



República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e Comércio Exterior
Instituto Nacional de Propriedade Industrial

(21) **PI0615665-7 A2**

(22) Data de Depósito: 05/09/2006
(43) Data da Publicação: 24/05/2011
(RPI 2107)



* B R P I O 6 1 5 6 6 5 A 2 *

(51) *Int.Cl.:*
G06K 5/00 2006.01
G06Q 40/00 2006.01

(54) Título: **MÉTODO PARA USAR UM NÚMERO DE CONTA ASSEGURADO PARA PROCESSAR TIPOS DE PROXIMIDADE DE TRANSAÇÕES FINANCEIRAS SEM FIO, MEIO LEGÍVEL POR COMPUTADOR, COMPUTADOR DE SERVIDOR, DISPOSITIVO DE CONSUMIDOR DE PROXIMIDADE PORTÁTIL PARA EXECUTAR TRANSAÇÕES SEM CONTATO, SISTEMA PARA EXECUTAR TRANSAÇÕES DE PAGAMENTO, E, MÉTODO PARA CONDUZIR TRANSAÇÕES FINANCEIRAS SEM FIO**

(30) Prioridade Unionista: 05/04/2006 US 11/398887,
06/09/2005 US 60/716435

(73) Titular(es): VISA INTERNATIONAL SERVICE ASSOCIATION,
VISA U.S.A. INC.

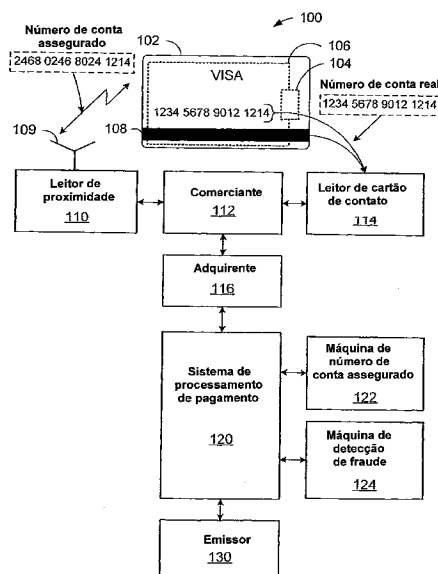
(72) Inventor(es): Barbara Patterson, Brian Maw, Patrick Faith,
Patrick Gauthier

(74) Procurador(es): Momsen, Leonardos & CIA.

(86) Pedido Internacional: PCT US2006034612 de 05/09/2006

(87) Publicação Internacional: WO 2007/030480 de 15/03/2007

(57) Resumo: MÉTODO PARA USAR UM NUMERO DE CONTA ASSEGURADO PARA PROCESSAR TIPOS DE PROXIMIDADE DE TRANSAÇÕES FINANCEIRAS SEM FIO, MEIO LEGÍVEL POR COMPUTADOR, COMPUTADOR DE SERVIDOR, DISPOSITIVO DE CONSUMIDOR DE PROXIMIDADE PORTÁTIL PARA EXECUTAR TRANSAÇÕES SEM CONTATO, SISTEMA PARA EXECUTAR TRANSAÇÕES DE PAGAMENTO, E, METODO PARA CONDUZIR TRANSAÇÕES FINANCEIRAS SEM FIO Um método e sistema para usar um número de conta assegurado para processar tipos de proximidade de transações financeiras sem fio associadas com dispositivos de proximidade de consumidor portáteis são expostos. Em uma concretização, o método inclui receber um tipo de proximidade de pedido de transação financeira sem fio junto com um número de conta assegurado de um dispositivo de consumidor de proximidade portátil, tal como um cartão inteligente sem contato, converter o número de conta assegurado ao número de conta real do usuário, e transmitir o pedido de transação financeira junto com o número de conta real do usuário para o emissor do número de conta real do usuário para autorização e processamento.



