РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 691 590**(13) **C2**

(51) МПК
G06Q 20/38 (2012.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06Q 20/38 (2019.02)

(21)(22) Заявка: **2016146744, 29.04.2015**

(24) Дата начала отсчета срока действия патента:
29.04.2015

Дата регистрации:
14.06.2019

Приоритет(ы):
(30) Конвенционный приоритет:
30.04.2014 US 61/986,558

(43) Дата публикации заявки: **31.05.2018** Бюл. № **16**

(45) Опубликовано: **14.06.2019** Бюл. № **17**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **30.11.2016**

(86) Заявка PCT:
US 2015/028364 (29.04.2015)

(87) Публикация заявки PCT:
WO 2015/168333 (05.11.2015)

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

(72) Автор(ы):
ЛАМ Джер-Веи (SG)

(73) Патентообладатель(и):
ВИЗА ИНТЕРНЭШНЛ СЕРВИС АССОСИЭЙШН (US)

(56) Список документов, цитированных в отчете о поиске: **US 2008/283591 A1, 20.11.2008. US 2012/0143754 A1, 07.06.2012. RU 2413991 C2, 10.03.2011. RU 2232418 C2, 10.07.2004.**

(54) СИСТЕМЫ И СПОСОБЫ ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ ИЗ ДАННЫХ

(57) Реферат:

Изобретение относится к средствам идентификации платежных данных и замены или удаления секретной информации из платежных данных защищенным устройством считывания карт. Техническим результатом является обеспечение предотвращения подделки доверительных данных в целях фальсификации и защиты от мошенничества, обеспечение быстрой идентификации мошеннических действий и идентификация источника мошеннического использования. Способ содержит признаки: устройством считывания осуществляется: прием данных от платежного устройства, идентификация, замена или удаление секретной информации из второй части данных устройства путем замены по меньшей мере части секретной информации данными для обнаружения мошенничества и подача первой части данных устройства и второй части данных устройства на хост-компьютер, имеющий связь с устройством считывания. Способ замены и удаления секретной информации раскрывает процесс замены и

RU 2691590 C2

RU 2691590 C2

удаления, реализуемый защищенным устройством считывания. 3 н. и 17 з.п. ф-лы, 11 ил.

RU 2691590 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 691 590**(13) **C2**

(51) Int. Cl.
G06Q 20/38 (2012.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06Q 20/38 (2019.02)

(21)(22) Application: **2016146744, 29.04.2015**

(24) Effective date for property rights:
29.04.2015

Registration date:
14.06.2019

Priority:
(30) Convention priority:
30.04.2014 US 61/986,558

(43) Application published: **31.05.2018** Bull. № **16**

(45) Date of publication: **14.06.2019** Bull. № **17**

(85) Commencement of national phase: **30.11.2016**

(86) PCT application:
US 2015/028364 (29.04.2015)

(87) PCT publication:
WO 2015/168333 (05.11.2015)

Mail address:
129090, Moskva, ul. B.Spasskaya, 25, stroenie 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
LAM Dzher-Vei (SG)

(73) Proprietor(s):
VIZA INTERNESHNL SERVIS ASSOSIEJSHN (US)

RU 2691590 C2

(54) SYSTEMS AND METHODS OF REPLACING OR REMOVING SECRET INFORMATION FROM DATA

(57) Abstract:

FIELD: data processing.

SUBSTANCE: invention relates to means of identifying payment data and replacing or removing secret information from payment data by a secure card reader. Method comprises the following features: a reading device: receiving data from a payment device, identifying, replacing or removing secret information from a second part of device data by replacing at least a portion of secret information with fraud detection data and providing a first portion of device data and a second data portion of the device to a host computer having communication with the reading device. Method of replacing and removing secret information discloses a replacement and removal process implemented by a secure reading device.

EFFECT: ensuring prevention of counterfeit of confidential data for the purpose of falsification and protection against fraud, provision of fast identification of fraudulent actions and identification of source of fraudulent use.

20 cl, 11 dwg

RU 2691590 C2

ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА РОДСТВЕННЫЕ ЗАЯВКИ

[0001] Эта заявка согласно 35 USC 119(e) испрашивает приоритет предварительной заявки на патент № 61/986 558, поданной 30 апреля 2014, раскрытие которой с помощью ссылки включено в данный документ во всей своей полноте для всех целей.

УРОВЕНЬ ТЕХНИКИ ИЗОБРЕТЕНИЯ

[0002] Настоящее изобретение относится к замене или удалению секретной информации из платежных данных. На некоторых рынках продавцы могут использовать отдельные устройства для получения авторизации для платежных транзакций и для отслеживания данных покупателя. Например, некоторые продавцы могут использовать терминалы электронного сбора данных, предоставленные эмитентами (например, банками), чтобы получать от эмитентов разрешение на платежные транзакции. Отдельный компьютер продавца может быть использован для отслеживания данных покупателя для целей расчетов или определения лояльности. Поскольку терминалы электронного сбора данных и компьютер продавца не интегрированы, это может привести к событию, именуемому «двойное проведение». Двойное проведение может относиться ко второму проведению платежной карты на терминале продавца после первого проведения для получения начального разрешения от банка. Второе проведение обычно выполняют для отслеживания детальной информации о потребителе в системе продавца, для целей расчетов или определения лояльности. Второе проведение может раскрыть все данные с платежной карты и часто выполняется на менее защищенном терминале продавца. Эти менее защищенные терминалы затем могут стать целью взлома или электронного подслушивания с целью получения данных карты. Это может повредить целостность платежной системы и подорвать доверие покупателей к работе продавца.

[0003] Варианты осуществления настоящего изобретения устраняют эти и другие недостатки, вместе и по отдельности.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0004] Варианты осуществления настоящего изобретения предусматривают системы и способы идентификации платежных данных и замены или удаления секретной информации из платежных данных с помощью защищенного устройства считывания карт. Например, покупатель может выполнить первое проведение платежной карты в кассовом терминале продавца для получения от эмитента разрешения на финансовую транзакцию. Продавец может затем выполнить второе проведение платежной карты на защищенном устройстве считывания карт для отслеживания данных покупателя. Согласно некоторым вариантам осуществления настоящего изобретения защищенное устройство считывания карт может идентифицировать платежные данные, заменять или удалять секретную информацию из платежных данных и подавать данные, в которых была заменена или удалена секретная информация, на компьютер продавца. Данные, в которых была заменена или удалена секретная информация, могут содержать часть платежных данных, которая может отличаться от данных до замены или удаления секретной информации. В некоторых вариантах осуществления защищенное устройство считывания карт может заменять или удалять секретную информацию только из доверительной части платежных данных, чтобы предотвращать подделку доверительных данных в целях фальсификации.

[0005] Согласно одному аспекту предлагается способ, включающий в себя прием устройством считывания данных устройства от платежного устройства; идентификацию устройством считывания первой части данных устройства и второй части данных устройства, содержащей секретную информацию; замену или удаление секретной

информации устройством считывания второй части данных устройства с целью удаления секретной информации путем замены по меньшей мере части секретной информации данными для обнаружения мошенничества; подачу устройством считывания первой части данных устройства и второй части данных устройства, в которой была заменена или удалена секретная информация, на компьютер продавца, соединенный по связи с устройством считывания.

[0006] В некоторых вариантах осуществления первая часть данных устройства может содержать номер основного счета или платежный токен, связанный с номером основного счета. Вторая часть данных устройства может содержать доверительные данные. Доверительные данные могут содержать код проверки подлинности карты (CVV). Данные для обнаружения мошенничества могут указывать продавца, терминал продавца, местоположение или временную информацию, связанную с данными устройства.

[0007] В некоторых вариантах осуществления замена или удаление секретной информации из второй части данных устройства дополнительно включает в себя замену второй части данных устройства нулями.

[0008] В некоторых вариантах осуществления способ дополнительно включает в себя генерирование сообщения с запросом авторизации на основании данных устройства и передачу сообщения с запросом авторизации на компьютер эквайера, имеющий связь с устройством считывания.

[0009] Согласно другому аспекту предлагается способ, включающий в себя прием устройством считывания данных устройства от платежного устройства; идентификацию устройством считывания первой части данных устройства, содержащей номер основного счета или платежный токен, связанный с номером основного счета, и второй части данных устройства, содержащей секретную информацию; замену или удаление секретной информации устройством считывания из второй части данных устройства с целью удаления секретной информации; и подачу устройством считывания первой части данных устройства и второй части данных устройства, в которой была заменена или удалена секретная информация, на устройство, имеющее связь с устройством считывания.

[0010] В некоторых вариантах осуществления замена или удаление секретной информации из второй части данных устройства включает в себя замену по меньшей мере некоторой части второй части данных устройства нулями. В некоторых вариантах осуществления замена или удаление секретной информации второй части данных устройства включает в себя замену по меньшей мере некоторой части секретной информации данными для обнаружения мошенничества. Данные для обнаружения мошенничества могут содержать идентификатор продавца или идентификатор устройства. В некоторых вариантах осуществления секретная информация содержит доверительные данные.

[0011] В некоторых вариантах осуществления устройство считывания карт не приспособлено передавать запрос авторизации платежа. В некоторых вариантах осуществления устройство считывания является частью по меньшей мере одного из терминала продавца, двери номера в отеле или регистрационного киоска авиалинии.

[0012] Согласно другому аспекту предлагается защищенное устройство считывания, содержащее процессор и компьютерно-читаемый носитель, связанный с процессором, компьютерно-читаемый носитель содержит код, вызывающий выполнение процессором: приема данных устройства с платежного устройства; идентификации первой части данных устройства, содержащей номер основного счета или платежный токен, связанный с номером основного счета, и второй части данных устройства, содержащей секретную

информацию; замены или удаления секретной информации из второй части данных устройства с целью удаления секретной информации; и подачи первой части данных устройства и второй части данных устройства, в которой была заменена или удалена секретная информация, на устройство, имеющее связь с защищенным устройством считывания.

[0013] В некоторых вариантах осуществления замена или удаление секретной информации из второй части данных устройства включает в себя замену по меньшей мере некоторой части второй части данных устройства нулями. В некоторых вариантах осуществления замена или удаление секретной информации второй части данных устройства включает в себя замену по меньшей мере некоторой части секретной информации данными для обнаружения мошенничества. Данные для обнаружения мошенничества могут содержать идентификатор продавца или идентификатор устройства. В некоторых вариантах осуществления секретная информация содержит доверительные данные.

[0014] В некоторых вариантах осуществления код дополнительно вызывает выполнение процессором генерирования сообщения с запросом авторизации на основании данных устройства; и передачи сообщения с запросом авторизации на компьютер эквайера, имеющий связь с защищенным устройством считывания.

[0015] Эти и другие варианты осуществления настоящего изобретения более подробно описаны ниже.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0016] На фиг. 1 показана иллюстративная система для замены или удаления секретной информации из данных согласно вариантам осуществления.

[0017] На фиг. 2 более подробно показано защищенное устройство считывания карт и компьютер продавца согласно вариантам осуществления.

[0018] На фиг. 3 показана другая иллюстративная система для замены или удаления секретной информации из данных согласно вариантам осуществления.

[0019] На фиг. 4 более подробно показан интегрированный POS-терминал и компьютер продавца согласно вариантам осуществления.

[0020] На фиг. 5 показан иллюстративный способ замены или удаления секретной информации из платежных данных согласно вариантам осуществления.

[0021] На фиг. 6 показан другой иллюстративный способ замены или удаления секретной информации из платежных данных согласно вариантам осуществления.

[0022] На фиг. 7 показан другой иллюстративный способ замены или удаления секретной информации из платежных данных согласно вариантам осуществления.

[0023] На фиг. 8 показан иллюстративный способ для осуществления отслеживания счета потребителя согласно вариантам осуществления.

[0024] На фиг. 9 показана таблица с примерами замены или удаления секретной информации из некоторых частей платежных данных согласно вариантам осуществления.

[0025] На фиг. 10 показана структурная схема, представляющая систему обработки транзакций согласно одному варианту осуществления настоящего изобретения.

[0026] На фиг. 11 показана блок-схема вычислительного устройства.

ПОДРОБНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

[0027] Варианты осуществления настоящего изобретения предусматривают системы и способы идентификации платежных данных и замены или удаления секретной информации из платежных данных с помощью защищенного устройства считывания карт. Например, покупатель может выполнить первое проведение платежной карты в

кассовом терминале продавца для получения от эмитента разрешения на финансовую транзакцию. Продавец может затем выполнить второе проведение платежной карты на защищенном устройстве считывания карт для отслеживания данных покупателя. Согласно некоторым вариантам осуществления настоящего изобретения защищенное устройство считывания карт может идентифицировать платежные данные, заменять или удалять секретную информацию из платежных данных и подавать данные, в которых была заменена или удалена секретная информация, на компьютер продавца. Данные, в которых была заменена или удалена секретная информация, могут содержать часть платежных данных, которая может отличаться от данных до замены или удаления секретной информации. В некоторых вариантах осуществления защищенное устройство считывания карт может заменять или удалять секретную информацию только из доверительной части платежных данных, чтобы предотвращать подделку доверительных данных в целях фальсификации. В некоторых вариантах осуществления замена или удаление секретной информации может включать в себя замену секретной информации данными для обнаружения мошенничества, такими как идентификатор продавца или идентификатор устройства продавца, так чтобы способствовать обнаружению мошенничества.

[0028] В большинстве случаев, когда осуществляется двойное проведение, второе проведение не связано с авторизацией или проведением транзакции, но применяется для создания вторичной записи для поддержки учета продавца, отчетности или программ управления взаимоотношениями с потребителями (например, лояльности или вознаграждений). Однако второе проведение платежной карты может подвергнуть опасности полные данные дорожек, закодированные в магнитной полосе платежной карты. Например, полные данные дорожек могут содержать данные дорожки 1 и дорожки 2 для финансовых карт. Дорожка 1 может содержать номер основного счета (PAN), имя покупателя, дату истечения срока действия, служебный код и доверительные данные, такие как код проверки подлинности карты (CVV) или проверочный код карты (CVC) и любые другие соответствующие данные. PAN может соответствовать стандарту ISO 7812 и содержать часть с идентификационным номером эмитента (IIN) или идентификационным кодом банка (BIN), и часть с номером личного счета. Данные дорожки 2 могут содержать PAN, дату истечения срока действия, служебный код и доверительные данные, как в дорожке 1, и любые другие соответствующие данные. POS-терминал может считывать данные дорожки 1 и/или данные дорожки 2. Например, в большинстве случаев номер основного счета может соответствовать номеру кредитной карты, напечатанному на платежной карте, и может иметь длину 19 символов. Дата истечения срока действия может иметь длину 4 символа, и CVV или CVC могут иметь длину 3 символа. На менее защищенных компьютерах продавца, которые уязвимы к постороннему вмешательству, данные дорожки могут быть подвержены риску мошенничества, например в целях получения поддельных платежных карт.

