РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 534 943**(13) **C2**

(51) МПК
*H04W 64/00* (2009.01)
*H04W 12/06* (2009.01)

# (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011135733/08, 28.01.2010**

(24) Дата начала отсчета срока действия патента:
**28.01.2010**

Приоритет(ы):
(30) Конвенционный приоритет:
**28.01.2009 GB 0901407.7**

(43) Дата публикации заявки: **10.03.2013** Бюл. № **7**

(45) Опубликовано: **10.12.2014** Бюл. № **34**

(56) Список документов, цитированных в отчете о поиске: **US 20080162346 A1, 03.07.2008 . US 20080227471 A1, 18.09.2008 . US 20030169881 A1, 11.09.2003 . US 20060237531 A1, 26.10.2006 . RU 2242795 C2, 20.12.2004**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **29.08.2011**

(86) Заявка PCT:
**GB 2010/000139 (28.01.2010)**

(87) Публикация заявки PCT:
**WO 2010/086608 (05.08.2010)**

Адрес для переписки:
**129090, Москва, ул. Б. Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"**

(72) Автор(ы):
**КЭРРОЛЛ Пэт (IE),**
**ПЕТЕРСЕН Джон (GB),**
**ЭЛФОРД Джонатан (GB)**

(73) Патентообладатель(и):
**ВЭЛИДСОФТ ЮКей ЛИМИТЕД (GB)**

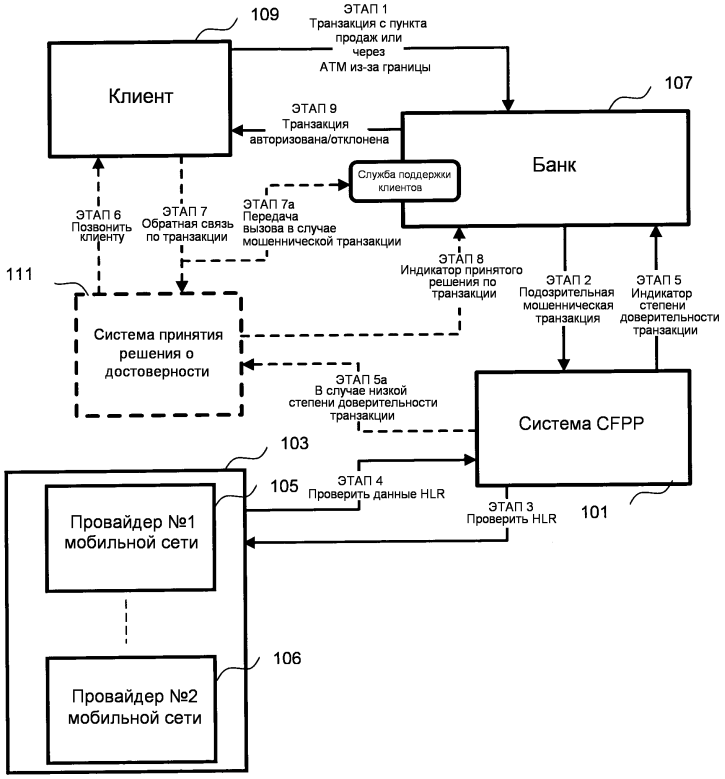
RU 2534943 C2

## (54) ПРЕДОТВРАЩЕНИЕ ЛОЖНОПОЛОЖИТЕЛЬНОГО ОПРЕДЕЛЕНИЯ КАРТЫ

(57) Реферат:

Изобретение относится к способу и системе аутентификации транзакции. Технический результат заключается в повышении оперативности аутентификации транзакции. Способ содержит этапы, на которых осуществляют прием запроса транзакции для определения, может ли запрос транзакции быть одобрен без дополнительной обработки, и разрешение транзакции, если определено, что запрос транзакции может быть одобрен без дальнейшей обработки, в противном случае осуществляют прием данных, идентифицирующих регион, где запрашивается транзакция, определение из регистра местоположения (LR) данных, полученных от провайдера мобильной сети для устройства мобильной связи, ассоциированного с лицом, запрашивающим транзакцию, причем данные идентифицируют регион, где расположено устройство мобильной связи, сравнение данных, идентифицирующих регион, где запрашивается транзакция, с данными, идентифицирующими регион, где расположено устройство мобильной связи, и в случае их совпадения, разрешение транзакции, а если данные региона не совпадают, не разрешение транзакции без дополнительной верификации

аутентичности, причем данные, идентифицирующие регион, содержат данные страны или данные, идентифицирующие штат или город. 2 н. и 12 з.п. ф-лы, 2 ил., 1 табл.




ФИГ. 1

RU 2534943 C2

RU 2534943 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 534 943**(13) **C2**

(51) Int. Cl.
*H04W 64/00* (2009.01)
*H04W 12/06* (2009.01)

## (12) ABSTRACT OF INVENTION

(21)(22) Application: **2011135733/08, 28.01.2010**

(24) Effective date for property rights:
**28.01.2010**

Priority:
(30) Convention priority:
**28.01.2009 GB 0901407.7**

(43) Application published: **10.03.2013** Bull. № **7**

(45) Date of publication: **10.12.2014** Bull. № **34**

(85) Commencement of national phase: **29.08.2011**

(86) PCT application:
**GB 2010/000139 (28.01.2010)**

(87) PCT publication:
**WO 2010/086608 (05.08.2010)**

Mail address:
**129090, Moskva, ul. B. Spasskaja, 25, stroenie 3, OOO "Juridicheskaja firma Gorodisskij i Partnery"**

(72) Inventor(s):
**KEhRROLL Peht (IE),**
**PETERSEN Dzhon (GB),**
**EhLFORD Dzhonatan (GB)**