“MÉTODO PARA USAR UM NÚMERO DE CONTA ASSEGURADO PARA PROCESSAR TIPOS DE PROXIMIDADE DE TRANSAÇÕES FINANCEIRAS SEM FIO, MEIO LEGÍVEL POR COMPUTADOR, COMPUTADOR DE SERVIDOR, DISPOSITIVO DE CONSUMIDOR DE PROXIMIDADE PORTÁTIL PARA EXECUTAR TRANSAÇÕES SEM CONTATO, SISTEMA PARA EXECUTAR TRANSAÇÕES DE PAGAMENTO, E, MÉTODO PARA CONDUZIR TRANSAÇÕES FINANCEIRAS SEM FIO”

REFERÊNCIAS CRUZADAS A PEDIDOS RELACIONADOS

10 Este pedido reivindica prioridade para o Pedido de Patente Provisório US Nº 60/714.635 depositado em 6 de setembro de 2005 (Registro de Agente Nº 16222U-022900US), intitulado "System And Method Using Ghost Account Number", que está incorporado por este meio por referência em sua totalidade.

15 FUNDAMENTO DA INVENÇÃO

 A presente invenção relaciona-se em geral a dispositivos de consumidor de proximidade portáteis usados em transações de pagamento sem fio, e em particular a várias concretizações de dispositivos de consumidor de proximidade portáteis, tais como cartões inteligentes sem contato de crédito e débito, que usam números de conta assegurados para transações financeiras sem fio.

 Geralmente, dispositivos de consumidor de proximidade portáteis tais como cartões inteligentes sem contato são projetados para prover o consumidor com um modo para se envolver em transações de compra conectando por modo sem fio os dispositivos de consumidor de proximidade portáteis diretamente com o dispositivo de ponto de vendas do comerciante, por exemplo usando sinais de radiofrequência (RF) ou infravermelho (IR). Por exemplo, cartões inteligentes sem contato permitem a um consumidor armazenar e transmitir dados financeiros e outros dados pessoais para um

dispositivo de comerciante que os usa para efetuar um pagamento durante uma transação de compra.

Porque dispositivos de consumidor de proximidade portáteis operam sem requerer conexão direta ao dispositivo aceitante, dispositivos de
5 consumidor de proximidade portáteis são esperados ganhar popularidade sobre outros tipos de dispositivos que requerem contato físico e/ou conexões físicas para se comunicarem com outros dispositivos e sistemas. Ilustrativamente, cartões inteligentes sem contato podem ser usados para substituir cartões de crédito regulares, como eles não precisam entrar em
10 contato com um terminal de transação para serem operados. Cartões de crédito regulares tendo faixas magnéticas e cartões inteligentes de contato devem entrar em contato com um leitor.

Dispositivos de consumidor de proximidade portáteis podem trocar dados por modo sem fio com um leitor de dispositivo de proximidade
15 de uma distância, contanto que o usuário esteja em alcance sem fio do leitor de dispositivo de proximidade. Infelizmente, devido à natureza sem fio dos dispositivos de consumidor de proximidade portáteis, é possível que o leitor de dispositivo de proximidade possa ser usado para interrogação sub-reptícia do dispositivo de consumidor de proximidade portátil interceptando as
20 comunicações do dispositivo eletrônico de proximidade portátil. Além disso, é concebível que um dispositivo de proximidade aceitante possa ser desenvolvido ou modificado para aumentar sua potência e sensibilidade e por esse meio aumentar sua habilidade para interrogar e interceptar sinais dos dispositivos de consumidor de proximidade portáteis de uma maior distância
25 que especificada em padrões usados para dispositivos de consumidor de proximidade portáteis.

Roubo de informação sensível usando interrogação sem fio ou interceptação de comunicações de dispositivos de consumidor de proximidade portáteis é uma preocupação principal para consumidores e negócios

semelhantes. Infelizmente, dada a sofisticação do equipamento de interrogação sem fio e a natureza de sinais sem fio, é fácil para interrogação sem fio ocorrer virtualmente a qualquer momento e lugar. Uma vez que a vítima da interrogação sem fio descobre que teve informação sensível roubada, é freqüentemente tarde demais para descobrir onde o roubo aconteceu. A vítima então deve lidar com as conseqüências e desagrado de corrigir o acesso não autorizado e possíveis usos da informação.