[0029] Согласно вариантам осуществления настоящего изобретения защищенное устройство считывания карт может идентифицировать данные платежной карты (например, формата ISO 7813), полученные с платежного устройства, и может заменять или удалять секретную информацию из платежных данных до предоставления платежных данных на компьютер продавца. Например, часть платежных данных может содержать доверительные данные, такие как CVV или CVC, которые могут быть нужны для создания поддельной карты. В некоторых вариантах осуществления замена или удаление секретной информации из данных может включать в себя изменение значения CVV или CVC на некоторое предопределенное значение, такое как нули. Благодаря замене или

удалению секретной информации из платежных данных (таких как доверительные данные), считанных защищенным устройством считывания карт, в результате атак, например, с применением USB-кейлоггеров или программных кейлоггеров, нельзя получить полные данные дорожек, таким образомЮ предотвращая фальсификацию платежных карт с использованием этих данных. Например, неуполномоченный субъект, который получает данные, в которых была заменена или удалена секретная информация, может быть в состоянии извлечь лишь некоторую информацию (например, номер личного счета или токен), но не всю необходимую информацию (например, доверительные данные, такие как CVV), которую требуют сети обработки платежей и/или эмитенты для авторизации платежных транзакций. Кроме того, замена или удаление секретной информации может включать в себя замену секретной информации данными для обнаружения мошенничества, такими как идентификатор продавца или идентификатор устройства продавца, чтобы способствовать обнаружению мошенничества. Например, неуполномоченный субъект, который получает и использует такие данные, в которых была заменена или удалена секретная информация, в качестве платежных данных, может быть легко определен. Данные, в которых была заменена или удалена секретная информация, могут быть поданы на компьютер продавца, который может быть использован конечной системой продавца для обработки, связанной с программами лояльности, расчетами, контролем возвратов и т. п. Варианты осуществления настоящего изобретения могут быть использованы с существующими POS-устройствами без каких-либо обновлений в программном/аппаратном обеспечении POS.

[0030] Перед обсуждением вариантов осуществления настоящего изобретения для понимания вариантов осуществления настоящего изобретения может быть полезным описание некоторых терминов.

[0031] «Устройство доступа» может представлять собой любое подходящее устройство для доступа к удаленному компьютеру. В некоторых вариантах осуществления настоящего изобретения устройство доступа может осуществлять связь с компьютером продавца или сетью обработки платежей и может взаимодействовать с портативным устройством, вычислительным устройством пользователя и/или мобильным устройством пользователя. Устройство доступа может в целом быть расположено в любом подходящем месте, таком как местоположение продавца. Устройство доступа может иметь любую подходящую форму. В некоторых примерах устройства доступа включают в себя устройства в точке продаж (POS), устройства считывания карт, сотовые телефоны, карманные персональные компьютеры, персональные компьютеры (PC), планшетные компьютеры, специализированные ручные устройства чтения, приставки, электронные кассовые аппараты (ECR), автоматические кассовые машины (ATM), виртуальные кассовые аппараты (VCR), киоски, системы безопасности, системы доступа, веб-сайты и т. п. Устройство доступа может использовать любой подходящий контактный или бесконтактный режим работы для отправки или приема данных от портативного устройства, или связанных с ним данных. В некоторых вариантах осуществления, в которых устройство доступа может содержать POS-терминал, может быть использован любой подходящий POS-терминал, и он может содержать устройство считывания, процессор и компьютерно-читаемый носитель. Устройство считывания может иметь любой подходящий контактный или бесконтактный режим работы. Например, для взаимодействия с портативным устройством иллюстративные устройства считывания карт могут содержать радиочастотные (RF) антенны, оптические сканеры, устройства считывания штрих-кодов или устройства

считывания магнитных полос.

[0032] «Замена или удаление секретной информации» может включать в себя удаление или изменение секретной информации. Например, замена или удаление секретной информации из данных может включать в себя удаление секретной информации из данных путем изменения данных. В некоторых вариантах осуществления в частях полных данных дорожек, считанных из платежного устройства, может быть заменена или удалена секретная информация. В некоторых вариантах осуществления замена или удаление секретной информации из данных может включать в себя замену частей данных предопределенным значением (таким как нули или цифробуквенная последовательность), или идентификатором, который может быть использован для идентификации, по отдельности или в сочетании, имени продавца, местоположения, терминала продавца или даты и времени. Например, в некоторых вариантах осуществления данные, в которых была заменена или удалена секретная информация, могут содержать все 7-ки, соответствующие продавцу A, или все 5-ки, соответствующие продавцу B. В некоторых вариантах осуществления данные, в которых была заменена или удалена секретная информация, могут включать в себя идентификатор (например, цифробуквенную последовательность), который содержит идентификатор продавца и идентификатор терминала в местоположении продавца. В некоторых вариантах осуществления данные, в которых была заменена или удалена секретная информация, могут относиться к конкретной части платежных данных, которая была изменена (например, платежные данные могут содержать первую часть, которая не была изменена, и часть, в которой была заменена или удалена секретная информация, которая была заменена предопределенным значением). В некоторых вариантах осуществления данные, в которых была заменена или удалена секретная информация, могут относиться к любым платежным данным, в которых по меньшей мере часть данных была удалена или заменена. В некоторых случаях замена или удаление секретной информации из части данных приводит к невозвратному удалению или стиранию данных. Удаленные или стертые данные не могут быть восстановлены на основании данных, в которых была заменена или удалена секретная информация. Такие способы замены или удаления секретной информации могут включать в себя замену данных значениями, которые не имеют связи с замененными данными (например, нулями, случайными величинами, идентификаторами продавца), или усечение данных или шифрование данных и уничтожение криптографического ключа. В других случаях замена или удаление секретной информации части данных делает данные недоступными для неуполномоченных субъектов, но доступными или восстановимыми для уполномоченных субъектов. Например, данные могут быть зашифрованы с помощью криптографического ключа, который доступен только для уполномоченных субъектов. Неуполномоченные субъекты не будут иметь возможности расшифровать зашифрованные данные без криптографического ключа, тогда как уполномоченные субъекты будут иметь возможность расшифровать данные с помощью криптографического ключа, а значит и восстановить данные.

[0033] «Платежное устройство» может относиться к любому устройству, которое может быть использовано для проведения финансовой транзакции, так чтобы предоставлять платежную информацию продавцу. Платежное устройство может иметь любую подходящую форму. Например, подходящие платежные устройства могут быть ручными и компактными, так что они могут помещаться в кошельке и/или кармане покупателя (*например*, они могут быть карманного формата). Они могут включать в себя смарт-карты, карты с магнитной полосой, устройства типа брелока (такие как

Speedpass™, поставляемые на рынок компанией Exxon-Mobil Corp.) и т. п. Другие примеры платежных устройств включают в себя сотовые телефоны, карманные персональные компьютеры (PDA), пейджеры, платежные карты, карты безопасности, карты доступа, флеш-карты, ретрансляторы, двумерные штрих-коды, электронный или цифровой кошелек и т. п. Если платежное устройство имеет форму дебетовой, кредитной или смарт-карты, платежное устройство также необязательно может иметь такие признаки как магнитные полосы. Такие устройства могут работать или в контактном, или в бесконтактном режиме. Данные устройства могут относиться к любой информации, полученной из платежного устройства.

[0034] «Платежные данные» могут включать в себя данные, связанные с платежной транзакцией. Платежные данные могут быть использованы (например, эмитентом) для подтверждения или отклонения транзакции. Платежные данные включают в себя данные устройства, собранные с платежного устройства (например, кредитной карты или банковской карты) и/или у держателя карты. Например, платежные данные могут включать в себя данные дорожек, закодированные в магнитных полосах платежного устройства. Платежные данные также могут включать в себя данные аутентификации, предоставленные самими потребителями, такими как подпись, личный идентификационный номер (PIN), или защитный код (например, код проверки подлинности карты 2, или CVV 2). В одном примере платежные данные могут включать в себя номер расчетного счета (PAN), дату истечения срока действия, имя покупателя, личный идентификационный номер, значение CVV или CVC и т. п. В некоторых вариантах осуществления первая часть данных может включать в себя недоверительные данные, а вторая часть данных может включать в себя доверительные данные. В некоторых вариантах осуществления доверительные данные могут включать в себя имя, номер ключа проверки Pin-кода (PVKI, 1 символ), проверочное значение PIN-кода (PVV, 4 символа), код проверки подлинности карты или проверочный код карты (CVV или CVC, 3 символа). В некоторых вариантах осуществления недоверительные данные могут включать в себя номер расчетного счета (PAN) или токен (описан ниже), номер счета лояльности и т. п.

[0035] «Секретные платежные данные» могут включать в себя часть платежных данных, которая требует замены или удаления секретной информации перед передачей, хранением и/или обработкой. Например, секретные платежные данные могут включать в себя секретные данные аутентификации, хранящиеся в поле доверительных данных дорожки. Такие секретные данные аутентификации могут включать в себя PVKI, PVV и CVV или CVC, обычно хранящиеся в дорожке 1 и/или дорожке 2 платежной карты. В некоторых других случаях секретные платежные данные могут включать в себя идентифицирующую информацию держателя карты или счета, такую как имя держателя карты.

[0036] «Токен» может включать в себя заменяющий идентификатор для информации. Например, платежный токен может включать в себя идентификатор для расчетного счета, который является заменой идентификатора счета, такого как номер основного счета (PAN). Например, токен может включать в себя ряд цифробуквенных символов, который может быть использован в качестве замены оригинального идентификатора счета. Например, токен «4900 0000 0000 0001» может быть использован вместо PAN «4147 0900 0000 1234». В некоторых вариантах осуществления токен может быть «сохраняющим формат» и может иметь численный формат, который соответствует идентификаторам счетов, используемым в существующих сетях обработки платежей (например, формат сообщения финансовой транзакции ISO 8583). В некоторых вариантах

осуществления токен может быть использован вместо PAN для запуска, авторизации, проведения или принятия платежной транзакции. Токен также может быть использован для представления оригинальных регистрационных данных в других системах, где обычно предоставляются оригинальные регистрационные данные. В некоторых вариантах осуществления значение токена может быть сгенерировано так, что восстановление оригинального PAN или другого идентификатора счета по значению токена не может быть произведено вычислительным путем. Кроме того, в некоторых вариантах осуществления формат токена может иметь такую конфигурацию, чтобы позволять субъекту, принимающему токен, идентифицировать его как токен и распознавать субъект, который эмитировал токен.

[0037] «Данные для обнаружения мошенничества» могут включать в себя любые данные, идентифицирующие конкретный субъект или этап, вовлеченные в данную транзакцию или процесс, так чтобы позволять обнаружение мошенничества или опасности на конкретном субъекте этапа. Например, данные для обнаружения мошенничества могут включать в себя информацию, указывающую, когда и/или где происходит данная операция над данными. Операция над данными может включать в себя передачу, прием, обработку, хранение или извлечение данных. Операция над данными может включать в себя замену или удаление секретной информации из данных, как описано в данном документе. Данные обнаружения мошенничества могут включать в себя информацию, идентифицирующую субъект (например, субъект предпринимательства и/или вычислительное устройство), связанный с данной операцией над данными. Такая информация, идентифицирующая субъект, может включать в себя, например, идентификатор продавца, который уникальным образом идентифицирует продавца (например, цифробуквенная последовательность, содержащая имя или идентификатор), код категории продавца (MCC), местоположение продавца, идентификатор устройства или терминала, который уникальным образом идентифицирует терминал или устройство (например, POS-терминал продавца) и т. п. Данные для обнаружения мошенничества также могут включать в себя информацию о местоположении и/или времени (например, метку времени), связанную с определенными операциями над данными.

[0038] «Защищенное устройство считывания карт» может включать в себя защищенное устройство для считывания платежных карт. Например, в некоторых вариантах осуществления защищенное устройство считывания карт может представлять собой устройство, выполненное с возможностью считывания платежных данных с платежного устройства и замены или удаления секретной информации из части платежных данных. В некоторых вариантах осуществления замена или удаление секретной информации из части платежных данных может включать в себя изменение значения этой части платежных данных. Например, значение может быть изменено на другое значение, например, все нули. Защищенное устройство считывания карт может быть выполнено с возможностью замены по меньшей мере части секретных платежных данных на данные для обнаружения мошенничества.

[0039] «Сообщение с запросом авторизации» может представлять собой электронное сообщение, которое отправляют на сеть обработки платежей и/или эмитенту платежной карты с целью запроса разрешения на транзакцию. Сообщение с запросом авторизации согласно некоторым вариантам осуществления может соответствовать ISO 8583, который является стандартом для систем, которые обмениваются информацией электронных транзакций, связанных с платежом, сделанным покупателем с помощью платежного устройства или расчетного счета. Сообщение с запросом авторизации

может содержать идентификатор счета эмитента, который может быть связан с платежным устройством или расчетным счетом. Сообщение с запросом авторизации также может содержать дополнительные элементы данных, соответствующие «идентифицирующей информации», включающей в себя, только для примера: служебный код, CVV (код проверки подлинности карты), dCVV (динамический код проверки подлинности карты), PAN (номер основного счета или «номер счета»), токен (например, заменитель PAN), имя пользователя, дату истечения срока действия и т. п. Сообщение с запросом авторизации также может содержать «информацию транзакции», такую как любая информация, связанная с текущей транзакцией, такой как сумма транзакции, идентификатор продавца, местоположение продавца, идентификационный номер банка эквайера (BIN), ID акцептанта карты и т. п., а также любую другую информацию, которая может быть использована при определении, следует ли идентифицировать и/или разрешать транзакцию.

[0040] «Сообщение с ответом на авторизацию» может представлять собой ответ в электронном сообщении на сообщение с запросом авторизации, сгенерированное финансовой организацией-эмитентом или сетью обработки платежей. Сообщение с ответом на авторизацию может включать в себя, только для примера, один или несколько из следующих индикаторов состояния: «подтверждение» -транзакция была подтверждена; «отклонение» -транзакция не была подтверждена; или «вызов центра» - ответ, для которого требуется больше информации, причем продавец должен позвонить по бесплатному телефонному номеру для авторизации. Сообщение с ответом на авторизацию также может включать в себя код авторизации, который может представлять собой код, который выдавший кредитную карту банк возвращает в ответ на сообщение с запросом авторизации в электронном сообщении (или прямо, или через сеть обработки платежей) на устройство доступа продавца (например, POS-оборудование), которое обозначает подтверждение транзакции. Указанный код может служить подтверждением авторизации.

[0041] Различные другие приложения, функции и преимущества представлены ниже в отношении разных вариантов осуществления. Следует понимать, что описание и графические материалы представляют ряд примеров, но альтернативы и изменения, возможные в рамках разных вариантов осуществления, не описаны полностью. Альтернативы и изменения, однако, будут очевидны среднему специалисту в данной области техники в свете указаний и предложений, содержащихся в данном документе.

[0042] На фиг. 1 показана иллюстративная система 100 для замены или удаления секретной информации из данных согласно вариантам осуществления. Система 100 может содержать платежное устройство 102, терминал 104 в точке продажи (POS-терминал), компьютер 106 эквайера, сеть 108 обработки платежей, компьютер 110 эмитента, защищенное устройство 112 считывания карт и компьютер 114 продавца.