(73) Proprietor(s):
**VEhLIDSOFT JuKej LIMITED (GB)**

RU 2534943 C2

## (54) PREVENTION OF FALSE POSITIVE CARD DETECTION

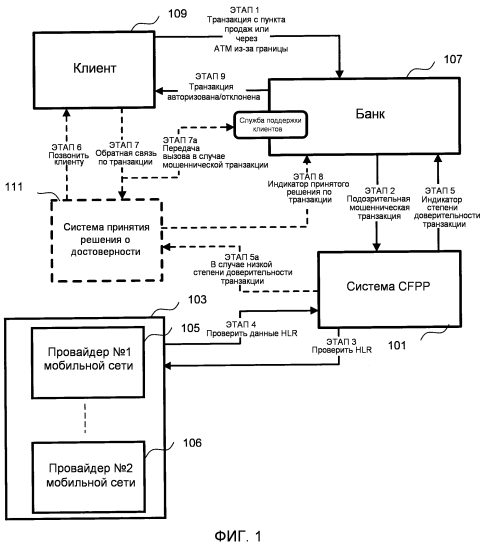
(57) Abstract:

FIELD: radio engineering, communication.

SUBSTANCE: invention relates to a transaction method and authentication system. The method comprises the following steps: receiving transaction request to determine whether the request can be approved without additional processing. If so, the permission is issued, otherwise, the region identification data is obtained, where transaction is requested. Then determination of location register (LR) data received from mobile network provider goes, for the mobile communication device associated with a person, requesting transaction. This data identifies the region where the mobile device is situated. Afterwards, comparison of transaction request region data to mobile device location data is performed. If the two sets of data coincide, the transaction is allowed, otherwise, additional authentication is required. The region identification data contains information about the country or state/city.

EFFECT: quicker transaction authentication.

14 cl, 2 dwg, 1 tbl




ФИГ. 1

## ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Данное изобретение относится к определению действительности запрашиваемой транзакции и к предотвращению ложноположительного определения, такого как предотвращение ложноположительного определения при предъявлении карты. Более конкретно, данное изобретение относится к финансовым транзакциям и к предотвращению ложноположительного определения при предъявлении карты, а также к предотвращению ложноположительного определения при предъявлении карты за границей.

## УРОВЕНЬ ТЕХНИКИ

Ложноположительное событие возникает, когда пользователь пытается выполнить легитимную финансовую транзакцию, которая отклоняется, поскольку финансовый провайдер (например, банк выдачи, предоставляющий клиентам дебетовую карту или кредитную карту) неправильно идентифицировал эту транзакцию, как потенциально мошенническую. Транзакция может представлять собой транзакцию с предоставлением карты из-за границы. Транзакция из-за границы может представлять собой транзакцию, при которой транзакция происходит в другом регионе, чем регион, где пользователь зарегистрирован у финансового провайдера. То есть транзакция с предоставлением карты из-за границы может представлять собой транзакцию, при которой пользователь снимает наличные деньги из ATM (банкомата), используя свой кредитную или дебетовую карту за границей, или в случае, когда пользователь приобретает товары в пункте продажи (PoS), используя свою кредитную или дебетовую карту за границей. В обоих случаях, карта должна быть физически представлена в точке транзакции, например, в ATM или в PoS. Это представляет собой отличие от транзакции "без предъявления карты", где присутствуют детали карты, например, имя держателя карты, номер карты, дата истечения срока действия, а также защитная информация. Саму карту не предъявляют в местоположении, где выполняется транзакция. Транзакция "без предъявления карты" может возникать в результате транзакции, представляющей заказ через Интернет или почту. Кроме того, транзакция может представлять собой транзакцию из-за границы, то есть транзакцию, в которой транзакция возникает в другой стране, чем страна, где банк выдачи держателя карты выдал эту карту.

Мошенничество с предоставлением карты из-за границы становится все более частым и в настоящее время достигает 40% всех преступлений, связанных с картами, для карт, выданных в Великобритании. Технология, такая как размещение на карте микросхемы и PIN (персональный идентификационный номер), является неэффективной для предотвращения мошенничества с предоставлением карты из-за границы, поскольку карты с использованием снятой информации (поддельные карты) просто используются в устройствах ATM и PoS в странах, которые не поддерживают технологию размещения микросхем и PIN на картах, таких как США, где проверка возвращается к магнитной полосе на карте. Технология размещения микросхемы и PIN позволяет выполнять оплату, используя дебетовые или кредитные карты. Вместо использования подписи для удостоверения платежей пользователь карты должен ввести номер PIN, известный только держателю карты.

Банки и другие провайдеры финансовых услуг обычно пытаются предотвратить мошенничество с предоставлением карты, используя программные механизмы управления риском 3-ей стороны или логику собственной разработки в процессе авторизации, выполняемой в режиме реального времени, при попытке определения, существует ли вероятность того, что транзакция является мошеннической. Другие отклоняют все транзакции из-за границы, если только держатель карты заранее не

подал провайдеру финансовой услуги точный курс своего путешествия (чего все еще может оказаться недостаточно).

Основная проблема в подходе с механизмом управления риском состоит в том, что механизмы управления риском являются чрезвычайно неточными при определении потенциально мошеннических транзакций. Частота ложноположительных определений, возникающих при использовании таких механизмов управления риском, чрезвычайно высока, типично от 80% до 90%, в результате чего возникает существенное неудобство и затраты для держателей карт и также для банков. Под частотой ложноположительных определений мы понимаем процент неправильно отклоненных транзакций среди общего количества отклоненных транзакций. В связи с высокими объемами и затратами, ассоциированными в настоящее время с ложноположительными определениями, провайдеры финансовых услуг типично не могут отклонять все транзакции, которые они хотели бы, в результате чего происходит авторизация мошеннических транзакций. Это возникает, когда стоимость предотвращения превышает стоимость мошенничества. Основные затраты для провайдера финансовых услуг и для клиентов возникают в процессе принятия решения в отношении ложноположительной транзакции.

Поэтому возникает проблема, связанная с тем, что провайдеры финансовой услуги часто неправильно идентифицируют и отклоняют действительные транзакции, как потенциально мошеннические, в частности, когда легитимный держатель карты выполняет эти транзакции в зарубежной стране, которая не является страной выдачи карты.

