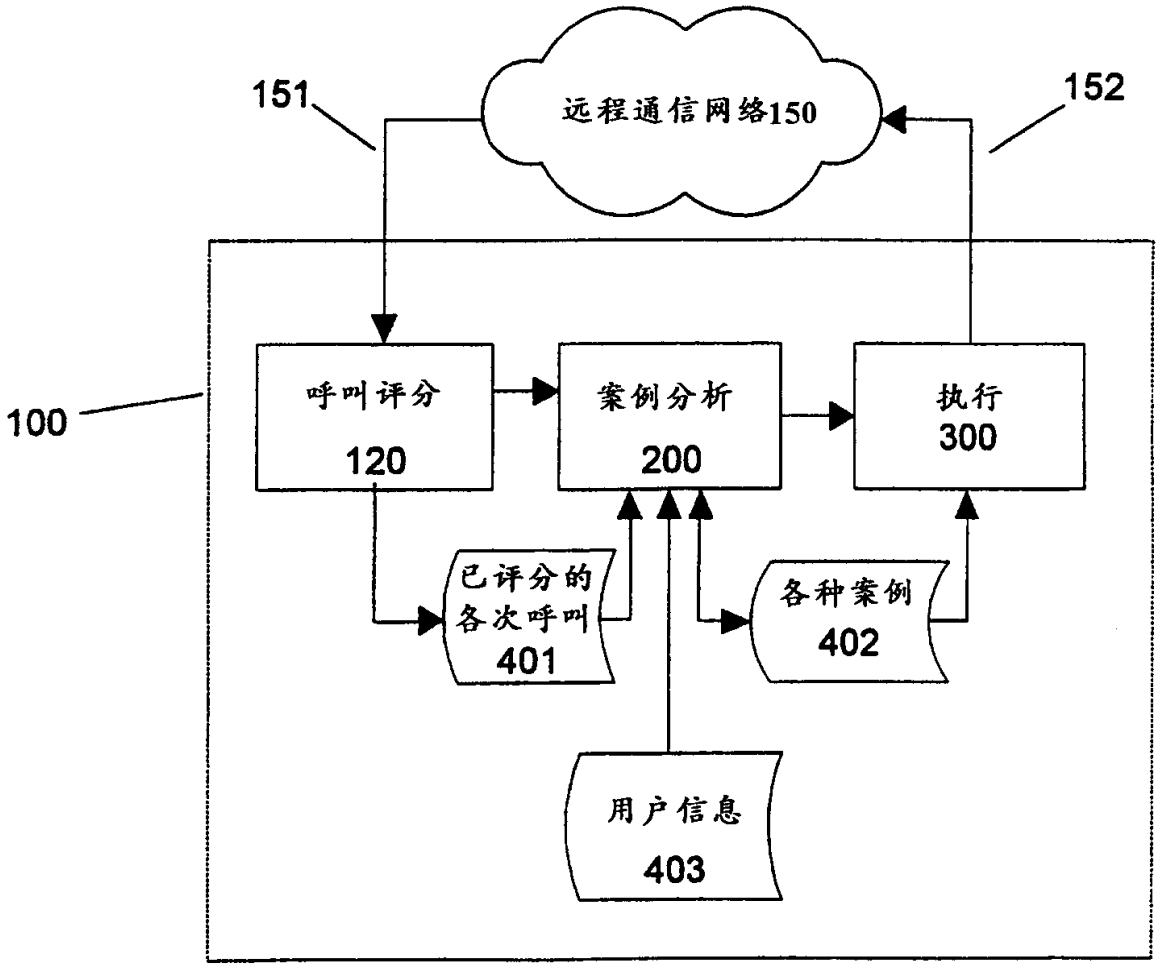

远程通信网络150
151
152
100
呼叫评分
120
案例分析
200
执行
300
已评分的
各次呼叫
401
各种案例
402
用户信息
403

图2

变量	描述
AccountAge	帐户的年龄
AccountType	帐户类型的表示（商业，住宿等）
CreditRating	顾客的信用额度

图 3