[0043] Платежное устройство 102 может быть использовано покупателем для проведения финансовой транзакции. Платежное устройство 102 может иметь форму платежной карты (например, дебетовые карты, кредитные карты, карты лояльности, предоплаченные карты и т. п.) или мобильного устройства (например, сотовые телефоны, ноутбуки, планшеты, карманные персональные компьютеры (PDA), устройства типа брелоков и т. п.). В некоторых вариантах осуществления платежное устройство 102 может быть выполнено с возможностью связи с одной или несколькими беспроводными сетями (например, сотовыми сетями, Wi-Fi и т. п.). Например, если платежное устройство 102 представляет собой мобильный телефон, оно может быть выполнено с возможностью связи с мобильной сетью.

[0044] В некоторых вариантах осуществления настоящего изобретения платежное устройство 102 может представлять собой платежное устройство на основе чипа, например, карту с чипом типа EMV (Europay, MasterCard® и Visa®). Например, платежное устройство 102 может включать в себя платежную карту с встроенным микропроцессорным чипом, в дополнение к стандартным магнитным полосам. Встроенный чип может защищать и хранить данные держателя карты. Покупатель (например, держатель карты) может быть аутентифицирован с помощью PIN-кода или подписи, с целью выполнения транзакции с помощью его карты с чипом.

[0045] Терминал 104 в точке продажи (POS-терминал) может быть выполнен с возможностью приема платежей, проведенных с помощью платежных устройств, таких как платежное устройство 102. Например, POS-терминал 104 может представлять собой терминал электронного сбора данных (EDC), который может считывать информацию, закодированную в платежной карте на основе чипа EMV, и передавать эту информацию на сеть обработки платежей/эмитенту для авторизации/проведения транзакции. В некоторых вариантах осуществления POS-терминал 104 может иметь форму бесконтактного считывающего устройства, которое может считывать данные чипа EMV на платежном устройстве, когда покупатель проводит или взмахивает платежным устройством вблизи от него. POS-терминал 104 может содержать компьютер, который может быть выполнен с возможностью связи с одним или несколькими субъектами с помощью одной или нескольких сетей связи для авторизации и проведения транзакции. Например, когда покупатель проводит или вставляет платежное устройство 102 в POS-терминал 104, POS-терминал 104 может генерировать сообщение с запросом авторизации и отправлять сообщение с запросом авторизации в сеть 108 обработки платежей через компьютер 106 эквайера. Следует понимать, что в разных вариантах осуществления могут быть использованы разные типы устройств доступа, включая, но без ограничения, POS-терминал.

[0046] Эквайер, как правило, представляет собой систему для субъекта (например, банка), которая управляет счетом конкретного продавца или другого субъекта. Компьютер 106 эквайера может переправлять сообщение с запросом авторизации для транзакции на компьютер 110 эмитента через сеть 108 обработки платежей.

[0047] Сеть 108 обработки платежей может включать в себя подсистемы, сети и операции обработки данных, применяемые для поддержки и доставки услуг авторизации и услуг клиринга и расчетов. Один пример сети 108 обработки платежей включает в себя VisaNet®, используемую Visa®. Сеть 108 обработки платежей может включать в себя проводную или беспроводную сеть, включая Интернет. Сеть 108 обработки платежей может направлять сообщение с запросом авторизации эмитенту 110.

[0048] Эмитент, как правило, представляет собой субъект предпринимательства (например, банк), который мог выдать платежную карту (например, кредитную или дебетовую), номера счетов или платежные токены, используемые для транзакций. Некоторые системы могут выполнять функции как эмитента, так и эквайера. Когда транзакция включает в себя расчетный счет, связанный с компьютером 110 эмитента, компьютер 110 эмитента может подтвердить счет и ответить сообщением с ответом на авторизацию на компьютер 106 эквайера через сеть 108 обработки платежей, которая может направить его на POS-терминал 104. Сообщение с ответом на авторизацию может включать в себя идентификатор для описания того, была транзакция подтверждена или отклонена. POS-терминал 104 может сообщать покупателю о результате авторизации на основании сообщения с ответом на авторизацию.

[0049] Позднее (например, в конце дня), между компьютером 106 эквайера, сетью

108 обработки платежей и компьютером 110 эмитента может быть выполнен процесс клиринга и расчета.

[0050] Как представлено на фиг. 1, POS-терминал 104 и компьютер 114 продавца не интегрированы или не приспособлены осуществлять связь друг с другом. Следовательно, продавец может быть вынужден выполнять несколько взаимодействий между платежным устройством 102 и разными системами для извлечения соответствующей информации из платежного устройства 102, которая может быть использована этими системами. Каждое дополнительное устройство, которое считывает данные с платежного устройства 102, представляет собой потенциальную цель, которая в случае несанкционированного доступа может раскрыть данные дорожек, закодированные в платежном устройстве 102. Например, в некоторых вариантах осуществления второе проведение платежного устройства 102 может быть выполнено на защищенном устройстве 112 считывания карт после первого проведения на POS-терминале 104. Например, второе проведение платежной карты может быть проведением магнитной полосы на защищенном устройстве 112 считывания карт. Второе проведение может быть не связано с авторизацией/расчетом и может быть использовано внутренней системой продавца для учета, контроля возвратов, программ лояльности и т. п. Второе проведение платежного устройства 102 может позволять защищенному устройству 112 считывания карт получать платежные данные, связанные со счетом покупателя. Например, платежные данные могут включать в себя полные данные дорожек, закодированные в магнитных полосах платежного устройства 102. В некоторых вариантах осуществления в результате второго проведения платежного устройства 102 можно получить данные о лояльности с полными данными дорожек, связанными со счетом покупателя, или без них. В некоторых вариантах осуществления данные о лояльности могут быть определены по некоторым частям полных данных дорожек (например, PAN). Следует понимать, что данные магнитных полос могут включать в себя закодированные данные, связанные с финансовым счетом покупателя, счетом лояльности, персональным идентификационным счетом, и любые другие подходящие данные, по отдельности или в сочетании, которые могут быть использованы для отслеживания счета покупателя.

[0051] Согласно некоторым вариантам осуществления защищенное устройство 112 считывания карт может не быть приспособлено или запрограммировано передавать запрос авторизации платежа. Скорее, защищенное устройство 112 считывания карт может быть выполнено с возможностью замены или удаления секретной информации из части платежных данных с применением способов, описанных в данном документе. Защищенное устройство 112 считывания карт может быть выполнено с возможностью идентификации первой части платежных данных и второй части платежных данных. Например, первая часть платежных данных может содержать номер расчетного счета или платежный токен, связанный с номером расчетного счета, данные о лояльности, персональный идентификатор или любые другие недоверительные данные, которых самих по себе не может быть достаточно для создания фальшивых карт, но которые могут быть использованы компьютером 114 продавца для учета, ведения отчетности или программ управления взаимодействиями с потребителями. В некоторых вариантах осуществления вторая часть платежных данных может содержать доверительные данные, такие как имя покупателя, CVV или CVC, или любые другие секретные данные. Защищенное устройство 112 считывания карт может быть выполнено с возможностью замены или удаления секретной информации из второй части платежных данных и подачи второй части платежных данных, в которой была заменена или удалена секретная информация, вместе с первой частью платежных данных на компьютер 114 продавца.

Альтернативно или дополнительно вторая часть платежных данных, в которой была заменена или удалена секретная информация, вместе с первой частью платежных данных может быть подана в хранилище данных (не показано), функционально соединенное с защищенным устройством 112 считывания карт и/или компьютером 114 продавца. В некоторых вариантах осуществления вторая часть платежных данных, в которой была заменена или удалена секретная информация, может содержать данные, которые отличаются от данных, полученных защищенным устройством 112 считывания карт из платежного устройства 102. Например, вторая часть платежных данных, в которой была заменена или удалена секретная информация, может содержать предопределенные значения (например, нули) или случайные значения. В качестве другого примера, вторая часть платежных данных, в которой была заменена или удалена секретная информация, может содержать данные для обнаружения мошенничества, такие как идентификатор продавца, идентификатор устройства, метка времени, информация о местоположении и т. п., так чтобы позволять обнаружение и/или отслеживание мошеннической деятельности.

[0052] В некоторых вариантах осуществления защищенное устройство 112 считывания карт может быть выполнено в виде автоматически конфигурируемого устройства, которое может быть подключено к компьютеру продавца, не требуя никаких обновлений компьютерной системы или POS-терминала продавца. Например, защищенное устройство 112 считывания карт может заменить имеющееся устройство считывания карт, не требуя никаких изменений интерфейса. В некоторых вариантах осуществления защищенное устройство 112 считывания карт может быть подключено к компьютеру 114 продавца с помощью существующего USB-соединения, не требуя никаких изменений формата данных для связи с компьютером 114 продавца.

[0053] Компьютер 114 продавца может быть выполнен с возможностью связи с защищенным устройством 112 считывания карт по проводному или беспроводному соединению. Компьютер 114 продавца может принимать платежные данные, которые могут содержать часть, в которой была заменена или удалена секретная информация, и которая не может быть использована в целях фальсификации. Компьютер 114 продавца может использовать первую часть платежных данных, предоставленную защищенным устройством 112 считывания карт, для программ учета и лояльности. Следует понимать, что в разных вариантах осуществления любое подходящее устройство (например, запоминающее устройство, хост-компьютер, серверный компьютер, портативное устройство и т. п.) может быть использовано вместо или в дополнение к компьютеру продавца для получения данных, в которых была заменена или удалена секретная информация, от защищенного устройства считывания карт. Устройство, которое принимает данные, в которых была заменена или удалена секретная информация, может быть или может не быть предоставлено тем же субъектом, что и поставщик защищенного устройства считывания карт.

[0054] На фиг. 2 более подробно представлены защищенное устройство 112 считывания карт и компьютер 114 продавца, представленные на фиг. 1, согласно вариантам осуществления.

[0055] В некоторых вариантах осуществления защищенное устройство 112 считывания карт может иметь гнездо 202, в которое покупатель может вставлять магнитную полосу платежного устройства 102 или проводить ею. В некоторых вариантах осуществления защищенное устройство 112 считывания карт может иметь магнитную считывающую головку, выполненную с возможностью считывания данных магнитной полосы. В некоторых вариантах осуществления мобильным устройством 102 можно взмахнуть

или провести возле защищенного устройства 112 считывания карт. Например, защищенное устройство 112 считывания карт может быть выполнено с возможностью связи с платежным устройством 102 с помощью радиоволн или технологии связи ближнего поля (NFC). Защищенное устройство 112 считывания карт может также содержать процессор и компьютерно-читаемый носитель, соединенный с процессором, причем компьютерно-читаемый носитель может содержать код, вызывающий выполнение процессором способов согласно вариантам осуществления настоящего изобретения. Например, компьютерно-читаемый носитель может содержать код для приема платежных данных от платежного устройства (например, платежного устройства 102), идентификации первой части платежных данных и второй части платежных данных, замены или удаления секретной информации из второй части платежных данных и подачи первой части платежных данных и второй части платежных данных, в которой была заменена или удалена секретная информация, на компьютер 114 продавца, имеющий связь с защищенным устройством 112 считывания карт. Следует понимать, что в разных вариантах осуществления защищенное устройство считывания карт может содержать разные типы устройств доступа или содержаться в них.

[0056] Конфигурация системы, представленная на фиг. 1-2, может быть экономичным образом приспособлена для обеспечения безопасности данных на имеющейся системе транзакций продавца. Стоимость защищенного устройства 112 считывания карт может быть относительно низкой. Кроме того, защищенное устройство 112 считывания карт может быть встроено в существующую систему продавца с внесением небольших изменений в существующие компоненты или без их внесения. Например, защищенное устройство считывания карт может быть выполнено в виде автоматически конфигурируемого устройства, которое может быть подключено к компьютеру продавца, не требуя никаких обновлений компьютерной системы или POS-терминала продавца.

[0057] На фиг. 3 показана другая иллюстративная система 300 для замены или удаления секретной информации из данных согласно вариантам осуществления. Система 300 подобна системе 100, представленной на фиг. 1, за исключением того, что предусмотрен единственный интегрированный POS-терминал 105, который сочетает функции POS-терминала 104 и защищенного устройства 112 считывания карт, представленных на фиг. 1. Например, интегрированный POS-терминал 105 может представлять собой EDC терминал, выполненный с возможностью получения платежных данных для авторизации и расчета. Определенные поля платежных данных (например, полных данных дорожек) могут быть удалены с целью замены или удаления секретной информации из данных. Данные, в которых была заменена или удалена секретная информация, такие как номер счета, могут быть отправлены на кассовый аппарат для расчетных целей без раскрытия полных данных дорожек. Следует понимать, что в разных вариантах осуществления интегрированный POS-терминал может содержать разные типы устройств доступа или содержаться в них.

[0058] Интегрированный POS-терминал 105 может быть выполнен с возможностью обработки платежных транзакций подобно POS-терминалу 104, представленному на фиг. 1. Например, интегрированный POS-терминал 105 может быть выполнен с возможностью приема платежных данных (например, полных данных дорожек) от платежного устройства 102 (посредством проведения или вставки платежного устройства 102 в интегрированный POS-терминал 105), генерирования сообщения с запросом авторизации, отправки сообщения с запросом авторизации в сеть 108 обработки платежей через компьютер 106 эквайера, приема сообщения с ответом на авторизацию

от компьютера 106 эквайера и сообщения результатов авторизации пользователю или компьютеру 114 продавца.

[0059] Интегрированный POS-терминал 105 также может быть выполнен с возможностью подачи платежных данных, в которых была заменена или удалена секретная информация, на компьютер продавца подобно защищенному устройству 112 считывания карт, представленному на фиг. 1. Например, интегрированный POS-терминал 105 может быть выполнен с возможностью идентификации части платежных данных, которая требует замены или удаления секретной информации. В одном варианте осуществления часть платежных данных, подлежащая замене или удалению секретной информации, не содержит PAN или платежного токена, связанного с PAN. PAN или токен могут быть необходимы или требоваться далее по ходу процесса продавцом в целях возврата, учета или отслеживания. В другом варианте осуществления по меньшей мере в части PAN может быть заменена или удалена секретная информация (например, определенные знаки PAN). Интегрированный POS-терминал 105 может быть выполнен с возможностью замены или удаления секретной информации из идентифицированной части данных путем замены части данных по меньшей мере частично данными для обнаружения мошенничества. Данные для обнаружения мошенничества могут содержать информацию, идентифицирующую продавца, местоположение продавца, устройство (например, интегрированный POS-терминал), метку времени и т. п., связанную с обработкой платежных данных. Альтернативно или дополнительно интегрированный POS-терминал 105 может быть выполнен с возможностью замены или удаления секретной информации из идентифицированной части данных путем замены части данных нулями или другими предопределенными значениями. Интегрированный POS-терминал 105 может быть выполнен с возможностью подачи платежных данных, в которых была заменена или удалена секретная информация, на компьютер 114 продавца. Платежные данные, в которых была заменена или удалена секретная информация, могут включать в себя часть платежных данных, в которой не была заменена или удалена секретная информация (например, PAN или токен), и часть платежных данных, в которой была заменена или удалена секретная информация (например, доверительные данные из данных дорожек, которые были заменены нулями или данными для обнаружения мошенничества). В некоторых случаях, когда секретную информацию удаляют или усекают, платежные данные, в которых была заменена или удалена секретная информация, и которые подают на компьютер 114 продавца, могут включать в себя только часть платежных данных, в которой была заменена или удалена секретная информация. Альтернативно или дополнительно платежные данные, в которых была заменена или удалена секретная информация, могут быть поданы в хранилище данных (не показано) или любое подходящее устройство, функционально соединенное с интегрированным POS-терминалом 105 и/или компьютером 114 продавца.