В результате, поскольку провайдер финансовой услуги отклонил транзакцию, он обычно входит в контакт с держателем карты, для подтверждения, была ли данная транзакция фактически мошеннической. Это выполняется либо вручную операторами центра по борьбе с мошенничеством, что является очень дорогостоящим, или электронным путем, используя услуги дальней связи, некоторые из которых могут быть неэффективными и дорогостоящими. Во многих случаях, однако, из-за длительного времени, требуемого провайдеру финансовой услуги для исследования данного процесса, держатель карты сам входит в контакт непосредственно с провайдером финансовой услуги (из-за границы) и пытается решить проблему.

Такой подход далек от удовлетворительного, поскольку стоимость разговоров по телефону с провайдером финансовой услуги из-за границы может быть предельно высокой. Кроме того, разность во временных зонах между странами может означать, что держатель карты не будет иметь возможности контакта с провайдером финансовой услуги, если в стране, где была выдана карта, в данный момент не рабочее время.

## СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Изобретение определено в его различных аспектах и в приложенной формуле изобретения, на которую должна быть сделана ссылка.

В соответствии с одним аспектом настоящего изобретения, способ получения данных вероятности, относящихся к действительности запрашиваемой финансовой транзакции, содержит следующие этапы: принимают данные местоположения, относящиеся к запрашиваемой транзакции; принимают данные, идентифицирующие устройство мобильной связи, ассоциированное с лицом, запрашивающим транзакцию; определяют из регистра исходного местоположения (HLR) данные местоположения устройства мобильной связи для устройства мобильной связи; сравнивают данные местоположения, относящиеся к транзакции, с данными местоположения из устройства мобильной связи; и определяют данные вероятности, относящиеся к действительности запрашиваемой транзакции, в зависимости от результата сравнения.

В соответствии с другим аспектом настоящего изобретения, устройство для получения данных вероятности, относящихся к действительности запрашиваемой финансовой транзакции, содержит средство для приема данных местоположения, относящихся к запрашиваемой транзакции; средство для приема данных, идентифицирующих устройство мобильной связи, ассоциированное с лицом, запрашивающим транзакцию; средство для определения из данных регистра исходного местоположения (HLR) для устройства мобильной связи данных местоположения для устройства мобильной связи; средство для сравнения данных местоположения, относящихся к транзакции, с данными местоположения из устройства мобильной связи; и средство для определения данных вероятности, относящихся к действительности запрашиваемой транзакции, в зависимости от результата сравнения.

Предпочтительные варианты осуществления изобретения обеспечивают получение данных вероятности, относящихся к действительности запрашиваемой финансовой транзакции, путем приема данных местоположения, относящихся к запрашиваемой транзакции; прием данных, идентифицирующих устройство мобильной связи, ассоциированное с лицом, запрашивающим транзакцию; определение из данных регистра исходного местоположения (HLR) для устройства мобильной связи данных местоположения для устройства мобильной связи; сравнение данных местоположения, относящихся к транзакции, с данными местоположения из устройства мобильной связи; и определение данных вероятности, относящихся к действительности запрашиваемой транзакции, в зависимости от результата сравнения.

Это позволяет определять вероятность легитимности транзакции для обеспечения для банка выдачи лучшего определения, следует ли разрешить или отклонить транзакцию. Это означает, что возникает меньшее количество ложноположительных определений транзакций, предоставляются улучшенные услуги для держателя карты, и уменьшаются затраты для банка выдачи.

## ПОДРОБНОЕ ОПИСАНИЕ ПРЕДПОЧТИТЕЛЬНЫХ ВАРИАНТОВ ОСУЩЕСТВЛЕНИЯ

Вариант осуществления изобретения описан ниже, только в качестве примера, со ссылкой на приложенные чертежи, на которых:

на фиг.1 показана схема архитектуры системы в соответствии с вариантом осуществления изобретения; и

на фиг.2 показана блок-схема последовательности операций, представляющая основные этапы, выполняемые вариантом осуществления изобретения.

Как показано на фиг.1, система предотвращения ложноположительного определения содержит сервер или компьютер 101. Сервер или компьютер 101 определяют, является ли транзакция, вероятно, мошеннической или нет, как описано более подробно ниже. Система может дополнительно содержать агрегатор 103 данных мобильной сети; мобильные сети 105, 106, устройство мобильной связи (не показано), банк 107 и клиента 109. Кроме того, система может также содержать систему 111 принятия решения, хотя этот признак не является существенным, и, таким образом, она представлена пунктирными линиями на фиг.1. Основные этапы, выполняемые вариантом осуществления изобретения, будут описаны ниже.

Как показано на фиг.2, пользователь вначале начинает транзакцию со средством для выполнения или осуществления транзакции на этапе 201. Средство для выполнения транзакции может представлять собой ATM или PoS. Если транзакция запрашивается в ATM, пользователь вставляет карту в ATM и вводит свой PIN. В качестве альтернативы, если транзакция запрашивается из PoS, то пользователь может физически передать эту

карту продавцу, который вставляет карту в считывающее устройство карты для обработки. Пользователь, в случае необходимости, может вводить PIN, если карта представляет собой карту с микросхемой или PIN. Другие схемы проверки, такие как подпись, также могут использоваться в качестве альтернативы или в дополнение к PIN. Во всех случаях карта содержит данные, ассоциированные с индивидуумом или пользователем, которые позволяют идентифицировать счет пользователя. Обычно эта информация представлена в форме последовательности десятичных чисел.