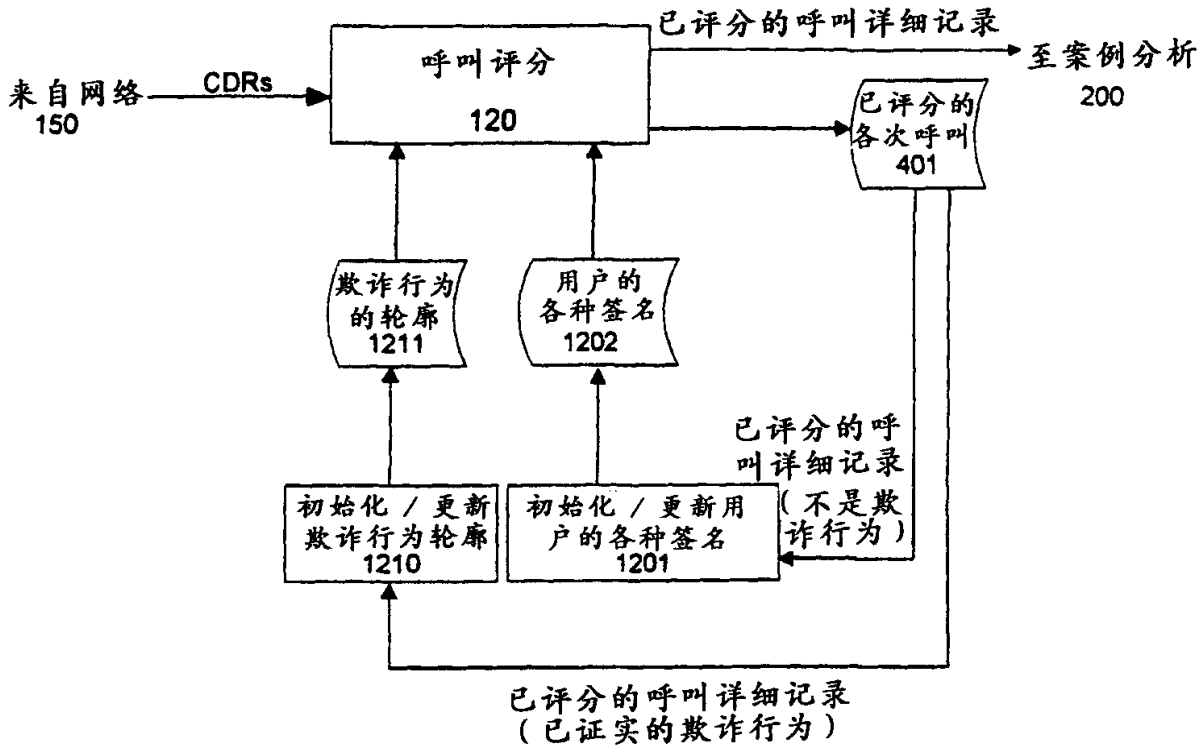

来自网络
150
CDRs
呼叫评分
120
已评分的呼叫详细记录
至案例分析
200
已评分的
各次呼叫
401
欺诈行为
的轮廓
1211
用户的
各种签名
1202
已评分的呼
叫详细记录
（不是欺
诈行为）
初始化 / 更新
欺诈行为轮廓
1210
初始化 / 更新用
户的各种签名
1201
已评分的呼叫详细记录
（已证实的欺诈行为）