[0060] В разных вариантах осуществления замена или удаление секретной информации из платежных данных может происходить по существу одновременно с авторизацией платежа, перед ней или после нее. Например, когда платежные данные приняты, генерация запроса авторизации может происходить независимо от замены или удаления секретной информации из платежных данных. В другом примере генерация запроса авторизации может происходить перед заменой или удалением секретной информации из платежных данных или после этого.

[0061] Следует понимать, что в разных вариантах осуществления любое подходящее устройство (например, запоминающее устройство, хост-компьютер, серверный компьютер, портативное устройство и т. п.) может быть использовано вместо или в

дополнение к компьютеру продавца для получения данных, в которых была заменена или удалена секретная информация, от интегрированного POS-терминала. Устройство, которое принимает данные, в которых была заменена или удалена секретная информация, может быть или может не быть предоставлено тем же субъектом, что и поставщик интегрированного POS-терминала.

[0062] На фиг. 4 более подробно представлены интегрированный POS-терминал 105 и компьютер 114 продавца, представленные на фиг. 3, согласно вариантам осуществления.

[0063] В некоторых вариантах осуществления интегрированный POS-терминал 105 может иметь гнездо 302, в которое покупатель может вставлять магнитную полосу платежного устройства 102 или проводить ею. В некоторых вариантах осуществления интегрированный POS-терминал 105 может иметь магнитную считывающую головку, выполненную с возможностью считывания данных магнитной полосы. В некоторых вариантах осуществления мобильным устройством 102 можно взмахнуть или провести возле интегрированного POS-терминала 105. Например, интегрированный POS-терминал 105 может быть выполнен с возможностью связи с платежным устройством 102 с помощью радиоволн или технологии связи ближнего поля (NFC). Интегрированный POS-терминал 105 может также содержать процессор и компьютерно-читаемый носитель, соединенный с процессором, причем компьютерно-читаемый носитель может содержать код, вызывающий выполнение процессором способов согласно вариантам осуществления настоящего изобретения. Например, компьютерно-читаемый носитель может содержать код для приема платежных данных от платежного устройства (например, платежного устройства 102), генерирования и отправки сообщения с запросом авторизации, идентификации первой части платежных данных и второй части платежных данных, замены или удаления секретной информации из второй части платежных данных и подачи первой части платежных данных и второй части платежных данных, в которой была заменена или удалена секретная информация, на компьютер 114 продавца, имеющий связь с защищенным устройством 112 считывания карт.

[0064] Конфигурация системы, представленная на фиг. 3, 4, может быть выполнена с возможностью обеспечения авторизации транзакций и замены или удаления секретной информации из данных, не требуя множественного доступа к платежному устройству (например, нескольких проведений карты). В частности, к платежному устройству необходимо осуществить лишь один доступ интегрированным POS-терминалом двойного назначения сразу и для авторизации платежа, и для отслеживания счета. Сокращенное раскрытие данных дорожек может уменьшить риск ошибок транзакции или утечки секретной информации. Кроме того, комплексный подход может сократить общее время обработки (например, время кассового обслуживания).

[0065] Согласно некоторым вариантам осуществления способы, описанные в данном документе, могут быть применены к или интегрированы с разнообразными системами, в которых платежное устройство, содержащее секретную информацию, применяют для не связанных с платежами целей. Например, способы, описанные в данном документе, могут быть реализованы посредством устройства управления доступом, такого как регистрационный киоск или терминал в аэропорте или отеле, замок двери номера в отеле и т. п., с целью идентификации или удостоверения личности держателей карт без раскрытия секретной информации на платежном устройстве. В частности, информация, содержащаяся в платежных данных, может быть предоставлена выборочно по мере необходимости, так что извлекается и предоставляется системе контроля доступа только информация, требующаяся для управления доступом (например, PAN или токен,

связанный с PAN, или номер лояльности), тогда как в остальных данных происходит замене или удаление секретной информации (например, удаление или замена другой несекретной информацией).

[0066] На фиг. 5 показан иллюстративный способ 500 замены или удаления секретной информации из платежных данных согласно вариантам осуществления. В частности, замена или удаление секретной информации из платежных данных может включать в себя замену некоторых секретных данных данными для обнаружения мошенничества. Аспекты способа 500 могут быть выполнены, в некоторых вариантах осуществления, защищенным устройством 112 считывания карт, представленным на фиг. 1-2, или интегрированным POS-терминалом 105, представленным на фиг. 3-4. Некоторые или все аспекты способа 500 (или любых других способов, описанных в данном документе, или их вариантов и/или сочетаний) могут быть выполнены под управлением одного или нескольких компьютеров/систем управления, снабженных выполняемыми командами, и могут быть реализованы в виде кода (например, выполняемых команд, одной или нескольких компьютерных программ или одного или нескольких приложений), выполняемого вместе на одном или нескольких процессорах, аппаратным обеспечением или их сочетанием. Код может храниться в компьютерно-читаемом носителе данных, например, в форме компьютерной программы, содержащей множество команд, выполняемых одним или несколькими процессорами. Компьютерно-читаемый носитель данных может быть постоянным. Порядок, в котором описаны операции, не предназначен для рассмотрения в качестве ограничения, и для осуществления способов любое количество описанных операций можно сочетать в любом порядке и/или параллельно.

[0067] Способ 500 может включать в себя получение 502 платежных данных от платежного устройства. Например, платежные данные могут быть получены защищенным устройством 112 считывания карт, когда платежное устройство 102 проводят или вставляют в гнездо 202 защищенного устройства 112 считывания карт, как показано на фиг. 2. В некоторых вариантах осуществления проведение платежного устройства 102 может быть вторым проведением платежного устройства 102 на защищенном устройстве 112 считывания карт после первого проведения на POS-терминале 104 для выполнения финансовой транзакции. В некоторых других вариантах осуществления защищенное устройство 112 считывания карт может быть интегрировано или функционально соединено с регистрационным киоском или другой системой управления доступом, так что проведение платежного устройства может быть использовано для идентификации и/или аутентификации держателя карты. В другом примере платежные данные могут быть получены интегрированным POS-терминалом 105, когда платежное устройство 102 проводят или вставляют в гнездо 302 интегрированного POS-терминала 105, как показано на фиг. 4.

[0068] Платежные данные могут включать в себя данные дорожек из платежного устройства. Данные дорожек могут включать в себя данные для одной или нескольких дорожек в заданном формате (например, ISO 7813). Например, данные дорожки 1 могут включать в себя недоверительные данные и доверительные данные. Недоверительные данные могут содержать PAN или токен, связанный с PAN, дату истечения срока действия, имя держателя карты и служебный код. Доверительные данные могут включать в себя секретные данные аутентификации, такие как PVKI, PVV, CVV или CVC. Данные дорожки 2 могут содержать PAN или токен, связанный с PAN, дату истечения срока действия, служебный код и доверительные данные, подобные данным дорожки 1. В некоторых вариантах осуществления данные дорожек могут необязательно включать

в себя данные дорожки 3, которые могут содержать доверительные данные и/или недоверительные данные. Например, данные дорожки 3 могут включать в себя информацию о лояльности или другую информацию для отслеживания счета потребителя.

[0069] Способ 500 может включать в себя идентификацию 504 первой части первой части платежных данных и второй части платежных данных, содержащей секретную информацию. Идентификация первой части и второй части платежных данных может включать в себя синтаксический анализ платежных данных согласно особому формату данных (например, ISO 7813), так чтобы извлекать предопределенные части или поля платежных данных. Например, первая часть может содержать недоверительные данные (например, PAN или токен), а вторая часть платежных данных может содержать доверительные данные, в которых может быть нужно заменить или удалить секретную информацию для предотвращения подделки. В другом варианте осуществления вторая часть может также содержать некоторые недоверительные данные (например, PAN или токен, имя, дату истечения срока действия или служебный код).

[0070] Во второй части, которая была идентифицирована, может быть заменена или удалена секретная информация 506 путем замены по меньшей мере некоторой доли второй части данными для обнаружения мошенничества. В некоторых случаях остаток второй части, если имеется, может быть оставлен как есть, заменен нулями или другими предопределенными значениями, или удален. В некоторых других случаях данные для обнаружения мошенничества могут выходить за пределы второй части. Как обсуждалось выше, «данные для обнаружения мошенничества» могут включать в себя любые данные, идентифицирующие конкретный субъект или этап, вовлеченные в данную транзакцию или процесс, так чтобы позволять обнаружение мошенничества или опасности на конкретном субъекте этапа. Например, данные для обнаружения мошенничества могут включать в себя информацию, указывающую, когда и/или где происходит данная операция над данными. Операция над данными может включать в себя передачу, прием, обработку, хранение или извлечение данных. Операция над данными может включать в себя замену или удаление секретной информации из данных, как описано в данном документе. Данные обнаружения мошенничества могут включать в себя информацию, идентифицирующую субъект (например, субъект предпринимательства и/или вычислительное устройство), связанный с данной операцией над данными. Такая информация, идентифицирующая субъект, может включать в себя, например, идентификатор продавца, который уникальным образом идентифицирует продавца, идентификатор устройства или терминала, который уникальным образом идентифицирует терминал или устройство и т. п. Такие идентификаторы устройства могут быть предоставлены или сгенерированы производителями, поставщиками услуг по продаже, продавцами, эквайерами или любыми подходящими субъектами. Примеры идентификатора устройства могут включать в себя идентификатор терминала (TID) или идентификационный номер терминала (TIN), назначенные POS-терминалу или рабочей станции, адрес Интернет-протокола (IP), адрес управления доступом к среде (MAC) и т. п. В некоторых случаях идентификатор устройства может быть получен на основе одного или нескольких параметров аппаратного и/или программного обеспечения устройства, идентифицируемого идентификатором устройства. Данные для обнаружения мошенничества также могут включать в себя информацию о местоположении и/или времени (например, метку времени), связанную с определенными операциями над данными. Данные для обнаружения мошенничества также могут включать в себя информацию, идентифицирующую данные, которыми оперирует

субъект, такие как сводка или цифровая подпись. Данные для обнаружения мошенничества также могут включать в себя другую информацию, такую как информация о транзакции, включая идентификатор транзакции, сумму транзакции и т. п.

[0071] В некоторых вариантах осуществления данные для обнаружения мошенничества могут заменять по меньшей мере часть PAN платежных данных, как часть способа замены или удаления секретной информации. В некоторых вариантах осуществления данные для обнаружения мошенничества, которые используют для замены PAN, могут быть сохраняющими формат, так что получающийся в результате PAN, в котором была заменена или удалена секретная информация, имеет такой же формат, что и обычные PAN. К примеру, часть PAN платежных данных до замены или удаления секретной информации и часть PAN платежных данных после замены или удаления секретной информации могут содержать одинаковое или похожее число знаков (например, 16, 17, 18 или 19 знаков). В одном примере данные для обнаружения мошенничества могут заменять ту часть PAN, которая не содержит IIN или BIN номера PAN, и/или последние четыре знака PAN. Сохраняющие формат данные, в которых была заменена или удалена секретная информация, могут показаться подлинными неуполномоченному субъекту, который затем может попытаться использовать данные, в которых была заменена или удалена секретная информация, для совершения мошенничества. Когда это происходит, данные для обнаружения мошенничества могут быть использованы для быстрой идентификации источника утечки данных. Например, настоящий PAN может быть «4000123456789010», где первые шесть знаков («400012») представляют IIN, а остальные десять знаков («3456789010») представляют номер личного счета. PAN, в котором была заменена или удалена секретная информация, может быть «4000122323239010», где данные для обнаружения мошенничества «232323» применяются для замены той части PAN, которая не содержит IIN, или последних четырех знаков номера личного счета. Данные для обнаружения мошенничества могут идентифицировать конкретного продавца или источник данных. Когда компьютер авторизации, такой как компьютер обработки платежей или компьютер эмитента, получает этот номер в платежной транзакции, компьютер авторизации может автоматически определить, что транзакция является мошеннической, и может, в то же время, быстро определить источник потенциальной утечки данных на основании данных для обнаружения мошенничества. Затем можно предпринять корректирующее действие для защиты данных в источнике данных с потенциальной утечкой или же расследовать, как и когда произошла утечка данных.

[0072] В некоторых вариантах осуществления данные для обнаружения мошенничества могут быть жестко закодированы, например, в аппаратном обеспечении или программно-аппаратном обеспечении. Например, идентификатор устройства может быть сохранен в предоставляемом производителем программируемом постоянном запоминающем устройстве (PROM) POS-терминала или устройства считывания карт. В некоторых других вариантах осуществления данные для обнаружения мошенничества могут быть сгенерированы динамически. Например, данные для обнаружения мошенничества могут содержать цифровую подпись, которую генерируют динамически на основании по меньшей мере части платежных данных. В качестве другого примера, данные для обнаружения мошенничества могут включать в себя случайным образом генерируемый номер, обновляемое значение счетчика или метку времени. Еще в других вариантах осуществления данные для обнаружения мошенничества могут быть получены из других источников, например, из удаленного или локального хранилища данных,

датчика (например, датчика системы глобального позиционирования (GPS)), удаленного устройства управления и т. п. Несколько примеров замены данных данными для обнаружения мошенничества представлены со ссылкой на таблицу на фиг. 9.

[0073] Могут быть предоставлены 508 платежные данные, в которых была заменена или удалена секретная информация, содержащие первую часть, в которой не была заменена или удалена секретная информация, и вторую часть, в которой была заменена или удалена секретная информация. В разных вариантах осуществления платежные данные, в которых была заменена или удалена секретная информация, могут быть предоставлены на любое подходящее устройство или систему для отображения, хранения или обработки. Например, платежные данные, в которых была заменена или удалена секретная информация, могут быть предоставлены на компьютер продавца или систему управления доступом, имеющие связь с защищенным устройством считывания карт. В одном примере первая часть, в которых не была заменена или удалена секретная информация, может содержать PAN или токен, которые являются неизменными, тогда как вторая часть, в которых была заменена или удалена секретная информация, может содержать данные для обнаружения мошенничества, которые заменяют по меньшей мере часть секретной информации, содержащейся во второй части. В другом примере вторая часть может содержать часть PAN или токена, и часть PAN или токена может быть заменена данными для обнаружения мошенничества. Секретная информация, замененная данными для обнаружения мошенничества, не предоставляется. Данные, в которых была заменена или удалена секретная информация, могут быть использованы в целях учета, программ лояльности или управления доступом без раскрытия полных данных дорожек, которые могут быть использованы в целях фальсификации. Кроме того, замена секретной информации по меньшей мере частично данными для обнаружения мошенничества приводит к эффективному использованию пространства, уже распределенного в платежных данных, таким образом позволяя представить больше информации меньшим объемом данных.