ATM или PoS затем связывается с провайдером 107 финансовой услуги (сторона, выдавшая карту) на этапе 203, и банк выдачи или провайдер 107 финансовой услуги начинает процесс авторизации. При этом провайдер финансовой услуги принимает запрос на транзакцию на этапе 205. ATM или PoS передает информацию, обеспечивающую возможность определить идентичность держателя карты. Такая информация может содержать номер карты и может быть передана с помощью обычного средства или с использованием средства беспроводной связи, как известно специалисту в данной области техники. Информация также может быть передана в любой соответственно зашифрованной форме, известной специалисту в данной области техники.

После того как банк или провайдер 107 финансовой услуги примет запрос на транзакцию, он может, в случае необходимости, выполнить дополнительную обработку для определения (используя программные механизмы управления риском или собственную логику), является ли транзакция, вероятно, мошеннической, например, если транзакция касается большой суммы денег. Однако если провайдер 107 финансовой услуги определяет, что транзакция, вероятно, является действительной, тогда он может перейти непосредственно к процессу авторизации на этапе 217, разрешая транзакцию на этапе 219. Если провайдер финансовой услуги определяет, что транзакция, вероятно, является мошеннической, то он передает запрос в сервер 101.

Однако если провайдер финансовой услуги не выполняет эту дополнительную обработку, то он передает информацию о транзакции непосредственно в сервер 101.

В одном варианте осуществления сервер 101 может быть расположен в пределах организации провайдера финансовой услуги. Однако в предпочтительных вариантах осуществления сервер 101 установлен физически отдельно от провайдера финансовой услуги, и информация транзакции (например, номер карты или/и имя, или/и сумму транзакции) передается с использованием беспроводного канала связи или обычной проводной технологии в сервер 101.

В одном варианте осуществления сервер 101 затем выделяет информацию кода страны, содержащуюся в информации транзакции, на этапе 207.

В альтернативном варианте осуществления провайдер финансовой услуги выделяет информацию кода страны из информации транзакции. Провайдер финансовой услуги может также назначать номер ссылки для транзакции. Это представляет преимущество, состоящее в том, что потенциально чувствительную финансовую информацию, такую как номер карты, не требуется передавать в сервер 101.

Провайдер финансовой услуги затем выполняет поиск в базе данных клиентов или в справочной таблице информации, идентифицирующей устройство мобильной связи, как показано в Таблице 1.

Таблица 1

Часть справочной таблицы в банке выдачи

| Имя держателя карты | Номер карты | Номер телефона |
|---|---|---|
| Мистер А. Смит | 5432 1234 5678 9998 | 00 44 7981 123 789 |
| Мистер А. Смит | 5432 1234 5678 9999 | 00 44 7981 123 789 |

| | | |
|---|---|---|
| Мистер Н. Джонс | 5432 1234 0123 4567 | 00 44 7981 567 831 |

Он выполняет это, используя идентификационную информацию держателя карты (например, номер карты) для поиска в справочной таблице. Справочная таблица содержит идентификационную информацию держателя карты для каждого держателя карты и информацию, обеспечивающую возможность определения устройства мобильной связи держателя карты. Идентификационная информация держателя карты для каждого пользователя ассоциирована, по меньшей мере, с одной частью информации, обеспечивающей возможность определения устройства связи держателя карты. Если устройство мобильной связи представляет собой портативный телефон, то эта информация может представлять собой (уникальный) телефонный номер портативного телефона, связанного с пользователем, выполняющим транзакцию. Кроме того, каждый держатель карты может иметь больше, чем одну запись в справочной таблице, поскольку он может иметь более, чем одну карту у провайдера финансовой услуги.

Провайдер финансовой услуги затем передает информацию, идентифицирующую устройство мобильной связи, а также выделенный код страны (то есть, местоположение), относящийся к транзакции, в сервер 101. Предпочтительно, также передается ссылочный номер транзакции. Это может представлять собой произвольный номер, назначаемый для транзакции провайдером финансовой услуги. Эта информация может быть передана в зашифрованной форме.

Сервер 101 принимает информацию, идентифицирующую устройство мобильной связи (номер мобильного телефона), от клиента 109 из банка выдачи, затем он выполняет поиск в HLR из коммерчески доступной базы данных. База данных HLR поддерживается каждым провайдером мобильной сети и содержит информацию о постоянных абонентах этого провайдера. В эту информацию включен сетевой код страны, который назначен в данный момент абоненту для использования абонентами, находящимися в роуминге. База данных HLR часто обновляется для учета изменений положения пользователя.

Сервер 101 выполняет поиск HLR, открывая один или более каналов связи в агрегатор 103 данных мобильной сети, на этапе 209. Агрегатор данных сети содержит информацию HLR для устройств мобильной связи, зарегистрированных у провайдера мобильной сети. Агрегатор данных сети может иметь данные HLR более чем одного провайдера 105, 106 услуги мобильной сети. Это представляет собой преимущество, состоящее в том, что нет необходимости каждый раз отдельно запрашивать провайдера услуги для получения данных HLR об устройствах мобильной связи, зарегистрированных у разных провайдеров услуг.

Агрегатор 103 данных сети имеет возможность выделить индикатор мобильного кода страны (MCC) для каждого постоянного абонента в базе данных регистра собственных абонентов (HLR) мобильной сети абонента, на этапе 211, используя информацию, обеспечивающую для устройства связи держателя карты возможность его определения (то есть, номер мобильного телефона). Код MCC, ассоциированный с информацией, идентифицирующей устройство мобильной связи (номер телефона), затем передается на сервер 101.

Сервер 101 затем сравнивает принятый индикатор страны, содержащийся в транзакции ATM или PoS (находящимися за границей) с принятым индикатором мобильного кода страны (MCC).

На этапе 213 рассчитывают вероятность того, что транзакция является легитимной. Существует множество способов, с помощью которых это может быть выполнено. Самый простой способ, с помощью которого детектируют легитимную транзакцию, состоит в проверке соответствия выделенного кода страны, в которой происходит

транзакция, определенному индикатору MCC. Например, транзакция с выделенным кодом страны, относящимся к Австралии, будет иметь высокую вероятность легитимности, если определенный индикатор MCC также отнесется к Австралии. В этом случае транзакция, вероятно, будет легитимной, поскольку, весьма вероятно, что легитимный держатель карты находится в том же или аналогичном местоположении, где расположено его устройство мобильной связи. Для легитимизации транзакции легитимный держатель карты, выполняющий транзакцию, вероятно, должен иметь устройство мобильной связи с собой. В этом случае, местоположение транзакции будет, по существу, тем же, что и местоположение устройства мобильной связи пользователя.