Em resposta a tal risco, muitos provedores de serviço de pagamento instigaram proteções para proteger compras de ataques fraudulentos, por exemplo, empregando tecnologias de criptografia para codificar o número de conta primário e outros dados associados com transações de conta. Criptografia geralmente envolve codificar dados de transação em uma extremidade de uma transmissão com uma chave, e então regenerar os dados de transação originais decifrando os dados codificados recebidos com a mesma chave na outra extremidade da transmissão. Enquanto tecnologias de criptografia se provaram ser altamente efetivas em prevenir roubo de informação, implementar ou atualizar à tecnologia de criptografia mais recente requer freqüentemente atualizações pelo sistemas de processamento de pagamento do usuário final. Devido ao custo, tempo e risco de interrupção de negócio potencial (por exemplo, perda de vendas), muitos comerciantes, por exemplo, resistem em fazer atualizações necessárias a seus procedimentos e sistemas para implementar tais proteções. Portanto, tais proteções tiveram sucesso limitado como elas são geralmente caras para implementar, podem ser superadas, e não foram aceitas completamente pela indústria de cartão de crédito, comerciantes, processadores de pagamento, etc.

Portanto, o que é precisado é um dispositivo e método efetivos em custo que integrem facilmente com sistemas de processamento de pagamento existentes e impeçam um usuário não autorizado de usar dados interrogados sem fio ou interceptados de um dispositivo de consumidor de

proximidade portátil.

BREVE SUMÁRIO DA INVENÇÃO

5 Concretizações da presente invenção provêm um aparelho e método para conduzir transações financeiras usando números de conta assegurados de dispositivos de consumidor de proximidade portáteis.

Concretizações da invenção incluem o uso de "números de conta assegurados". Estes podem incluir números de conta "fantasmas". Um número de conta fantasma pode ser um que está relacionado ao número de conta real de uma pessoa.

10 Em uma concretização, a presente invenção provê um método incluindo receber uma mensagem de pedido de autorização, que inclui um número de conta assegurado. O número de conta assegurado está associado com um número de conta real. Nesta concretização, a mensagem de pedido de autorização se origina de uma transação que resulta de uma interação baseada
15 sem fio entre um dispositivo de consumidor de proximidade portátil incluindo um módulo de comunicação sem fio e uma memória pré-carregada com o número de conta assegurado e um dispositivo de leitor de proximidade incluindo um segundo módulo de comunicação sem fio. O número de conta assegurado é transmitido por modo sem fio do dispositivo de consumidor de
20 proximidade portátil ao dispositivo de leitor de proximidade. O número de conta assegurado pode então ser transmitido a um computador de servidor operado por um adquirente, sistema de processamento de pagamento, e/ou emissor. Depois que o número de conta assegurado é recebido pelo computador de servidor, o número de conta real é determinado. Uma vez que
25 o real número de conta seja determinado, o emissor, por exemplo, pode proceder com seus métodos e processos de autorização de transação habituais. O emissor pode então enviar uma mensagem de resposta de autorização de volta ao dispositivo de leitor de proximidade para informar o consumidor que a transação está ou não está autorizada.

Em outra concretização, a presente invenção provê um dispositivo de consumidor de proximidade portátil para executar transações sem contato. O dispositivo de consumidor de proximidade portátil inclui uma primeira antena, uma primeira memória incluindo um número de conta assegurado acoplado à primeira antena, e uma segunda memória, em que a segunda memória inclui um número de conta real, em que o número de conta real está associado com o número de conta assegurado.

Em outra concretização, a presente invenção provê um sistema para executar transações de pagamento. O sistema inclui um sistema de processamento de pagamento capaz de converter um número de conta assegurado a número de conta real de um usuário. Em resposta ao sistema de processamento de pagamento receber um pedido de autorização de transação incluindo o número de conta assegurado, o sistema de processamento de pagamento determina o número de conta real do usuário associado com o número de conta assegurado, e verifica que o pedido de autorização de transação estava associado com uma transação de pagamento sem fio.

Estas e outras concretizações da invenção são descritas em detalhe adicional abaixo.

BREVE DESCRIÇÃO DOS DESENHOS

Figura 1 é um diagrama de bloco de alto nível ilustrando uma concretização de um sistema de processamento de transação de acordo com concretizações da invenção;

Figura 2 é um diagrama de bloco de alto nível ilustrando uma concretização de um circuito de processamento de dados para um dispositivo de consumidor de proximidade portátil de acordo com concretizações da invenção;

Figura 3 é um fluxograma de alto nível ilustrando uma concretização de um método de executar um processo de transação de número de conta assegurado de acordo com concretizações da invenção; e

Figura 4 é um fluxograma de alto nível ilustrando uma concretização de um método de executar um processo de transação envolvendo uma transmissão baseada sem fio de um número de conta assegurado de um dispositivo de consumidor de proximidade portátil para um leitor de dispositivo de proximidade de acordo com concretizações da invenção.