[0074] В некоторых вариантах осуществления данные, в которых была заменена или удалена секретная информация, могут быть предоставлены на компьютер авторизации или систему обнаружения мошенничества для обнаружения мошеннических действий на счетах потребителей. Данные для обнаружения мошенничества, которые включены в данные, в которых была заменена или удалена секретная информация, могут быть использованы для быстрой идентификации источника потенциальной утечки данных (например, продавца), таким образом предотвращая и/или сдерживая потенциальное мошенничество. Например, неуполномоченный субъект, который получает данные PAN, в которых была заменена или удалена секретная информация, содержащие некоторые данные для обнаружения мошенничества, может не понять, что в данных была заменена или удалена секретная информация, и попытаться использовать данные, в которых была заменена или удалена секретная информация, в качестве платежных данных для совершения мошенничества. Когда такие данные, в которых была заменена или удалена секретная информация, получает компьютер авторизации, такой как компьютер для обработки платежей или компьютер эмитента, компьютер авторизации может автоматически определить, что транзакция является мошеннической, и может, в то же время, быстро идентифицировать источник потенциальной утечки данных на основании данных для обнаружения мошенничества. Затем можно предпринять корректирующее действие для защиты данных в источнике данных с потенциальной утечкой или же расследовать, как и когда произошла утечка данных. Например, счет потребителя может быть помечен продавцом или эмитентом как потенциально

подверженный риску. Помеченный счет потребителя может быть проконтролирован и/или проанализирован на мошеннические действия. В качестве другого примера, продавец, который был идентифицирован посредством данных для обнаружения мошенничества, может быть помещен в черный список или блокирован для будущих транзакций. В некоторых случаях данные для обнаружения мошенничества могут быть сравнены с известными мошенническими данными, которые указывают на известных продавцов-мошенников или подверженные риску терминалы продавцов, с целью обнаружения мошенничества.

[0075] На фиг. 6 показан другой иллюстративный способ 600 замены или удаления секретной информации из платежных данных согласно вариантам осуществления. В частности, PAN или токен платежных данных может быть исключен из замены или удаления секретной информации. Аспекты способа 500 могут быть выполнены, в некоторых вариантах осуществления, защищенным устройством 112 считывания карт, представленным на фиг. 1-2, или интегрированным POS-терминалом 105, представленным на фиг. 3-4.

[0076] Способ 600 может включать в себя прием 602 платежных данных от платежного устройства способом, подобным описанному на этапе 502 способа 500.

[0077] Способ 600 может включать в себя идентификацию 604 первой части, содержащей PAN или токен, и второй части платежных данных. Идентификация первой части и второй части платежных данных может включать в себя синтаксический анализ платежных данных согласно специальному формату данных (например, ISO 7813), так чтобы извлекать предопределенные части платежных данных. Например, часть PAN или токена может быть идентифицирована как следующая сразу за начальной меткой «%» и кодом формата «B», и перед разделителем «^» в данных дорожки 1, и как следующая сразу за начальной меткой «;» и перед разделителем «=» в данных дорожки 2. Вторая часть может содержать некоторую или всю информацию после части PAN или токена. Например, вторая часть может содержать имя, дату истечения срока действия, служебный код и/или доверительные данные.

[0078] Способ 600 включает в себя замену или удаление секретной информации 606 из второй части без замены или удаления секретной информации из первой части. Первая часть и вторая часть могут обработаны по-разному по нескольким причинам. В некоторых случаях в первой части может не быть заменена или удалена секретная информация, поскольку информацию, содержащуюся в первой части, необходимо сохранить по обоснованным деловым причинам. Например, идентификатор счета, такой как PAN или токен, как правило, необходим далее по ходу процесса (например, компьютеру продавца) в целях возврата, учета или отслеживания. Замена или удаление секретной информации из PAN или токена усложнили бы такие задачи. В некоторых других случаях в первой части может не быть заменена или удалена секретная информация, поскольку информация, содержащаяся в первой части, не является настолько секретной, как информация во второй части. Например, первая часть может содержать токен, который является лишь заменяющим идентификатором для PAN. Раскрытие токена не привело бы к раскрытию лежащего в его основе PAN. В некоторых других случаях в первой части может не быть заменена или удалена секретная информация, поскольку нормативные требования к безопасности данных могут не быть настолько строгими для первой части, как для второй части. Например, соответствие Стандарту безопасности данных отрасли платежных карт (PCI DSS) требует, чтобы секретные данные аутентификации (например, CVV) ни при каких обстоятельствах не сохранялись после авторизации транзакции, тогда как хранение

PAN разрешено в случае шифрования или иной защиты.

[0079] Замена или удаление секретной информации из второй части может включать в себя постоянное исключение доступа к информации во второй части. Постоянное исключение доступа к данным может эффективно предотвратить потенциальное мошенничество с данными. Кроме того, данные во второй части могут быть навсегда удалены, поскольку, как правило, они далее по ходу процесса не требуются (например, в отличие от PAN) для обработки, не связанной с платежами. К примеру, данные аутентификации, такие как CVV, как правило, нужны только для авторизации транзакции, а не в целях возврата, учета, отслеживания, управления доступом или идентификации. В некоторых вариантах осуществления постоянное исключение доступа к информации может включать в себя перезапись по меньшей мере части второй части бесполезными данными (например, нулями или любыми другими символами), перезапись по меньшей мере части второй части полезными данными (например, данными для обнаружения мошенничества), отсечение по меньшей мере части второй части, шифрование по меньшей мере части второй части и «выбрасывание» или уничтожение криптографического ключа, или любое сочетание вышеуказанного. Несколько примеров замены или удаления секретной информации из данных представлены со ссылкой на таблицу на фиг. 9.

[0080] Платежные данные, в которых была заменена или удалена секретная информация, содержащие первую часть, в которой не была заменена или удалена секретная информация, и вторую часть, в которой была заменена или удалена секретная информация, могут быть предоставлены 608, например, на компьютер продавца, локальное или удаленное хранилище данных, или любое другое вычислительное устройство или систему. В целом, платежные данные, в которых была заменена или удалена секретная информация, могут быть предоставлены для отображения, хранения, обработки или иного использования подходящим устройством или системой. В некоторых вариантах осуществления данные, в которых была заменена или удалена секретная информация, могут быть предоставлены на компьютер авторизации или систему обнаружения мошенничества для обнаружения мошеннических действий на счетах потребителей. Например, когда неуполномоченный субъект применяет данные, в которых была заменена или удалена секретная информация, в качестве платежных данных для совершения мошенничества, данные, в которых была заменена или удалена секретная информация, могут быть проанализированы компьютером авторизации для обнаружения мошенничества. Например, просто наличие нулей (или других неверных значений) вместо верных значений в данных, в которых была заменена или удалена секретная информация, может указывать, что данные неправильно используются неуполномоченным субъектом с незаконными целями. После обнаружения мошенничества на основе данных, в которых была заменена или удалена секретная информация, для предотвращения или сдерживания мошенничества могут быть предприняты корректирующие действия. Например, компьютер продавца или компьютер авторизации могут пометить счет потребителя как рискованный или подверженный риску и могут подвергнуть помеченный счет дальнейшему анализу или контролю. Альтернативно или дополнительно данные, в которых была заменена или удалена секретная информация, могут содержать данные для обнаружения мошенничества, которые идентифицируют источник утечки данных (например, продавца), что дополнительно способствует этому обнаружению и/или предотвращению мошенничества. Например, само наличие данных для обнаружения мошенничества может указывать на мошенничество, подобно наличию нулей или других неверных

значений. Например, поле с доверительными данными данных, в которых была заменена или удалена секретная информация, может содержать данные для обнаружения мошенничества вместо CVV, как требуется для авторизации. Дополнительно данные для обнаружения мошенничества могут идентифицировать продавца или терминал продавца, от которых происходит платежная транзакция. Такие идентифицированные продавец или терминал продавца могут быть помещены в черный список или блокированы (например, системой обработки платежей или эмитентом) от будущих транзакций в качестве части корректирующих действий, которые могут быть предприняты для предотвращения дальнейшего мошенничества.

[0081] На фиг. 7 показан другой иллюстративный способ 700 замены или удаления секретной информации из платежных данных согласно вариантам осуществления. Аспекты способа 700 могут быть выполнены, в некоторых вариантах осуществления, интегрированным POS-терминалом 105, представленным на фиг. 3-4, или системой 100, представленной на фиг. 1.

[0082] Способ 700 может включать в себя прием 702 платежных данных способом, подобным описанному на этапе 502 способа 500. Например, покупатель может выполнить первое проведение своей платежной карты на POS-терминале или может взмахнуть или провести своим платежным устройством на бесконтактном считывающем устройстве, чтобы запустить финансовую транзакцию.

[0083] Сообщение с запросом авторизации может быть сгенерировано 704 и передано 706 (например, на компьютер эквайера). В некоторых вариантах осуществления сообщение с запросом авторизации может содержать платежные данные и данные транзакции. Например, данные транзакции могут содержать сумму транзакции, идентификатор продавца, количество единиц товара, дату и время транзакции и любую другую соответствующую информацию. Сообщение с запросом авторизации может быть направлено (например, компьютером эквайера) на сеть обработки платежей, которая может направить сообщение с запросом авторизации на компьютер эмитента для авторизации. Компьютер эмитента может обработать сообщение с запросом авторизации, чтобы определить, следует ли подтвердить или отклонить транзакцию. Компьютер эмитента может сгенерировать сообщение с ответом на авторизацию с результатами авторизации и отправить сообщение с ответом на авторизацию на интегрированный POS-терминал через сеть обработки платежей и компьютер эквайера.

[0084] Платежные данные могут быть подвергнуты замене или удалению секретной информации 708 и предоставлены 710 (например, на компьютер продавца, в хранилище данных или любое другое вычислительное устройство) в целях учета, отслеживания, идентификации, управления доступом и/или обнаружения мошенничества. В некоторых вариантах осуществления этапы 708 и 710 могут быть осуществлены способом, подобным этапам 506 и 508, представленным на фиг. 5, или этапам 606 и 608, представленным на фиг. 6, выше. Например, данные, в которых была заменена или удалена секретная информация, и которые отклоняются от правильных платежных данных, но неправомерно используются в качестве платежных данных, могут быть обнаружены компьютером продавца или компьютером авторизации (например, компьютером обработки платежей или компьютером эмитента) для идентификации неуполномоченного субъекта. Кроме того, когда данные, в которых была заменена или удалена секретная информация, содержат данные для обнаружения мошенничества, данные для обнаружения мошенничества могут быть использованы для дополнительного ускорения процесса обнаружения мошенничества, например, с помощью информации, идентифицирующей продавца. Когда мошенничество обнаружено

на основании данных, в которых была заменена или удалена секретная информация, соответствующим субъектом может быть предпринято любое подходящее корректирующее действие. Например, счет может быть проанализирован, проконтролирован, внесен в черный список или иным образом обработан продавцом, эквайером, обработчиком платежей или эмитентом.

[0085] Порядок, в котором описаны операции, не предназначен для рассмотрения в качестве ограничения, и для осуществления способа 700 любое количество описанных операций можно сочетать в любом порядке и/или параллельно. Например, в некоторых вариантах осуществления этапы 708 и/или 710 могут быть выполнены параллельно с этапами 704 и/или 706. Другими словами, замена или удаление секретной информации из платежных данных может быть выполнено параллельно с обработкой авторизации платежа. В других вариантах осуществления этапы 708 и/или 710 могут быть выполнены перед или после этапов 704 и/или 706.

[0086] На фиг. 8 показан иллюстративный способ 800 осуществления отслеживания счета потребителя согласно вариантам осуществления. Отслеживание счета потребителя может быть выполнено на основе платежных данных, в которых была заменена или удалена секретная информация, таких как описаны в данном документе. Аспекты способа 800 могут быть выполнены, в некоторых вариантах осуществления, компьютером 114 продавца, представленным на фиг. 1 и 3.

[0087] Способ 800 может включать в себя прием 802 платежных данных, в которых была заменена или удалена секретная информация, таких как предоставляются защищенным устройством 112 считывания карт, представленным на фиг. 1-2, или интегрированным POS-терминалом 105, представленным на фиг. 3-4. Платежные данные могли быть подвергнуты замене или удалению секретной информации с помощью способов, описанных в данном документе (например, представленных на фиг. 5-7).

[0088] Способ 800 может включать в себя получение 804 PAN на основе платежных данных, в которых была заменена или удалена секретная информация. Платежные данные, в которых была заменена или удалена секретная информация, могут содержать первую часть, в которой не была заменена или удалена секретная информация, и вторую часть, в которых была заменена или удалена секретная информация. Первая часть платежных данных, в которых была заменена или удалена секретная информация, может содержать PAN или токен. Когда в первой части платежных данных, в которых была заменена или удалена секретная информация, имеется PAN, PAN может быть извлечен. Когда в первой части вместо PAN имеется токен, PAN можно получить на основании токена. Например, токен может быть извлечен из первой части платежных данных, в которых была заменена или удалена секретная информация, и использован для поиска соответствующего PAN на основе карты или другой структуры данных, которая хранит взаимосвязь между токенами и соответствующими PAN. Такая взаимосвязь может храниться в хранилище токенов, поддерживаемом эмитентом токенов, как описано со ссылкой на фиг. 10. Компьютер продавца может осуществлять связь с эмитентом токенов для получения PAN, соответствующего токену. В альтернативном варианте осуществления токен может быть извлечен из первой части платежных данных, в которых была заменена или удалена секретная информация, и использован в целях отслеживания счета потребителя как есть, вместо использования лежащего в его основе PAN.

[0089] Когда платежные данные, в которых была заменена или удалена секретная информация, получают путем замены секретной информации данными для обнаружения мошенничества (как было описано со ссылкой на фиг. 5), способ 800 может

необязательно включать в себя получение 806 данных для обнаружения мошенничества на основании платежных данных, в которых была заменена или удалена секретная информация. Например, данные для обнаружения мошенничества могут быть извлечены из предопределенной части (например, части с доверительными данными) платежных данных, в которых была заменена или удалена секретная информация. Данные для обнаружения мошенничества могут содержать идентификатор продавца, идентификатор устройства, идентификатор местоположения, метку времени и т. п., или любое их сочетание.