Данные HLR устройства мобильной связи могут быть определены, используя технологии, известные специалисту в данной области техники, например, используя мобильную сеть GSM (Глобальная система мобильной связи) или используя мобильные сети 3-го поколения. Это позволяет определять положение устройства мобильной связи с точностью, по меньшей мере, 50 м.

В одном варианте осуществления система может быть выполнена таким образом, что транзакцию определяют как действительную, только если определенное таким образом местоположение устройства мобильной связи находится в пределах определенного расстояния от местоположения, где возникает транзакция, например, 50 или 100 м.

В альтернативном варианте осуществления система выполнена таким образом, что транзакцию определяют как действительную, только если устройство мобильной связи определяется как находящееся в том же городе или в штате, или в стране, что и место, где происходит транзакция. Этот вариант осуществления является полезным, поскольку пользователи карт часто оставляют мобильные устройства дома или в отеле при выполнении транзакции.

В некоторых случаях, код страны транзакции не будет соответствовать индикатору MCC, даже при том, что транзакция осуществляется легитимным пользователем. Это может происходить, если транзакция происходит в месте, близком к границе страны, например, границе Франции и Германии. В этом случае, если индикатор MCC определен, как находящийся близко к границе, транзакция может быть разрешена даже при том, что код страны транзакции и индикатор MCC не соответствуют друг другу, при условии, что транзакция происходит в стране, которая является соседней (то есть, в пределах заданного расстояния) со страной, соответствующей коду, определенному с использованием MCC.

Система также может определять вероятность того, что транзакция является мошеннической, на этапе 213, вместо просто определения, является ли транзакция действительной (1) или мошеннической (0). В этом случае для транзакции может быть назначено число между 0 и 1.

В одном варианте осуществления вероятность того, что транзакция является мошеннической, больше, когда расстояние между местоположением транзакции и устройством мобильной связи пользователя велико.

На этапе 215 запрос на транзакцию обновляют, используя определенное значение вероятности, например, 0,9 (что означает, что существует 90% вероятности того, что транзакция является действительной) или используя все число, например, 1 или 0 (что означает, что транзакция была определена со 100%-ой вероятностью, что она является действительной или мошеннической). Вероятность затем передают в банк или провайдеру 101 финансовой услуги, как часть информации транзакции, и на этапе 217 банк или провайдер финансовой услуги разрешает или отклоняет транзакцию, в

зависимости от определенной вероятности. Если транзакции разрешена, она выполняется на этапе 219.

Таким образом, варианты осуществления изобретения уменьшают количество транзакций с ложноположительным определением.

Последствия уменьшения количества ложноположительных определений представляют собой потенциальное увеличение детектирования истинных положительных определений (мошеннических транзакций), разрешая отклонить большее количество подозрительных транзакций. Под истинно положительными мы понимаем мошеннические транзакции, отклоненные из-за того, что они были идентифицированы, как потенциально мошеннические. Поэтому, варианты осуществления изобретения, для достижения максимальной эффективности, требуют, чтобы держатель карты имел с собой и активировал свои устройства мобильной связи (мобильные телефоны), находясь за рубежом (хотя и не обязательно лично имел их при себе), и также требует, чтобы банк выдачи регистрировал точную информацию мобильного телефона в своих базах данных держателей карт. Такая тенденция все чаще используется из-за увеличения случаев ложноположительных определений из-за границы и активно поощряется банками. Ассоциация систем клиринговых платежей (APACS) рекомендует держателям карт удостоверяться, что их компания, выдавшая карту, имеет обновленные детали контакта с ними, включающие в себя номер мобильного телефона, в частности, при поездках за границу.

В дополнительном варианте осуществления предусмотрен автоматизированный процесс принятия решения на этапе 221, однако он является необязательным. Это позволяет немедленно и автоматически принимать решения для любой транзакции, отклоненной из-за того, что она имеет низкую вероятность легитимности (потенциально мошеннической транзакция). Процесс автоматизированного принятия решения позволяет прогнозировать, является ли отклонение истинно-положительным определением (мошеннической транзакция) или ложноположительным (легитимная транзакция). В зависимости от результата, автоматизированный процесс принятия решения соединяет держателя карты непосредственно с банком или провайдером финансовой услуги (то есть, департаментом по борьбе с мошенничеством) для разрешения проблемы с мошеннической картой и любой предыдущей мошеннической транзакцией. В качестве альтернативы, он позволяет обновлять информацию держателя карты и просит держателя карты повторно передать отклоненную транзакцию. Поскольку процесс принятия решения может происходить непосредственно после отклонения транзакции, это ускоряет весь процесс, обеспечивает лучшее впечатление для клиента и обеспечивает возможность для держателя карты повторно попытаться выполнить транзакцию, в случае ложноположительного определения, сразу же после первоначальной отклоненной транзакции.

В вариантах осуществления изобретения используется информация HLR совместно с представленными на карте данными финансовой транзакции для прогнозирования вероятности легитимности. Использование базы данных HLR для определения местоположения в стране абонента имеет преимущества над такими методами, как отслеживание широты/долготы, в том, что касается стоимости, временных характеристики и конфиденциальности. Варианты осуществления изобретения обеспечивают идентификацию большего количества действительных положительных финансовых транзакций, выполняемых из-за границы при предъявлении карты, одновременно уменьшая количество ложноположительных транзакций.