图4

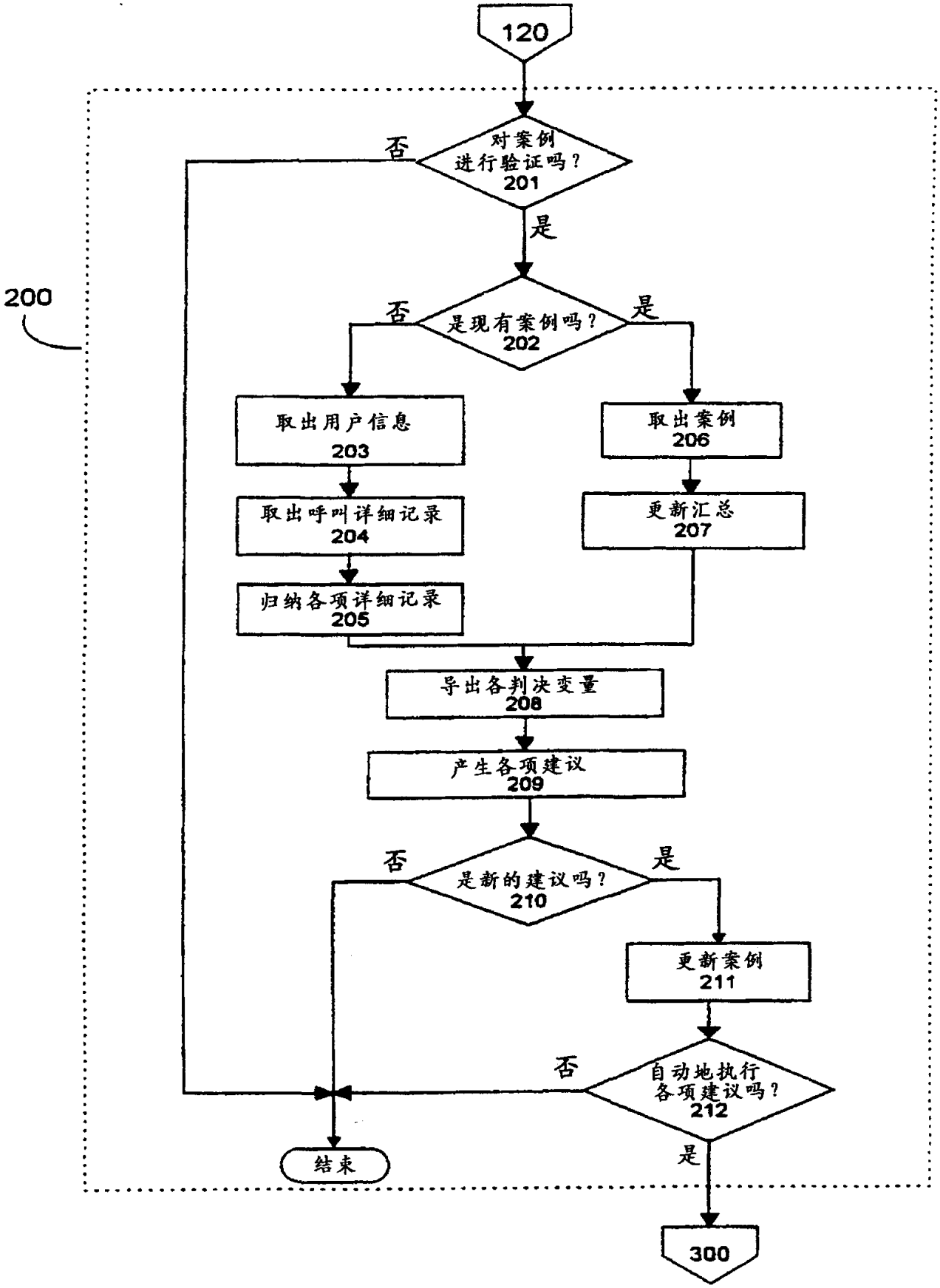

120
对案例进行验证吗？
201
否
是
200
是现有案例吗？
202
否
是
取出用户信息
203
取出呼叫详细记录
204
归纳各项详细记录
205
取出案例
206
更新汇总
207
导出各判决变量
208
产生各项建议
209
是新的建议吗？
210
否
是
更新案例
211
自动地执行各项建议吗？
212
否
是
结束
300