[0090] По меньшей мере частично на основании платежных данных, в которых была заменена или удалена секретная информация, можно обновить 808 информацию о счете потребителя. В некоторых вариантах осуществления информация о счете потребителя может быть идентифицирована или извлечена по PAN или платежному токену, связанным со счетом потребителя. Информация о счете потребителя может быть обновлена данными для обнаружения мошенничества (например, идентификатором продавца, идентификатором устройства продавца и т. п.). В некоторых вариантах осуществления платежные данные, в которых была заменена или удалена секретная информация, могут включать в себя другие данные, в которых не была заменена или удалена секретная информация, и которые могут быть извлечены и использованы для обновления информации о счете потребителя. Например, такие данные, в которых не была заменена или удалена секретная информация, могут включать в себя номер программы лояльности, детальную информацию о транзакции (например, сумму транзакции) и т. п. В некоторых случаях данные для обнаружения мошенничества, извлеченные из платежных данных, в которых была заменена или удалена секретная информация, могут быть использованы для определения того, следует ли счет потребителя пометить, приостановить, контролировать или иным образом воздействовать на него. Например, данные для обнаружения мошенничества могут быть сравнены с известными мошенническими данными, которые указывают на известных мошеннических продавцов или подверженные риску терминалы продавцов. Если имеется совпадение, то счет потребителя может быть помечен как потенциально подверженный риску, приостановленный и/или контролируемый на предмет мошеннической активности. В некоторых примерах известные мошеннические данные могут быть получены из хранилища данных или системы обнаружения мошенничества, которые могут иметь связь с устройством, которое получает данные, в которых была заменена или удалена секретная информация.

[0091] На фиг. 9 представлена таблица 900 с примерами замены или удаления секретной информации из некоторых частей платежных данных согласно вариантам осуществления.

[0092] Записи 902 и 904 представляют пример платежных данных, содержащих данные дорожки 1 и дорожки 2 перед заменой или удалением секретной информации и после этого. Как представлено в записи 902, данные дорожки 1 до замены или удаления секретной информации имеют следующий вид: «%B4000123456789010^SMITH/JOHN^160710214738105590102037?», где «4000123456789010» -это PAN или токен, «^»- это разделитель, «СМИТ/ДЖОН» -это имя держателя карты, «1607» -это дата истечения срока действия (июль 2016 года), «102» -это служебный код, а «1473810559010203» -это доверительные данные. Данные дорожки 2 до замены или удаления секретной информации имеют следующий вид: «;4000123456789010=160710212423468?», где «4000123456789010» - это PAN или токен, «=» - это разделитель, «1607» - это дата истечения срока действия (июль 2016 года), «102» - это служебный код, а «12423468» -

это доверительные данные. Иллюстративные данные после замены или удаления секретной информации представлены в записи 904. Первая часть данных дорожек, в которой не заменяют или удаляют секретную информацию, может содержать PAN или токен («4000123456789010»), а вторая часть, в которой заменяют или удаляют секретную информацию, может содержать остальные части данных (например, имя, дату истечения срока действия, служебный код, доверительные данные). Как показано, замена или удаление секретной информации может включать в себя обнуление данных, подлежащих замене или удалению секретной информации. В некоторых вариантах осуществления данные замены или удаления секретной информации могут содержать другие значения.

[0093] Записи 906 и 908 представляют пример платежных данных, содержащих данные дорожки 1, дорожки 2 и дорожки 3 перед заменой или удалением секретной информации и после этого. Как представлено в записи 906, данные дорожки 1 и дорожки 2 могут быть подобны данным дорожки 1 и дорожки 2, представленным в записи 902. Данные дорожки 3 могут содержать данные о лояльности (например, «81293812»), используемые для отслеживания программ лояльности. Как представлено записью 908, в данных дорожки 1 и дорожки 2 может быть заменена или удалена секретная информация подобно замене или удалению секретной информации из данных дорожки 1 и дорожки 2 в примере выше. Однако из данных дорожки 3 может не быть заменена или удалена секретная информация, поскольку они не содержат секретной информации. Таким образом, в этом примере данные после замены или удаления секретной информации содержат только PAN или токен, и данные о лояльности, которых не может быть достаточно для целей фальсификации в случае, если компьютер продавца станет мишенью кейлоггера или хакера.

[0094] Запись 910 представляет иллюстративные данные дорожки 1 и дорожки 2 после замены или удаления секретной информации, где секретная информация заменена данными для обнаружения мошенничества. Данные для обнаружения мошенничества могут включать в себя идентификатор продавца «93787221». Данные для обнаружения мошенничества могут быть использованы для замены данных, в которых была заменена или удалена секретная информация, в любом подходящем месте. Например, как показано, идентификатор продавца представлен в части данных дорожки 1, в которых была заменена или удалена секретная информация. Остальные секретные данные могут быть подвергнуты замене или удалению секретной информации (например, обнулены) подобно записи 904.

[0095] Запись 912 представляет еще иллюстративные данные дорожки 1 и дорожки 2 после замены или удаления секретной информации, где секретная информация заменена данными для обнаружения мошенничества. Данные для обнаружения мошенничества могут содержать идентификатор продавца «93787221», а также идентификатор терминала «7263859264725928» (например, связанный с POS-терминалом). Идентификатор продавца может быть размещен в части дорожки 2, в которой была заменена или удалена секретная информация, тогда как идентификатор терминала может быть размещен в части дорожки 1, в которых была заменена или удалена секретная информация. В разных вариантах осуществления данные для обнаружения мошенничества могут быть использованы для идентификации продавца, терминала или местоположения, способствуя идентификации взломанных терминалов продавцов.

[0096] Запись 914 представляет еще иллюстративные данные дорожки 1 и дорожки 2 после замены или удаления секретной информации, где секретная информация заменена данными для обнаружения мошенничества. В этом примере данные для обнаружения мошенничества «232323» заменяют часть PAN или токена. Данные для обнаружения

мошенничества заменяют часть PAN или токена, которая не содержит IIN или BIN номера PAN или токена, и/или по меньшей мере четыре последних знака PAN или токена, так что IIN или BIN, и/или по меньшей мере четыре последние знака PAN или токена по-прежнему могут быть извлечены из данных, в которых была заменена или удалена секретная информация, например, в целях идентификации или отслеживания.

[0097] Запись 916 представляет еще иллюстративные данные дорожки 1 и дорожки 2 после замены или удаления секретной информации, где секретная информация заменена данными для обнаружения мошенничества. В этом примере данные для обнаружения мошенничества «23232323» заменяют часть PAN или токена, которая содержит часть IIN или BIN оригинального PAN или токена («400012»), но оставляют последние четыре знака PAN или токена неизменными, так что последние четыре знака PAN или токена по-прежнему могут быть извлечены из данных, в которых была заменена или удалена секретная информация, например, в целях идентификации или отслеживания. Еще в других вариантах осуществления данные для обнаружения мошенничества могут заменять часть последних четырех знаков оригинального PAN или токена, или как часть IIN, так и последние четыре знака оригинального PAN или токена.

[0098] В некоторых вариантах осуществления данные, в которых была заменена или удалена секретная информация, могут быть сохраняющими формат. То есть, получающиеся в результате данные, в которых была заменена или удалена секретная информация, могут сохранять тот же формат (например, количество символов для разных частей), что и оригинальные данные до замены или удаления секретной информации. Такие сохраняющие формат данные, в которых была заменена или удалена секретная информация, могут не быть видимыми для неуполномоченных субъектов, которые могут затем попытаться использовать данные, в которых была заменена или удалена секретная информация, в качестве платежных данных для совершения мошеннических транзакций. Когда это происходит, данные для обнаружения мошенничества, включенные в данные, в которых была заменена или удалена секретная информация, могут быть использованы для быстрой идентификации источника утечки и предотвращения или сдерживания потенциальной утечки данных.

[0099] Варианты осуществления настоящего изобретения относятся к защищенному устройству считывания карт, которое может автоматически обнулять доверительные данные, так что, если терминал продавца подвержен риску, полные данные дорожек из платежной карты не получают. Дополнительно защищенное устройство считывания карт может заменять доверительные данные информацией, которая может идентифицировать продавца, терминал продавца или местоположение, способствуя идентификации взломанных терминалов. Благодаря замене или удалению секретной информации из доверительных данных можно обеспечить безуспешность атак на терминал продавца, например, производимых с помощью USB-кейлоггеров или программных кейлоггеров, поскольку полные данные дорожек не могут быть доступны для создания фальшивых карт. Данные, в которых была заменена или удалена секретная информация, могут быть предоставлены на конечную систему продавца для обработки, связанной с программами лояльности, учетом, контролем возврата и т. п., без риска для полных данных дорожек.

[0100] На фиг. 10 показана структурная схема, представляющая систему 1000 обработки транзакций согласно одному варианту осуществления настоящего изобретения. Для простоты представления на фиг. 10 представлено определенное число компонентов. Однако следует понимать, что варианты осуществления настоящего изобретения могут содержать более одного каждого компонента. Кроме того, некоторые

варианты осуществления настоящего изобретения могут не содержать все компоненты, которые представлены на фиг. 10. Кроме того, компоненты, представленные на фиг. 10, могут осуществлять связь посредством любой подходящей среды связи (включая Интернет), с применением любого подходящего протокола связи.

[0101] Система 1000 обработки транзакций может содержать владельца 1010 счета, который может использовать устройство 1020 запроса токена для запроса платежного токена. Хотя, как представлено на фиг. 10, устройством 1020 запроса токена управляет владелец 1010 счета, им может управлять любой другой подходящий субъект, включая продавца, эквайера и т. п. Как представлено на фиг. 10, устройство 1020 запроса токена может осуществлять связь с компьютером 1030 продавца и компьютерной системой 1060 эмитента токена. Компьютерная система 1060 эмитента токена, компьютер 1030 продавца, компьютер эквайера, компьютер 1050 платежной сети и компьютер 1070 эмитента все могут осуществлять связь друг с другом. Разные субъекты могут иметь возможность осуществлять связь по любому подходящему сетевому соединению или системе связи, включая Интернет и/или любую сеть сотовой связи.

[0102] Компьютерная система 1060 эмитента токена может содержать серверный компьютер 1060A эмитента токена и хранилище 1060B токенов и управляет базой 106°C данных, соединенной с компьютером 1060A эмитента токена. В некоторых вариантах осуществления компьютерная система 1060 эмитента токена может быть охарактеризована как эмитент токена или проверщик токена. В других вариантах осуществления эмитент токена и проверщик токена могут представлять собой отдельные субъекты, где эмитент токена может генерировать токены, а проверщик токена может подтверждать или проверять токены, выданные эмитентом токена.

[0103] Система 1000 обработки транзакций может дополнительно содержать компьютер 1040 эквайера, компьютер 1050 платежной сети и компьютер 1070 эмитента. Устройство 1020 запроса токена может быть выполнено с возможностью связи с компьютером 1030 продавца, компьютером 1040 эквайера, компьютером 1050 платежной сети и компьютером 1070 эмитента по каналу 1080 для транзакций. Канал 1080 для транзакций может содержать путь связи между одним или несколькими из устройства 1020 запроса токена, компьютера 1030 продавца, компьютера 1040 эквайера, компьютера 1050 платежной сети и компьютера 1070 эмитента. Канал 1080 для транзакций может представлять собой канал связи, который позволяет осуществлять связь с компьютером 1070 эмитента во время транзакции электронного платежа.

[0104] Канал 1080 для транзакций может содержать один или несколько подканалов. Подканалы 1080A, которые могут обеспечивать связь между устройством 1020 запроса токена и компьютером 10 продавца, могут содержать подканал бесконтактной или контактной связи между компьютером 1030 продавца и устройством 1020 запроса токена. Они также могут содержать подканал связи между компьютером 1030 продавца и устройством 1020 запроса токена, которое использует сеть связи, такую как Интернет.

[0105] Владелец 1010 счета может быть пользователем портативного пользовательского устройства (например, кредитной карты). Владелец 1010 счета в некоторых ситуациях также может быть назван «покупателем». Владелец 1010 счета может использовать устройство связи (например, мобильный телефон), которое может служить как устройство 1020 запроса токена во время транзакции с продавцом.

[0106] Устройство 1020 запроса токена может представлять собой устройство, которое может запрашивать платежный токен. В некоторых вариантах осуществления оно может быть связано с расчетным счетом владельца 1010 счета. Устройство 1020 запроса токена может представлять собой, без ограничения, мобильное устройство, такое как

мобильный телефон, планшет, PDA, ноутбук, устройство типа брелока или любое подходящее устройство. В других вариантах осуществления устройство 1020 запроса токена может представлять собой стационарное устройство, такое как настольный компьютер. В некоторых вариантах осуществления устройство 1020 запроса токена может включать в себя цифровой или мобильный кошелек, и/или платежное приложение, которое может быть связано с одним или несколькими расчетными счетами владельца 1010 счета. В некоторых вариантах осуществления устройство 1020 запроса токена может быть выполнено с возможностью отображения компьютерно-читаемого кода, такого как QR-код или штрих-код. Устройство 1020 запроса токена также может содержать камеру или сканирующее устройство, выполненное с возможностью сканирования компьютерно-читаемого кода.

[0107] Хотя это и не показано на фиг. 10, в некоторых вариантах осуществления владелец 1010 счета может использовать устройство 1020 запроса токена для взаимодействия с запросчиком токена, который может быть предоставлен посредством удаленного компьютера (например, поставщиком мобильного кошелька) и т. п. Соответственно, владелец 1010 счета может использовать устройство 1020 запроса токена для получения токена, который хранится на удаленном серверном компьютере, управляемом поставщиком мобильного кошелька, который мог ранее получить платежный токен от компьютерной системы 1060 эмитента токена. Соответственно, в некоторых вариантах осуществления может быть несколько устройств запроса токена и/или устройство связи владельца 1010 счета (например, мобильное устройство, портативный компьютер, настольный компьютер), которое может быть использовано для предоставления ранее запрошенного токена на компьютер 1030 продавца.

[0108] Компьютер 1030 продавца может быть связан с продавцом. Компьютер 1030 продавца может представлять собой устройство доступа, такое как POS-терминал в местоположении продавца, компьютер, соединенный с устройством доступа продавца, или удаленный серверный компьютер, на котором размещен и/или работает веб-сайт, используемый продавцом. В некоторых вариантах осуществления продавцом, использующим компьютер 1030 продавца, может быть продавец, использующий функцию card-on-file (хранение и повторное использование данных карты при последующих заказах в онлайне, COF). Продавец, использующий функцию card-on-file, может хранить информацию о счете для владельца 1010 счета в удаленной базе данных для последующих платежей (например, повторяющихся или периодических платежей). Компьютер 1030 продавца может быть выполнен с возможностью генерирования сообщения с запросом авторизации для транзакции, которая запускается владельцем 1010 счета.

[0109] Компьютер 1040 эквайера может находиться под управлением эквайера. Эквайер, как правило, представляет собой систему для субъекта (например, банка), который имеет коммерческую связь с конкретным продавцом, поставщиком кошелька или другим субъектом. Компьютер 1040 эквайера может осуществлять связь с компьютером 1030 продавца и компьютером 1050 платежной сети, и может открывать и управлять счетом продавца. В некоторых вариантах осуществления компьютер 1040 эквайера может направлять сообщение с запросом авторизации на компьютер 1050 платежной сети и сообщение с ответом на авторизацию на компьютер 1030 продавца во время транзакции для подтверждения обработки платежной транзакции.