Варианты осуществления изобретения также позволяют идентифицировать

неправильные номера мобильных телефонов (те, которые больше не используются), применяя информацию HLR, исключая, таким образом, ошибки обработки. Это также позволяет идентифицировать такие номера и обеспечивает для провайдера финансовой услуги возможность запрашивать новые телефонные номера держателя карты. Варианты осуществления изобретения могут выполняться как услуга, размещенная на чужом сервере, или внутри учреждения. Хотя варианты осуществления изобретения были описаны со ссылкой на финансовые карты, фактически нет необходимости определять какую-либо карту при выполнении транзакции. Например, пользователь может использовать биометрическую информацию, такую как отпечаток (отпечатки) пальцев или сканирование сетчатки глаза в качестве уникального идентификатора своего счета при одновременном предоставлении информации авторизации. Информация авторизации может представлять собой дополнительный PIN или может быть представлена самой биометрической информацией.

В других вариантах осуществления для пользователя может быть предоставлена уникальная кодовая комбинация и/или номер PIN, для ввода в ATM. Это позволяет его провайдеру финансовой услуги предоставлять для пользователя наличные деньги из ATM без необходимости использования физической карты. Снятые наличные деньги затем дебетуются со счета пользователя, который идентифицируется с использованием уникального кода.

Следует понимать, что настоящее изобретение найдет применение при определении действительности или аутентичности любой транзакции, попытка которой выполняется через ATM или PoS, или любое другое средство, для выполнения транзакции. Транзакция может представлять собой финансовую транзакцию. Кроме того, варианты осуществления изобретения могут быть воплощены в аппаратных средствах или в программных средствах. Варианты осуществления могут быть выполнены в ATM или в PoS, или в другом средстве для выполнения транзакции, хотя предпочтительно выполнять систему в централизованном компьютере или в сервере 101. В дополнение к использованию информации базы данных регистра исходного местоположения, система 101 может использовать информацию базы данных регистра посещаемого местоположения. Эти базы данных могут называться базами данных регистра местоположения (LR).

В одном варианте осуществления данные местоположения, относящиеся к месту, в котором запрашивается финансовая транзакция, могут содержать данные, идентифицирующие регион, где запрашивается транзакция. Например, варианты осуществления изобретения могут использовать индикатор кода страны ATM или индикатор кода страны PoS. Такие индикаторы страны финансовой транзакции могут представлять собой этикетки, такие как "UK" или "44" и могут использоваться для идентификации определенного региона, но не содержат достаточную информацию, для определения, где этот регион расположен, или даже, где в данном регионе расположен или установлен ATM или PoS.

Кроме того, данные местоположения устройства мобильной связи могут содержать данные, идентифицирующие регион, где расположено устройство мобильной связи.

Например, в вариантах осуществления изобретения может использоваться индикатор мобильного кода страны (MCC), такой как "UK" или "44". Сервер 101 может выделять индикатор мобильного кода страны из данных регистра исходного местоположения. Сервер 101 может выделять индикатор мобильного кода страны из данных LR или из номеров мобильных устройств, в которых используются данные, идентифицирующие устройство мобильной связи, которое связано с лицом, запрашивающим транзакцию.

Данные LR, соответствующие мобильному устройству пользователя, запрашивающего транзакцию, затем могут анализироваться для извлечения индикатора кода страны. Например, поиск поля "MCC" в базе данных LR выявит соответствие, и значение данных, ассоциированное с этим соответствием, представляет собой значение MCC или индикатор. Данные, идентифицирующие устройство мобильной связи, могут представлять собой номер мобильного телефона или другую информацию абонента, такую как Международный идентификатор мобильного абонента (IMSI).

Данные, идентифицирующие регион, где расположено устройство мобильной связи, могут представлять собой этикетку, такую как "UK" или "44" и использоваться для идентификации определенной области, где расположено устройство, но не содержат достаточную информацию для определения, где расположен этот регион или даже, где в этом регионе находится или размещено устройство.

Использование данных, идентифицирующих регион, вместо самих данных определения местоположения, обеспечивает преимущества, состоящие в том, что сервер 101 не знает положение устройства мобильной связи, поэтому поддерживается конфиденциальность пользователя. Сервер 101 знает только значение его идентификатора, который представляет определенный регион. Например, если устройство мобильной связи пользователя расположено в пределах Великобритании, данные, идентифицирующие регион, где расположено мобильное устройство, могут представлять собой номер, такой как "44". Такая информация не позволяет определять положение устройства мобильной связи.

Далее, используя данные, идентифицирующие регион, вместо самих данных о местоположении, обеспечивается преимущество, состоящее в том, что сервер 101 или компьютер не знают положение или место размещения ATM или PoS, где пользователь пытается сделать транзакции. Таким образом, также обеспечивается преимущество, состоящее в том, что поддерживается конфиденциальность пользователя.

Кроме того, индикатор или данные, идентифицирующие регион, где запрашивается финансовая транзакция, не являются уникальными. То есть, всем ATM или PoS в пределах определенного географического региона назначается определенный индикатор страны, такой как "44".

Кроме того, индикатор или данные, идентифицирующие регион, где расположено устройство мобильной связи, ассоциированное с пользователем, запрашивающим транзакцию, также не являются уникальными. То есть, индикатор страны мобильного телефона, назначенный определенному телефону, не является уникальным, и при этом множество мобильных телефонов в определенном регионе или стране совместно использует один и тот же код.

Использование индикаторов, которые не являются уникальными, имеет преимущество, состоящее в том, что упрощается этап сравнения данных, идентифицирующих регион, где запрашивается финансовая транзакция, с данными, идентифицирующими регион, где расположено устройство мобильной связи.

Это связано с тем, что нет необходимости определять расстояние ATM или PoS от устройства мобильной связи, например, используя положение (x1, y1, z1) мобильного устройства и положение (x2, y2, z2) ATM или PoS. При этом требуется только сравнить данные или идентификатор региона, где расположен ATM или PoS, с данными или идентификатором региона, где расположено устройство мобильной связи. Это упрощает и, следовательно, улучшает время отклика системы. Это также является предпочтительным для повышения конфиденциальности пользователя.