DESCRIÇÃO DETALHADA

Concretizações da invenção são dirigidas ao uso de um número de conta assegurado pré-carregado sobre um dispositivo de consumidor de proximidade portátil. Dispositivos de consumidor de proximidade portáteis podem ser qualquer dispositivo de consumidor portátil tal como um cartão de débito/crédito inteligente sem contato, cartão de débito/crédito habilitado por chip de contato, um PDA, telefone móvel, e similar, capaz de transmissão sem fio de um número de conta assegurado, em vez do número de conta primário de um usuário (PAN) ou o número de conta real de um usuário. Como descrito aqui, o termo "próximo" pode ser usado intercambiavelmente com termos tal como sem contato relativo a transações comunicadas por modo sem fio de entre dispositivos próximos um ao outro.

Números de conta assegurados podem incluir números de conta "fantasmas". Em uma concretização, um número de conta fantasma pode ser um que está relacionado ao número de conta real de uma pessoa. O número de conta assegurado pode ser considerado um número de conta capaz de parecer com o número de conta real de um usuário (por exemplo, um PAN real). Por exemplo, se o número de conta real de um usuário contiver dezenove dígitos, o número de conta assegurado também pode conter dezenove dígitos. É contemplado que o número de conta assegurado pode ser de qualquer comprimento contanto que pareça com um número de conta real, tal como um número de cartão de crédito, número de cartão de débito, número de cartão de presente, e similar. Por exemplo, o número de conta assegurado

pode parecer com um número de cartão de presente que é de vinte e um dígitos em comprimento, quando o número de conta real do usuário é dezenove dígitos de comprimento. O número de conta assegurado também pode ser um número estático. O termo "estático" significa que o número de
5 conta assegurado não tem que mudar entre transações, mas pode mudar quando o usuário muda contas, o número de conta real do usuário expira, o dispositivo de consumidor de proximidade portátil é perdido ou roubado, etc. O número de conta assegurado também pode ser descrito usando termos tais como falso, simulado, chamariz, substituto, e similar, que significam uma
10 seqüência alfanumérica que é usada em lugar do número de conta real de um usuário para executar transações.

Em concretizações da invenção, o número de conta assegurado pode ser pré-carregado em uma primeira memória em um dispositivo de consumidor de proximidade portátil, enquanto o número de conta real do
15 usuário é armazenado em uma segunda memória no dispositivo de consumidor de proximidade portátil. A primeira e segunda memórias podem usar tecnologias de memória de dados diferentes. Por exemplo, a primeira memória pode incluir um chip de memória, e a segunda memória pode estar na forma de uma faixa magnética.

20 O dispositivo de consumidor de proximidade portátil pode operar em uma variedade de modos de transmissão sem fio tal como um modo sem contato ou um modo infravermelho, modo de RF (isto é, Radiofrequência) e similar, e opcionalmente pode ser operado em um modo de contato tal como por uma interface de comunicação ligada por fios. O
25 número de conta assegurado é usado em transações sem fio. O número de conta regular do usuário é usado e transmitido quando o dispositivo de consumidor de proximidade portátil é usado em um modo de contato, ou quando o consumidor executa uma transação de entrada direta (por exemplo, entrando com um número de conta real sobre uma forma da Web para

comprar mercadorias na Internet).

Posto de outro modo, o número de conta assegurado não é usado para transações de contato ou transações de entrada direta. Por exemplo, em uma transação não sem fio, quando no número de conta assegurado é entrado sobre uma forma da Web por um portal de comerciante da Internet, a transação não será não autorizada. Isto é útil se alguém (por exemplo, um ladrão) interceptar sub-repticiamente o número de conta assegurado durante uma transação de compra e obtiver o número de conta assegurado. Porque o número de conta assegurado é configurado para parecer com um número de conta real, ele enganará o usuário não autorizado em acreditar que é um número de conta operável. Porém, se o usuário não autorizado entrar com o número de conta assegurado sobre uma forma da Web para conduzir uma transação, a transação não é autorizada pelo emissor, a menos que, por exemplo, o emissor esteja usando a transação como um meio para pegar o usuário não autorizado. Além disso, o número de conta assegurado é configurado tal que usuários não autorizados não possam recuperar o número de conta real para uso em transações fraudulentas, sem acesso a um banco de dados configurado para manter o número de conta real secreto de acesso não autorizado. Como será explicado em detalhe adicional abaixo, é vantajoso como pode tornar mais fácil detectar uma transação não autorizada e descobrir fraude potencial. Além disso, o número de conta assegurado não provê informação suficiente para rotear a transação ao emissor apropriado desde que a conta assegurada não provê um número de caminho de transação válido (por exemplo, número de identificação de banco). Assim, a presente invenção cria múltiplos desafios para prevenir a transação que o ladrão tenta conduzir de ser autorizada.