[0110] Компьютер 1050 платежной сети может быть выполнен с возможностью предоставления услуг авторизации и услуг клиринга и расчетов для платежных транзакций. Компьютер 1050 платежной сети может содержать подсистемы, сети и

операции обработки данных, применяемые для поддержки и доставки услуг авторизации, услуг стоп-листов и услуг клиринга и расчетов. Примером сети обработки платежей может служить VisaNet™. Сети обработки платежей, такие как VisaNet™, могут обрабатывать транзакции кредитных карт, транзакции дебетовых карт и другие типы коммерческих транзакций. VisaNet™, в частности, включает в себя систему Visa Integrated Payments (VIP), которая обрабатывает запросы авторизации, и систему Base II, которая выполняет услуги клиринга и расчетов. Кроме того, сеть обработки платежей может содержать серверный компьютер и может использовать любую подходящую проводную или беспроводную телекоммуникационную сеть, включая Интернет. В некоторых вариантах осуществления компьютер 1050 платежной сети может направлять запрос авторизации, полученный от компьютера 1040 эквайера, на компьютер 1070 эмитента по каналу связи. Компьютер 1050 платежной сети может также направлять сообщение с ответом на авторизацию, полученное от компьютера 1070 эмитента, на компьютер 1040 эквайера.

[0111] Компьютер 1070 эмитента может находиться под управлением организации, открывшей счет. Как правило, организация, открывшая счет, представляет собой субъект (например, банк), который открывает и поддерживает счет держателя 1010 счета. Счет может быть кредитным, дебетовым, предварительно оплаченным или счетом любого другого типа.

[0112] В некоторых вариантах осуществления компьютер 1070 эмитента может представлять собой компьютер, содержащий процессор и материальный постоянный компьютерно-читаемый носитель, соединенный с процессором. Материальный энергонезависимый компьютерно-читаемый носитель может содержать код, выполняемый процессором, для осуществления способа. Способ включает в себя получение от компьютера эмитента токена пользовательского интерфейса для предоставления набора параметров для генерации правила запроса платежного токена. Способ дополнительно включает в себя генерирование набора параметров и отправку набора параметров на компьютер эмитента токена.

[0113] Компьютерная система 1060 эмитента токена может представлять собой отдельный субъект или может быть соединена с, интегрирована в и/или эксплуатироваться или управляться любым из субъектов, представленных на фиг. 10. Компьютерная система 1060 эмитента токена может выдавать токены и может проверять статус токенов. В таких случаях компьютерная система 1060 эмитента токена альтернативно может быть названа как проверщик токенов или эмитент токенов. Дополнительно в некоторых вариантах осуществления эмитент токенов и проверщик токенов могут содержать отдельные субъекты и/или системы, которые могут быть выполнены с возможностью выдачи или генерирования токенов и подтверждения или проверки токенов.

[0114] Примеры таких подсистем или компонентов представлены на фиг. 11. Любая из подсистем или компонентов, представленных на фиг. 11, может быть включена в любое из ранее описанных устройств, аппаратов или систем. Подсистемы, представленные на фиг. 11, взаимно соединены посредством системной шины 1100. Показаны дополнительные подсистемы, такие как принтер 1108, клавиатура 1114, несъемный диск 1116 (или другое запоминающее устройство, содержащее компьютерно-читаемый носитель), монитор 1120, который соединен с адаптером 1110 дисплея, и другие. Периферийные устройства и устройства ввода/вывода (I/O), которые соединяются с I/O контроллером 1102 (который может быть процессором или другим подходящим контроллером), могут быть соединены с компьютерной системой любым количеством

средств, известных в данной области техники, таких как последовательный порт 1112. Например, последовательный порт 1112 или внешний интерфейс 1118 могут быть использованы для соединения вычислительного устройства с глобальной сетью, такой как Интернет, устройством ввода типа мышь или сканером. Соединение по системной шине позволяет центральному процессору 1106 осуществлять связь с каждой подсистемой и управлять выполнением команд из системной памяти 1104 или несъемного диска 1116, а также обмен информацией между подсистемами. Системная память 1104 и/или несъемный диск 1116 могут представлять собой компьютерно-читаемый носитель.

[0115] Кроме того, хотя настоящее изобретение было описано с помощью конкретного сочетания аппаратного и программного обеспечения в форме управляющей логики и программного кода и команд, следует понимать, что другие сочетания аппаратного и программного обеспечения также находятся в рамках объема настоящего изобретения. Настоящее изобретение может быть осуществлено только в аппаратном обеспечении или только в программном обеспечении, или с помощью их сочетаний.

[0116] Программные компоненты или функции, описанные в этой заявке, могут быть реализованы в виде программного кода, подлежащего выполнению на одном или нескольких процессорах, с применением любого подходящего компьютерного языка, такого как, например, Java, C++ или Perl, с использованием, например, обычного или объектно-ориентированного подхода. Программный код может быть сохранен в виде последовательности инструкций или команд в компьютерно-читаемом носителе, таком как оперативное запоминающее устройство (RAM), постоянное запоминающее устройство (ROM), магнитный носитель, такой как жесткий диск или дискета, или оптический носитель, такой как CD-ROM. Любой такой компьютерно-читаемый носитель может также находиться на одном вычислительном устройстве или в нем, и может присутствовать на разных вычислительных устройствах или в них в пределах системы или сети.

[0117] Настоящее изобретение может быть реализовано в форме управляющей логики в программном или аппаратном обеспечении, или в их сочетании. Управляющая логика может храниться в носителе информации в виде множества команд, приспособленных управлять устройством обработки информации для выполнения набора этапов, раскрытых в вариантах осуществления настоящего изобретения. На основании описания и указаний, представленных в данном документе, среднему специалисту в данной области техники будут понятны другие пути и/или способы для осуществления настоящего изобретения.

[0118] Описание, приведенное выше, является иллюстративным и не является ограничительным. Многие варианты настоящего изобретения станут очевидными специалистам в данной области техники по прочтении настоящего описания. Следовательно, объем изобретения следует определять не со ссылкой на вышеприведенное описание, но вместо этого следует определять со ссылкой на рассматриваемые пункты формулы изобретения, наряду с их полным объемом или эквивалентами.

[0119] В некоторых вариантах осуществления любая из сущностей, описанных в данном документе, может быть реализована компьютером, который выполняет любую или все раскрытые функции и этапы.

[0120] Один или несколько признаков из любого варианта осуществления можно сочетать с одним или несколькими признаками любого другого варианта осуществления без отхода от объема настоящего изобретения.

[0121] Формы единственного числа обозначают «один или несколько», если иное не

указано отдельно.

[0122] Все патенты, патентные заявки, публикации и описания, упомянутые выше, включены в данный документ с помощью ссылки во всей своей полноте для всех целей. Ни один из указанных документов не принимается в качестве прототипа.

(57) Формула изобретения

1. Способ замены и удаления секретной информации, включающий в себя:

прием устройством считывания данных устройства от платежного устройства;

идентификацию устройством считывания первой части данных устройства и второй части данных устройства, содержащей секретную информацию;

замену или удаление секретной информации устройством считывания из второй части данных устройства с целью удаления секретной информации путем замены по меньшей мере части секретной информации данными для обнаружения мошенничества; и

подачу устройством считывания первой части данных устройства и второй части данных устройства, в которой была заменена или удалена секретная информация, на хост-компьютер, имеющий связь с устройством считывания.

2. Способ по п. 1, в котором первая часть данных устройства содержит номер основного счета или платежный токен, связанный с номером основного счета.

3. Способ по п. 1, в котором вторая часть данных устройства содержит доверительные данные.

4. Способ по п. 3, в котором доверительные данные содержат код проверки подлинности карты (CVV).

5. Способ по п. 1, в котором замена или удаление секретной информации из второй части данных устройства дополнительно включает в себя замену второй части данных устройства нулями.

6. Способ по п. 1, в котором данные для обнаружения мошенничества указывают продавца, терминал продавца, местоположение или временную информацию, связанную с данными устройства.

7. Способ по п. 1, который дополнительно включает в себя генерирование сообщения с запросом авторизации на основании данных устройства и передачу сообщения с запросом авторизации на компьютер эквайера, имеющий связь с устройством считывания.

8. Способ замены и удаления секретной информации, включающий в себя:

прием устройством считывания данных устройства от платежного устройства;

идентификацию устройством считывания первой части данных устройства, содержащей номер основного счета или платежный токен, связанный с номером основного счета, и второй части данных устройства, содержащей секретную информацию;

замену или удаление секретной информации устройством считывания из второй части данных устройства с целью удаления секретной информации; и

подачу устройством считывания первой части данных устройства и второй части данных устройства, в которой была заменена или удалена секретная информация, на устройство, имеющее связь с устройством считывания.

9. Способ по п. 8, в котором замена или удаление секретной информации из второй части данных устройства включает в себя замену по меньшей мере некоторой части второй части данных устройства нулями.

10. Способ по п. 8, в котором замена или удаление секретной информации из второй

части данных устройства включает в себя замену по меньшей мере некоторой части секретной информации данными для обнаружения мошенничества.

11. Способ по п. 10, в котором данные для обнаружения мошенничества содержат идентификатор продавца или идентификатор устройства.

12. Способ по п. 8, в котором секретная информация содержит доверительные данные.

13. Способ по п. 8, в котором устройство считывания не приспособлено для передачи запроса авторизации платежа.

14. Способ по п. 8, в котором устройство считывания является частью по меньшей мере одного из терминала продавца, двери номера в отеле или регистрационного киоска авиалинии.

15. Защищенное устройство считывания, содержащее процессор и компьютерно-читаемый носитель, соединенный с процессором, причем компьютерно-читаемый носитель содержит код, вызывающий выполнение процессором:

приема данных устройства от платежного устройства;

идентификации первой части данных устройства, содержащей номер основного счета или платежный токен, связанный с номером основного счета, и второй части данных устройства, содержащей секретную информацию;

замены или удаления секретной информации из второй части данных устройства с целью удаления секретной информации; и

подачи первой части данных устройства и второй части данных устройства, в которой была заменена или удалена секретная информация, на устройство, имеющее связь с защищенным устройством считывания.

16. Защищенное устройство считывания по п. 15, в котором замена или удаление секретной информации из второй части данных устройства включает в себя замену по меньшей мере некоторой части второй части данных устройства нулями.

17. Защищенное устройство считывания по п. 15, в котором замена или удаление секретной информации из второй части данных устройства включает в себя замену по меньшей мере некоторой части секретной информации данными для обнаружения мошенничества.

18. Защищенное устройство считывания по п. 17, в котором данные для обнаружения мошенничества содержат идентификатор продавца или идентификатор устройства.

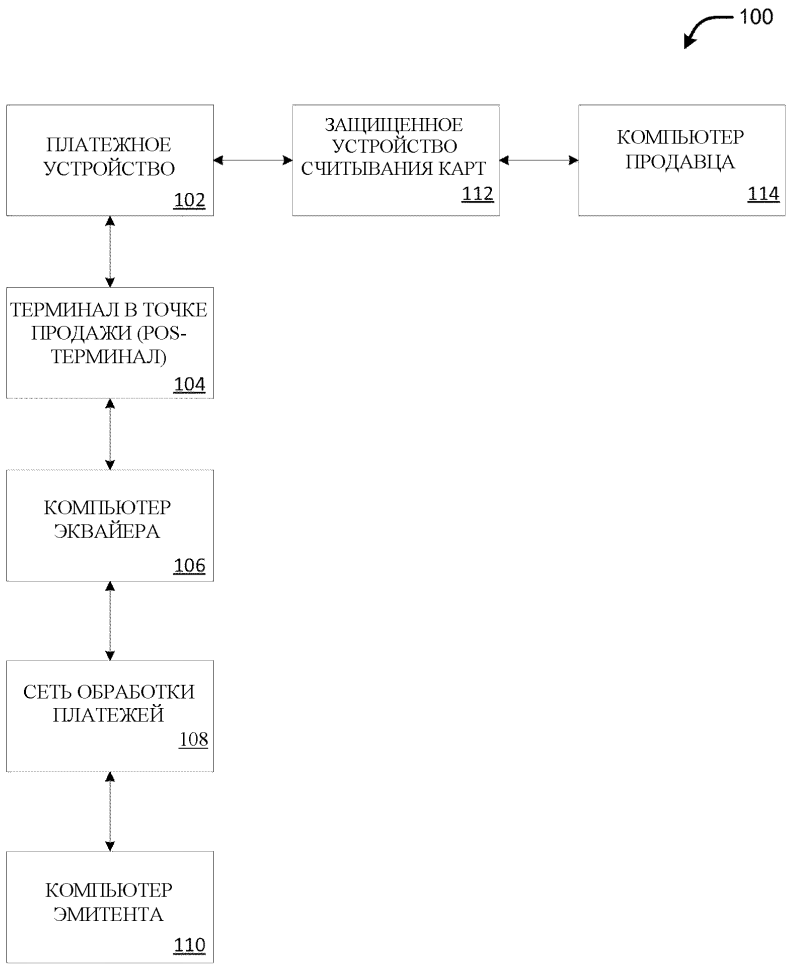
19. Защищенное устройство считывания по п. 15, в котором секретная информация содержит доверительные данные.

20. Защищенное устройство считывания по п. 15, в котором код дополнительно вызывает выполнение процессором:

генерирования сообщения с запросом авторизации на основании данных устройства; и

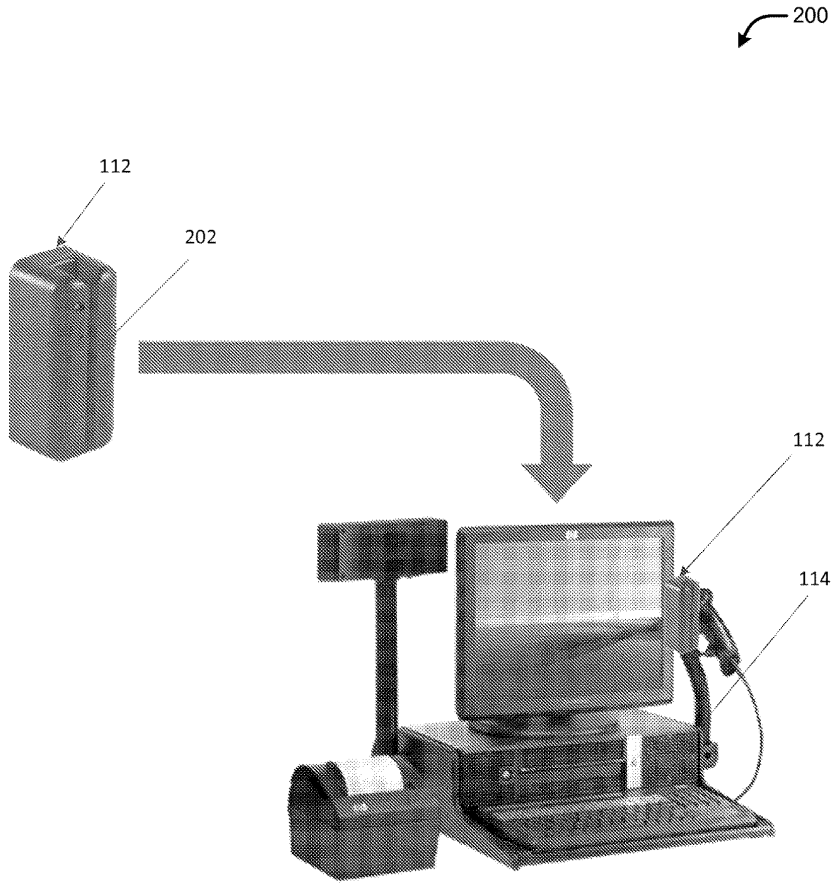
передачу сообщения с запросом авторизации на компьютер эквайера, имеющий связь с защищенным устройством считывания.