Транзакция может быть удостоверена или определена, как аутентичная, если

идентификатор региона, где располагается ATM или PoS, соответствуют идентификатору региона, где расположено устройство мобильной связи.

В некоторых странах также могут быть предусмотрены дополнительные идентификаторы региона, в которых расположено мобильное устройство. Например, для транзакций в пределах Соединенных Штатов Америки, данные, идентифицирующие регионы, где располагается мобильное устройство, также могут содержать идентификатор города или штата. Этот идентификатор также размещается в данных HLR. Однако такие идентификаторы города или штата также не являются уникальными, поскольку множеству мобильных устройств может быть назначен один и тот же идентификатор города или штата. Кроме того, идентификаторы города или штата могут не содержать достаточную информацию для обеспечения возможности определения местоположения региона, занимаемого городом или штатом, или фактически для определения, в каком месте в пределах региона города или штата расположено мобильное устройство.

Как описано выше в вариантах осуществления изобретения прием данных HLR может осуществляться из агрегатора мобильной сети. Кроме того, транзакция может представлять собой транзакцию с предъявлением карты или транзакцию без предъявления карты, или транзакцию из-за границы. Данные местоположения устройства мобильной связи могут быть приняты из более чем одного сетевого агрегатора. Данные LR могут содержать данные от более чем одного провайдера услуги мобильной сети. Кроме того, вероятность легитимности запрашиваемой транзакции может быть определена в режиме реального времени или после авторизации.

Кроме того, в вариантах осуществления изобретения транзакция может быть отклонена, если определенная вероятность легитимности ниже заданного значения. Данные вероятности также можно использовать для идентификации ложноположительных транзакций. Информация о транзакции и данные, идентифицирующие устройство мобильной связи, могут быть приняты от провайдера финансовой услуги. Способ также может содержать этап автоматического контакта с человеком, запрашивающим транзакцию, например, по телефону.

Варианты осуществления изобретения также могут содержать этап управления средством для выполнения транзакции, в зависимости от результата сравнения. Этот этап может представлять собой альтернативу этапу аутентификации транзакции, в зависимости от результата сравнения.

Например, если данные, идентифицирующие регион, где запрашивается транзакция, соответствуют данным, идентифицирующим регион, где расположено устройство мобильной связи, ATM или PoS, или другим средством для выполнения транзакции можно управлять таким образом, что наличные деньги будут выданы, или этот PoS выполнит транзакцию.

## Формула изобретения

1. Способ аутентификации транзакции, содержащий этапы:

приема (205) запроса транзакции;

обработки запроса транзакции, чтобы определить, может ли запрос транзакции быть одобрен без дополнительной обработки; и

разрешения (217) транзакции, если определено, что запрос транзакции может быть одобрен без дальнейшей обработки;

причем, если определено, что запрос транзакции не может быть одобрен без дальнейшей обработки, способ дополнительно содержит:

прием (207) данных, идентифицирующих регион, где запрашивается транзакция;

определение (211) из регистра местоположения (LR) данных, полученных от провайдера мобильной сети для устройства мобильной связи, ассоциированного с лицом, запрашивающим транзакцию, причем данные идентифицируют регион, где расположено устройство мобильной связи;

сравнение (213) данных, идентифицирующих регион, где запрашивается транзакция, с данными, идентифицирующими регион, где расположено устройство мобильной связи; и

если сравниваемые данные региона совпадают, разрешение (217) транзакции или, если данные региона не совпадают, не разрешение транзакции без дополнительной верификации аутентичности;

причем данные, идентифицирующие регион, где расположено устройство мобильной связи, содержит данные мобильного кода страны (MCC) или данные, идентифицирующие штат или город, а данные, идентифицирующие регион, где запрашивается транзакция, содержат данные страны транзакции или данные, идентифицирующие штат или город.

2. Способ по п.1, дополнительно содержащий этап приема данных, идентифицирующих устройство мобильной связи, ассоциированное с лицом, запрашивающим транзакцию.

3. Способ по п.1 или 2, дополнительно содержащий этап приема (209) данных LR для мобильного устройства, ассоциированного с лицом, запрашивающим транзакцию.

4. Способ по п.2, в котором данные, идентифицирующие устройство мобильной связи, ассоциированное с лицом, запрашивающим транзакцию, используют для определения региона, где расположено устройство мобильной связи, из данных LR.

5. Способ по п.1, дополнительно содержащий этап извлечения данных, идентифицирующих регион, где запрашивается транзакция, из данных транзакции, принимаемых из средства для выполнения транзакции, путем поиска данных транзакции.

6. Способ по п.1, в котором данные LR содержат данные регистра исходного местоположения или данные регистра посещаемого местоположения.

7. Способ по п.1, в котором данные LR принимают из агрегатора мобильной сети, хранящего данные LR множества мобильных устройств, зарегистрированных у разных провайдеров мобильной услуги.

8. Способ по п.1, в котором транзакция выполняется между двумя регионами.

9. Способ по п.1, в котором транзакция выполняется в пределах одного региона.

10. Способ по п.1, причем, если сравниваемые данные региона не совпадают, способ дополнительно содержит этапы

отклонения (217) транзакции и

установления (221) соединения между устройством мобильной связи пользователя, запрашивающего транзакцию, и провайдером услуги транзакции,

причем соединение осуществляют через голосовую телефонную связь в режиме реального времени или с использованием службы коротких сообщений (SMS).

11. Способ по п.1, в котором данные, идентифицирующие регион, где запрашивается транзакция, и данные, идентифицирующие регион, где расположено устройство мобильной связи, принимают от провайдера финансовой услуги или из средства для выполнения транзакции.

12. Способ по п.1, дополнительно содержащий этап управления средством для выполнения транзакции в зависимости от результата сравнения.