Os dispositivos de consumidor de proximidade portáteis de acordo com concretizações da invenção podem ser usados com dispositivos de interrogação sem fio autorizados (por exemplo, dispositivos de leitor de

proximidade autorizados) que também podem ter módulos de comunicação e transmissão sem fio (por exemplo, receptor, transceptor, etc.). Tais dispositivos de interrogação autorizados podem estar presentes em terminais de ponto-de-venda (POS), BANCO 24 HORAS e similares. Tais dispositivos de interrogação são bem conhecidos na arte. Os dispositivos de consumidor de proximidade portáteis de acordo com concretizações da invenção podem operar com qualquer número de tais dispositivos de interrogação sem fio autorizados usando uma variedade de padrões operacionais. Por exemplo, um tal padrão pode ser o padrão 'Europay-Mastercard-Visa' (EMV) iniciado por um grupo de trabalho criado em 1993 pelas três organizações de pagamento principais do mundo: EUROPAY (EPI), MASTERCARD (MCI) e VISA.

Como notado acima e abaixo, um dispositivo de consumidor de proximidade portátil exemplar pode incluir uma memória tal como um chip de memória e/ou um microprocessador. Qualquer um pode ser acoplado operacionalmente aos módulos de comunicação e/ou transmissão no dispositivo de consumidor de proximidade portátil. A memória poderia estar na forma de uma chip de memória ou poderia ser lógica por fios. A informação na memória pode incluir informação tal como a informação de conta bancária de um usuário, número de conta assegurado, informação de número de conta de crédito ou débito, informação de saldo de conta, informação de consumidor, etc.

Em algumas concretizações, durante um processo para autorizar uma transação de pagamento eletrônica, o número de conta assegurado é transmitido por modo sem fio de um dispositivo de consumidor de proximidade portátil ao dispositivo de leitor de proximidade executando a transação, tal como por exemplo, um terminal de transação de cartão inteligente sem contato. O número de conta assegurado é então transmitido do terminal de transação de cartão inteligente sem contato a um comerciante, para o adquirente do comerciante, para um sistema de processamento de

pagamento, e então para o emissor. Em uma concretização, um ou mais aparelhos computacionais a qualquer um destas entidades podem ser usados para converter o número de conta assegurado no número de conta real do usuário de forma que o emissor possa responder a uma mensagem de pedido de autorização submetida.

Em concretizações da invenção, uma mensagem de pedido de autorização para uma transação é criada depois que um consumidor compra um bem ou serviço em um terminal de POS usando um dispositivo de consumidor de proximidade portátil tal como um cartão de crédito ou débito. A mensagem de pedido de autorização pode ser enviada do terminal de POS localizado a um comerciante ao adquirente do comerciante, para um sistema de processamento de pagamento, e então para um emissor.

Um "comerciante" em concretizações da invenção pode ter qualquer característica adequada. Um comerciante pode incluir entidades tais como corporações, firmas individuais, organizações sem lucro, ou um grupo específico de tais entidades. Exemplos de comerciantes incluem restaurantes, teatros, depósitos de gasolina e combustível, supermercados, varejistas de vestuário, lojas de departamentos, etc. O comerciante tem um ou mais terminais de POS que podem interagir com os dispositivos de consumidor de proximidade portáteis. Qualquer terminal de POS adequado pode ser usado incluindo leitores de cartão como descrito aqui. Os leitores de cartão podem incluir qualquer modo de contato ou proximidade de operação adequado. Por exemplo, leitores de cartão exemplares podem incluir antenas de RF (radiofrequência), leitores de faixa magnética, etc., para interagir com os dispositivos de consumidor de proximidade portáteis.