图5A

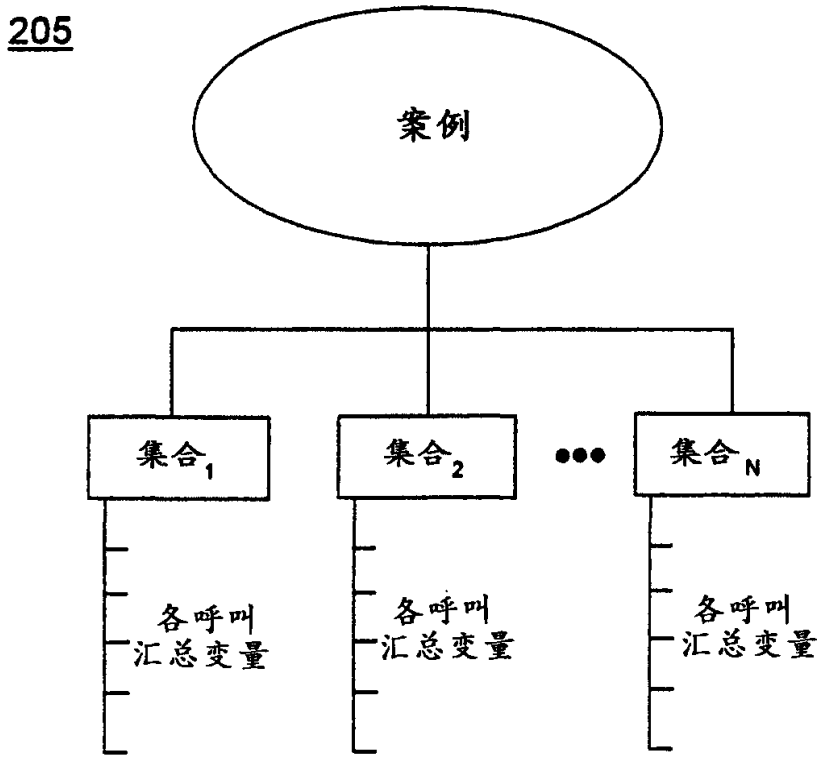


图5B

	变量	每个	描述
410	FirstAlertAt	案例	首次出现高分呼叫的时间
	CaseScore	案例	案例总数
420	Number of Calls	集合	在集合中的呼叫总次数
	Total Minutes	集合	在集合中的所有呼叫的时长总和
	CF Count	集合	在集合中使用呼叫转移的呼叫次数总和
	TWC Count	集合	使用三方呼叫或转移的呼叫次数总和
	Op Count	集合	在集合中请求话务员服务的呼叫次数总和
	Roaming Count	集合	在集合中始发点是一个漫游位置的呼叫次数总和（仅限于无线电）
	International Count	集合	在集合中被呼号码为国际号码的呼叫次数总和
421	Hot Number Count	集合	在集合中被呼号码为可编辑的热线号码表中的成员的呼叫次数总和
430	Day Score Dist	集合	对在集合中的所有呼叫而言的X的概率分布，其中，X是一星期中的星期几对该呼叫的分数的贡献。在可配置的分布中的各要素的数目 [“一星期中的星期几的贡献分布”]
431	Hour Score Dist	集合	一天中的几点钟的贡献分布
	Duration Score Dist	集合	时长的贡献分布
	TBC Score Dist	集合	介于两次呼叫中的时间间隔的贡献分布
	Dialing Score Dist	集合	拨号的贡献分布
	CW Score Dist	集合	使用呼叫等待的贡献分布
	TWC Score Dist	集合	使用三方呼叫/转移的贡献分布
	Operator Score Dist	集合	话务员服务请求的贡献分布
	CF Score Dist	集合	使用呼叫转移的贡献分布
	Origination Score Dist	集合	始发位置的贡献分布
	Roaming Score Dist	集合	出现漫游的贡献分布（仅限于无线电）
	Handoff Score Dist	集合	越区切换次数的贡献分布
	Security Score Dist	集合	网络安全报警的贡献分布
	Carrier Score Dist	集合	载频选择的贡献分布
	International Score Dist	集合	使用国际服务的贡献分布

图6

变量	描述
****	来自图4的任何呼叫汇总变量或各变量的组合
AccountAge	帐户的年龄
PreviousFalseAlarms	先前已经开辟的不是欺诈行为的案例的数目
AccountType	帐户类型(商业,住宿等)的表示
CreditRating	顾客的信用额度
AlertCounts	轮廓偏离报警的次数以及冲突/速度违规报警次数