13. Система для аутентификации транзакции, содержащая:

сервер (107) финансовых услуг, сконфигурированный, чтобы:

принимать (205) запрос транзакции;

обрабатывать запрос транзакции, чтобы определять, может ли запрос транзакции быть одобрен без дополнительной обработки; и

разрешать (217) транзакцию, если определено, что запрос транзакции может быть одобрен без дальнейшей обработки, и сервер (101) снижения ложноположительного определения, сконфигурированный, если определено, что запрос транзакции не может быть одобрен без дальнейшей обработки, чтобы:

принимать (207) данные, идентифицирующие регион, где запрашивается транзакция;

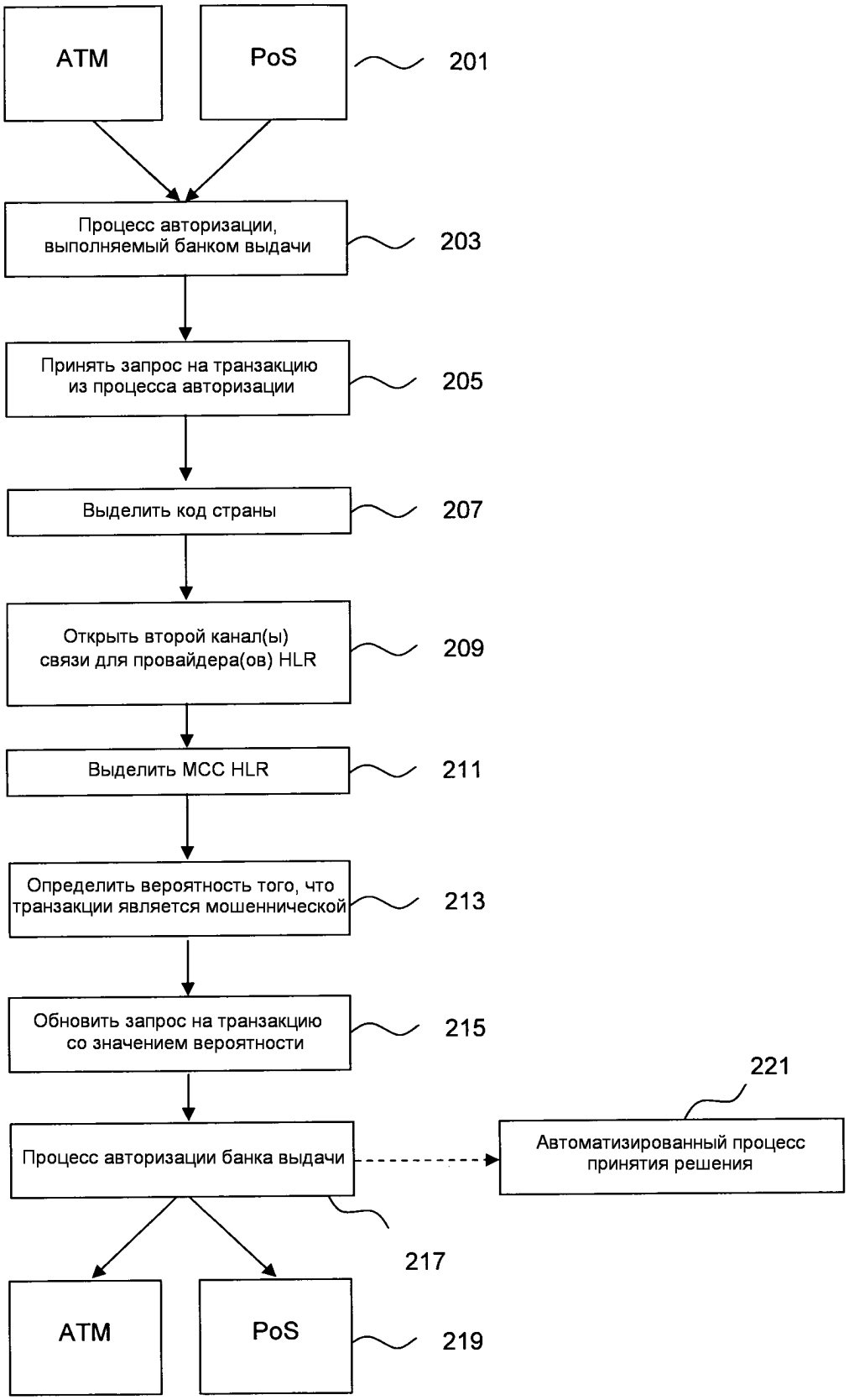
определять (211) из регистра местоположения (LR) данные, полученные от провайдера мобильной сети для устройства мобильной связи, ассоциированного с лицом, запрашивающим транзакцию, причем данные идентифицируют регион, где расположено устройство мобильной связи;

сравнивать (213) данные, идентифицирующие регион, где запрашивается транзакция, с данными, идентифицирующими регион, где расположено устройство мобильной связи; и

если сравниваемые данные региона совпадают, разрешать (217) транзакцию или, если данные региона не совпадают, не разрешать транзакцию без дополнительной верификации аутентичности;

причем данные, идентифицирующие регион, где расположено устройство мобильной связи, содержат данные мобильного кода страны (MCC) или данные, идентифицирующие штат или город, а данные, идентифицирующие регион, где запрашивается транзакция, содержат данные страны транзакции или данные, идентифицирующие штат или город.

14. Система по п.13, дополнительно сконфигурированная для выполнения способа по любому из пп.2-12.


ATM
PoS
201
Процесс авторизации, выполняемый банком выдачи
203
Принять запрос на транзакцию из процесса авторизации
205
Выделить код страны
207
Открыть второй канал(ы) связи для провайдера(ов) HLR
209
Выделить MCC HLR
211
Определить вероятность того, что транзакции является мошеннической
213
Обновить запрос на транзакцию со значением вероятности
215
221
Автоматизированный процесс принятия решения
Процесс авторизации банка выдачи
217
ATM
PoS
219

ФИГ. 2