Um "adquirente" é tipicamente uma entidade empresarial, por exemplo, um bando comercial que tem uma relação empresarial com um comerciante particular. Um "emissor" é tipicamente uma entidade empresarial (por exemplo, um banco) que emite um dispositivo de consumidor de

proximidade portátil tal como um cartão de crédito ou débito para um consumidor. Algumas entidades tais como American Express executam ambas funções de emissor e adquirente. Concretizações da invenção abrangem tais emissor-adquirentes de entidade única.

5 Uma "mensagem de pedido de autorização" pode incluir um pedido para autorização para conduzir uma transação de pagamento eletrônica ou algum outro tipo de atividade. Pode incluir um ou mais do número de conta de pagamento de um titular de conta, código de moeda corrente, quantia de venda, selo de transação mercantil, cidade de aceitante, estado/país de
10 aceitante, número de transação de POS, tipo de transação de POS, etc. Opcionalmente, a mensagem de pedido de autorização pode ser protegida usando um método de criptografia segura por exemplo, SSL de 128 bits ou equivalente a fim de prevenir dados de serem comprometidos. Em outras concretizações, uma "mensagem de pedido de autorização" pode incluir um
15 pedido para permissão para entrar em um local predeterminado (por exemplo, como usado para distintivos de acesso sem fio).

 Tipicamente, uma transação de pagamento eletrônica é autorizada se o consumidor conduzindo a transação tiver fundos suficientes ou créditos para conduzir a transação. Reciprocamente, se houver fundos
20 insuficientes ou créditos na conta do consumidor, ou se o dispositivo de consumidor de proximidade portátil do consumidor estiver em uma lista negra (por exemplo, está indicado como roubado), então uma transação de pagamento eletrônica não pode ser autorizada (por exemplo, recusada).

 Figura 1 é um diagrama de bloco de alto nível ilustrando uma
25 concretização de uma sistema de processamento de transação 100. O sistema de processamento de transação 100 inclui um comerciante 112, um adquirente 116, um sistema de processamento de pagamento 120, e um emissor de número de conta 130.

 O sistema de processamento de transação 100 também inclui

um dispositivo de leitor de proximidade 110 capaz de receber por modo sem fio números de conta assegurados, e um leitor de contato opcional 114, capaz de receber números de conta reais de um consumidor de dispositivo de proximidade portátil 102 tal como um cartão inteligente de crédito ou débito.

- 5 O dispositivo de leitor de proximidade 110 e/ou o leitor de contato 114 pode estar localizado no comerciante 112, ou pode ser simplesmente operado pelo comerciante 112.

O dispositivo de consumidor de proximidade portátil 102 de acordo com concretizações da invenção pode estar em qualquer forma adequada. Por exemplo, o dispositivo de consumidor de proximidade portátil 102 pode ser segurado à mão e compacto de forma que possa caber na carteira e/ou bolso de um consumidor (por exemplo, de tamanho de bolso). Por exemplo, o dispositivo de consumidor de proximidade portátil 102 pode incluir cartões inteligentes, cartões de crédito ou débito ordinários (com uma 15 faixa magnética e sem um microprocessador), um dispositivo de chaveiro, chave Fob, etc. Outros exemplos de dispositivos de consumidor de proximidade portáteis sem contato 102 incluem telefones celulares, assistentes digitais pessoais (PDAs), radiolocalizadores, cartões de pagamento, cartões de segurança, cartões de acesso, mídia inteligente, 20 transponders, e similares. Tais dispositivos de consumidor de proximidade portáteis 102 podem ter uma ou mais antenas 106 acopladas a dispositivos de transmissão sem fio que podem transmitir e/ou receber sinais e dados por um meio de comunicação sem fio.

O sistema de processamento de pagamento 120 pode incluir 25 subsistemas de processamento de dados, redes, e operações usadas para suportar e entregar serviços de autorização, serviços de arquivo de exceção, e serviços de compensação e pagamento. Um sistema de processamento de pagamento exemplar 120 pode incluir VisaNet™. Sistemas de processamento de pagamento tais como VisaNet™ são capazes de processar transações de

cartão de crédito, transações de cartão de débito, e outros tipos de transações comerciais. VisaNet™, em particular, inclui um sistema de mensagem única (SMS) que autoriza automaticamente e provê informação suficiente para compensar automaticamente e pagar uma transação financeira, e/ou um sistema de VIP (sistema de Pagamentos Integrados Visa) que processa pedidos de autorização e um sistema de Base II, que executa serviços de compensação e pagamento.