1


100
ПЛАТЕЖНОЕ УСТРОЙСТВО
102
ЗАЩИЩЕННОЕ УСТРОЙСТВО СЧИТЫВАНИЯ КАРТ
112
КОМПЬЮТЕР ПРОДАВЦА
114
ТЕРМИНАЛ В ТОЧКЕ ПРОДАЖИ (POS-ТЕРМИНАЛ)
104
КОМПЬЮТЕР ЭКВАЙЕРА
106
СЕТЬ ОБРАБОТКИ ПЛАТЕЖЕЙ
108
КОМПЬЮТЕР ЭМИТЕНТА
110

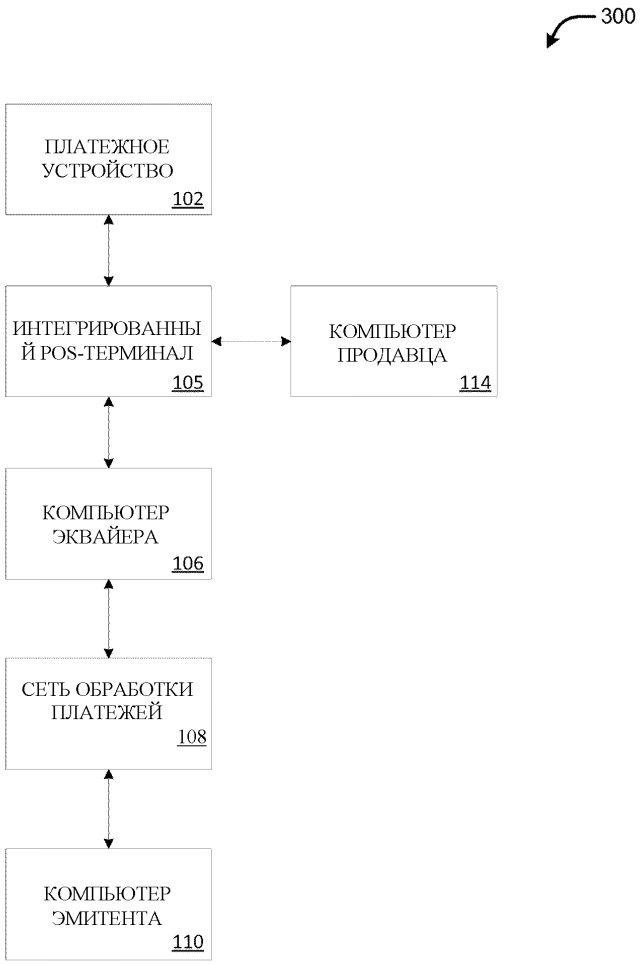
ФИГ. 1

2



ФИГ. 2

3


300
ПЛАТЕЖНОЕ УСТРОЙСТВО
102
ИНТЕГРИРОВАННЫЙ POS-ТЕРМИНАЛ
105
КОМПЬЮТЕР ПРОДАВЦА
114
КОМПЬЮТЕР ЭКВАЙЕРА
106
СЕТЬ ОБРАБОТКИ ПЛАТЕЖЕЙ
108
КОМПЬЮТЕР ЭМИТЕНТА
110

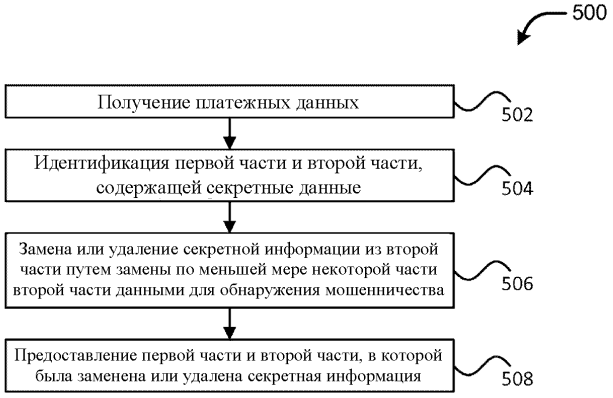
ФИГ. 3

4


400
Авторизация и проведение
USB/последовательный кабель
PAN отправлен на кассовый аппарат
Нет данных дорожек
302
114
105

ФИГ. 4

5


500
Получение платежных данных
502
Идентификация первой части и второй части, содержащей секретные данные
504
Замена или удаление секретной информации из второй части путем замены по меньшей мере некоторой части второй части данными для обнаружения мошенничества
506
Предоставление первой части и второй части, в которой была заменена или удалена секретная информация
508

ФИГ. 5

6


600
Получение платежных данных
602
Идентификация первой части, содержащей PAN или токен, и второй части
604
Замена или удаление секретной информации из второй части
606
Предоставление первой части и второй части
608

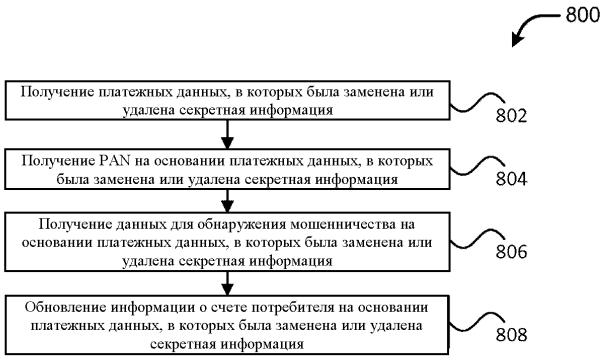
ФИГ. 6

7


700
Получение платежных данных
702
Генерирование сообщения с запросом авторизации
704
Передача сообщения с запросом авторизации
706
Замена или удаление секретной информации из платежных данных
708
Предоставление платежных данных, в которых была заменена или удалена секретная информация
710

ФИГ. 7

8


800
Получение платежных данных, в которых была заменена или удалена секретная информация
802
Получение PAN на основании платежных данных, в которых была заменена или удалена секретная информация
804
Получение данных для обнаружения мошенничества на основании платежных данных, в которых была заменена или удалена секретная информация
806
Обновление информации о счете потребителя на основании платежных данных, в которых была заменена или удалена секретная информация
808

ФИГ. 8

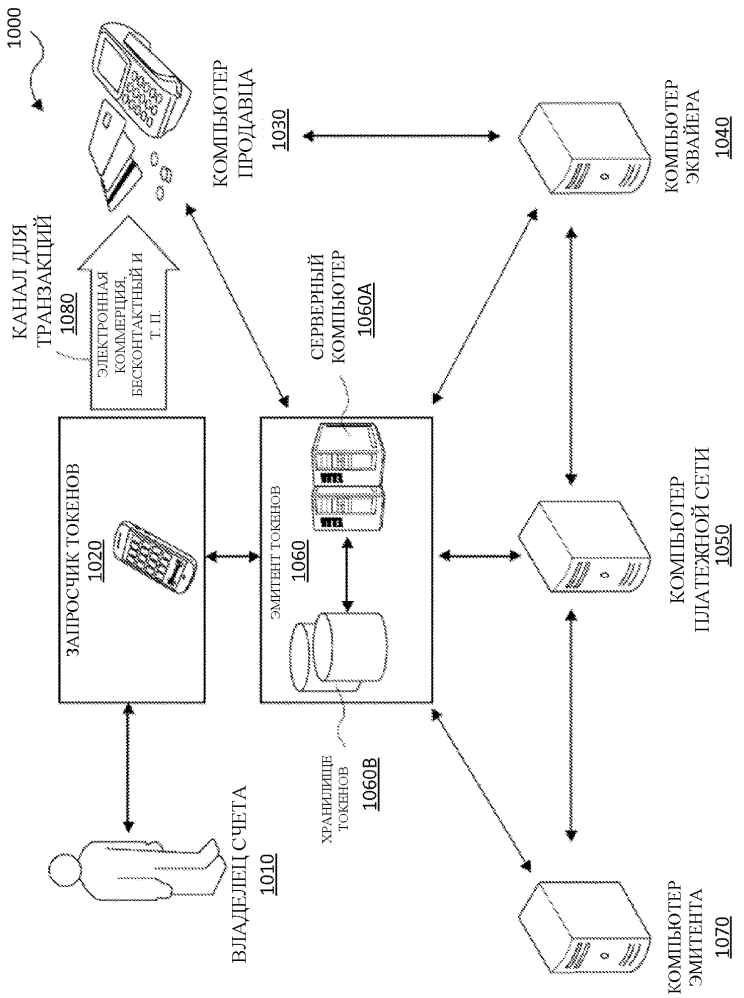
9

900

ДАННЫЕ ДОРОЖКИ 1 И ДОРОЖКИ 2 **ДО ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ** 902	%B4000123456789010^ СМИТ/ДЖОН ^16071021473810559010203? ;4000123456789010=16071021242346 8?
ДАННЫЕ ДОРОЖКИ 1 И ДОРОЖКИ 2 **ПОСЛЕ ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ** 904	%B4000123456789010^0000000000^00000000000000000000000? ;4000123456789010=000000000000000?
ДАННЫЕ ДОРОЖКИ 1, ДОРОЖКИ 2 И ЛОЯЛЬНОСТИ **ДО ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ** 906	%B4000123456789010^ СМИТ/ДЖОН ^16071021473810559010203? ;4000123456789010=16071021242346 8? ;81293812
ДАННЫЕ ДОРОЖКИ 1, ДОРОЖКИ 2 И ЛОЯЛЬНОСТИ **ПОСЛЕ ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ** 908	%B4000123456789010^0000000000^00000000000000000000000? ;4000123456789010=000000000000000? ;81293812
ДАННЫЕ ДОРОЖКИ 1 И ДОРОЖКИ 2 **ПОСЛЕ ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ (ОБНАРУЖЕНИЕ МОШЕННИЧЕСТВА)** 910	%B4000123456789010^0000000000^93787221000000000000000? ;4000123456789010=000000000000000?
ДАННЫЕ ДОРОЖКИ 1 И ДОРОЖКИ 2 **ПОСЛЕ ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ (ОБНАРУЖЕНИЕ МОШЕННИЧЕСТВА)** 912	%B4000123456789010^0000000000^72638592647259280000000? ;4000123456789010=93787221000000?
ДАННЫЕ ДОРОЖКИ 1 И ДОРОЖКИ 2 **ПОСЛЕ ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ (ОБНАРУЖЕНИЕ МОШЕННИЧЕСТВА)** 914	%B4000122323239010^0000000000^00000000000000000000000? ;4000122323239010=000000000000000?
ДАННЫЕ ДОРОЖКИ 1 И ДОРОЖКИ 2 **ПОСЛЕ ЗАМЕНЫ ИЛИ УДАЛЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ (ОБНАРУЖЕНИЕ МОШЕННИЧЕСТВА)** 916	%B4000232323239010^0000000000^00000000000000000000000? ;4000232323239010=000000000000000?

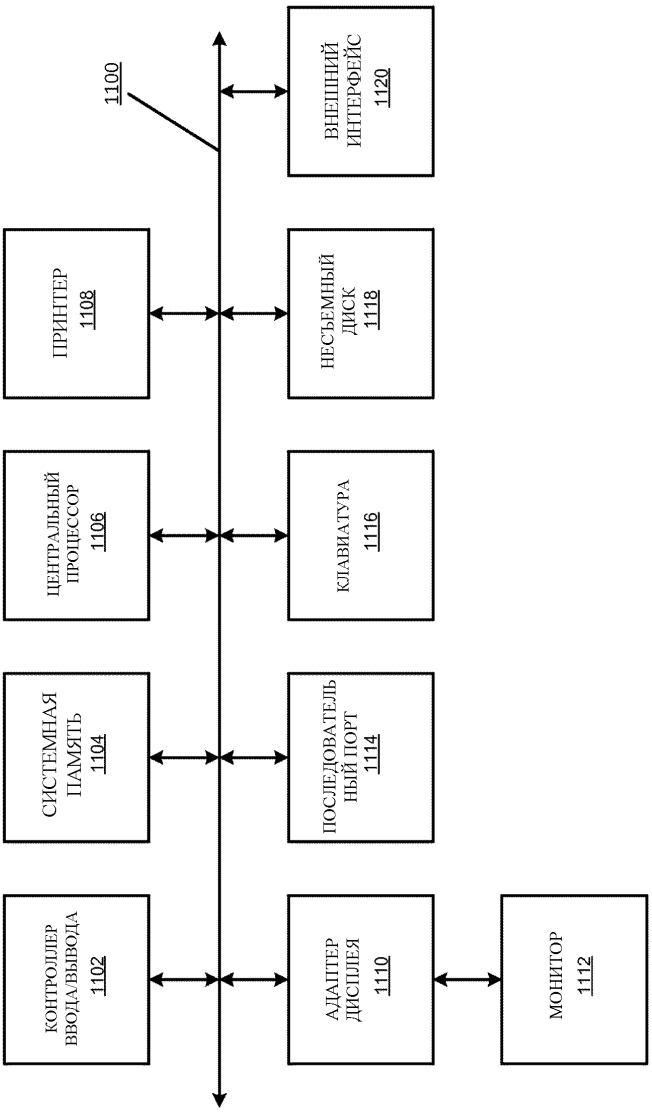
ФИГ. 9

10


1000
КОМПЬЮТЕР ПРОДАВЦА 1030
КОМПЬЮТЕР ЭКВАЙЕРА 1040
КАНАЛ ДЛЯ ТРАНЗАКЦИЙ 1080
ЭЛЕКТРОННАЯ КОММЕРЦИЯ, БЕСКОНТАКТНЫЙ И Т. П.
СЕРВЕРНЫЙ КОМПЬЮТЕР 1060A
ЗАПРОСЧИК ТОКЕНОВ 1020
ЭМИТЕНТ ТОКЕНОВ 1060
КОМПЬЮТЕР ПЛАТЕЖНОЙ СЕТИ 1050
ХРАНИЛИЩЕ ТОКЕНОВ 1060B
ВЛАДЕЛЕЦ СЧЕТА 1010
КОМПЬЮТЕР ЭМИТЕНТА 1070

ФИГ. 10

11


1100
ВНЕШНИЙ ИНТЕРФЕЙС 1120
ПРИНТЕР 1108
НЕСЪЕМНЫЙ ДИСК 1118
ЦЕНТРАЛЬНЫЙ ПРОЦЕССОР 1106
КЛАВИАТУРА 1116
СИСТЕМНАЯ ПАМЯТЬ 1104
ПОСЛЕДОВАТЕЛЬНЫЙ ПОРТ 1114
КОНТРОЛЛЕР ВВОДА/ВЫВОДА 1102
АДАПТЕР ДИСПЛЕЯ 1110
МОНИТОР 1112

ФИГ. 11