440

450

图7

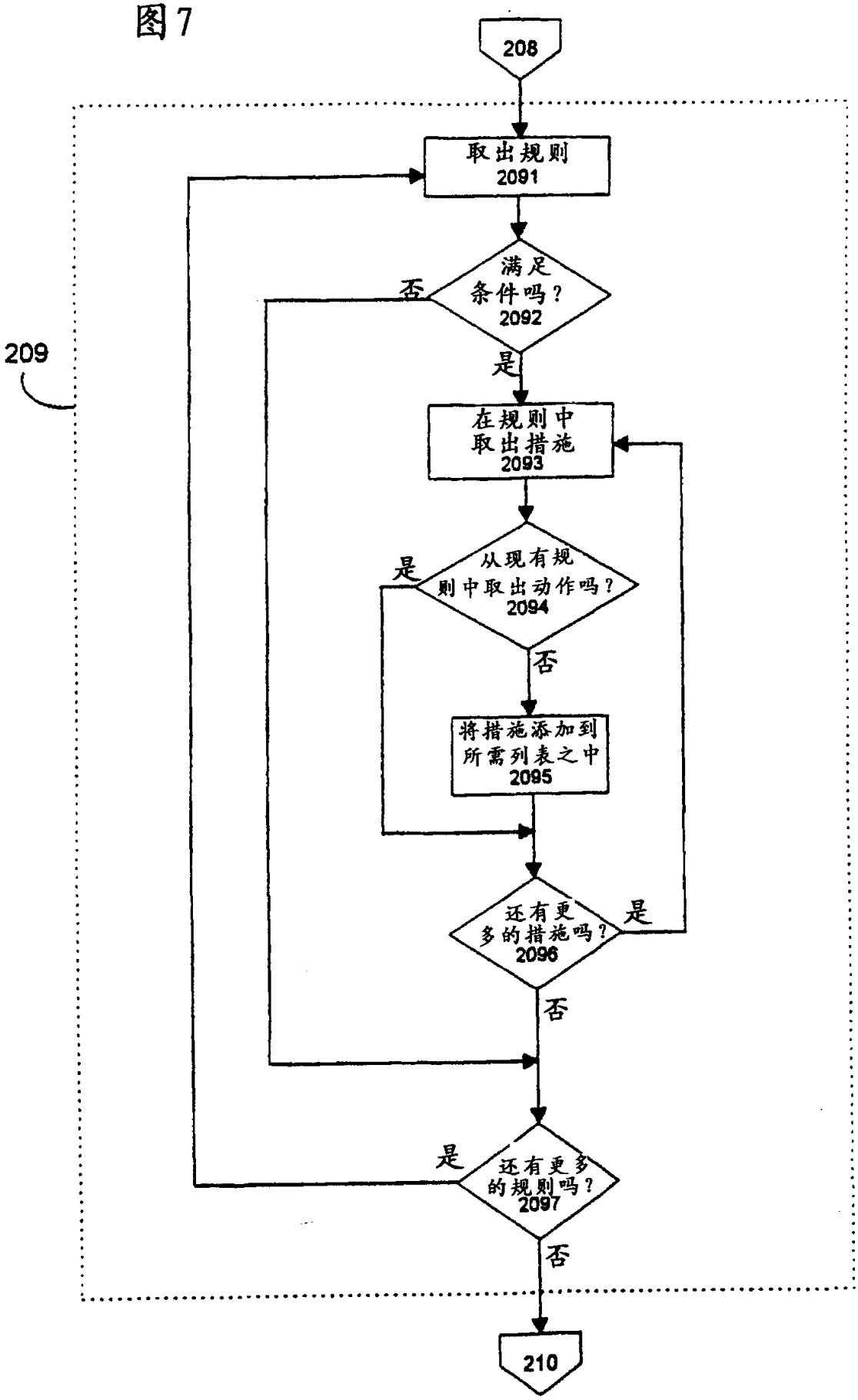

208
取出规则
2091
满足
条件吗？
2092
否
是
209
在规则中
取出措施
2093
从现有规
则中取出动作吗？
2094
是
否
将措施添加到
所需列表之中
2095
还有更
多的措施吗？
2096
是
否
还有更多
的规则吗？
2097
是
否
210

图8

动作	描述和各项参数
封锁个人识别号码	封锁一个多用户无线电或用户卡帐户的一个用户 参数PIN，ESN或子帐户
封锁帐户	封锁所有的帐户活动 参数：无
封锁市场	从特定区域封锁无线电或用户卡帐号的使用 参数：区域列表
封锁拨号	封锁国际拨号 参数：无
封锁服务	封锁呼叫转移或三方呼叫／转移的使用 参数：待封锁的服务
设置拦截	令下一次可疑的呼叫被传送到一个值班员或系统那里　参数：值班员或系统
排队	将案例放置到特定的队列中去，供调查人员使用 参数：队列标识（ID）
判断	将案例分类为可疑的合法、欺诈或订购欺诈 参数：判断
通知	产生报警：应当立即调查该案例 参数：无