O sistema de processamento de pagamento 120 pode incluir um computador de servidor. Um computador de servidor é tipicamente um computador poderoso ou agrupamento de computadores. Por exemplo, o computador de servidor pode ser um computador de grande porte, um agrupamento de minicomputadores, ou um grupo de servidores funcionando como uma unidade. Em um exemplo, o computador de servidor pode ser um servidor de banco de dados acoplado a um servidor da Web. O sistema de processamento de pagamento 120 pode usar qualquer rede por fios ou sem fio adequada, incluindo a Internet.

Em uma concretização, o dispositivo de leitor de proximidade 110 é capaz de receber por modo sem fio um número de conta assegurado de um dispositivo de consumidor de proximidade portátil 102. Por exemplo, como ilustrado na Figura 1, o número de conta assegurado "2468 0246 8024 1214" pode ser transmitido por modo sem fio de uma antena 106 do dispositivo de consumidor de proximidade portátil 102 para uma antena 109 acoplada a um transceptor sem fio do dispositivo de leitor de proximidade 110 durante uma transação financeira por um consumidor (por exemplo, usuário de um dispositivo de consumidor de proximidade portátil). Como descrito acima, o leitor de contato 114 é capaz de receber o número de conta real de um usuário do dispositivo de consumidor de proximidade portátil 102. Por exemplo, para um cartão inteligente de crédito/débito, o leitor de contato 114 é capaz de recuperar informação de uma faixa magnética, ou manualmente

(por exemplo, por um operador do leitor de contato 114). Ilustrativamente, o leitor de contato 114 é capaz de ler o número de conta real do usuário "1234 5678 9012 1214" da faixa magnética 108, e/ou um operador pode entrar com o número de conta real do usuário "1234 5678 9012 1214" no leitor de contato 114 manualmente.

O número de conta assegurado pode ser derivado do número de conta real do usuário usando qualquer algoritmo adequado. Por exemplo, um algoritmo exemplar multiplica os primeiros doze números do número de cartão real do usuário por dois e então toma o último dígito do número novo, por exemplo, 1234 5678 9012 1214, para converter o número de conta do usuário a um número de conta assegurado, por exemplo, 2468 0246 8024 1214. Neste exemplo, o algoritmo pode deixar um único dígito em cada local de dígito. Como ilustrado acima, quando o número cinco é multiplicado por dois, o algoritmo suprime o um resultante dos "10" para deixar o zero. Certamente, outros algoritmos podem ser usados. Qualquer tal algoritmo preferivelmente deixa os últimos quatro dígitos do número de conta real inalterados. Recibos de cartão de crédito típicos mascaram a primeira série de números do número de conta de um usuário, mas expõe os últimos quatro dígitos. Não alterando os últimos quatro dígitos, o consumidor não sabe se um número de conta assegurado ou o número de conta real é usado em uma transação particular. Isto é vantajoso, como evita confusão por parte do consumidor e pode intimidar atividades fraudulentas relacionadas à recuperação de recibos.

O número de conta assegurado resultante pode ser armazenado em um banco de dados junto com o número de conta real em uma tabela de consulta com outros números de conta assegurados e reais correspondentes. O banco de dados pode ser acessível ao adquirente 116, sistema de processamento de pagamento 120, e/ou o emissor 130. O banco de dados é preferivelmente acessível a pelo menos um do sistema de processamento de

pagamento 120 e/ou o emissor 130, desde que o emissor 130 autoriza ou não autoriza a transação do usuário.

Os números de conta assegurados podem ser pré-carregados no dispositivo de consumidor de proximidade portátil 102 do usuário. O um ou mais algoritmos podem ser usados a qualquer hora, por exemplo, antes de fabricação, durante a fabricação, ou durante processamento do dispositivo de proximidade portátil de consumidor 102, para gerar os números de conta assegurados. Por exemplo, o algoritmo pode ser usado ao gerar números de conta reais, durante produção do dispositivo de consumidor de proximidade portátil 102, durante ativação de número de conta, ou ao preparar para pré-carregar os números de conta assegurados nos dispositivos de consumidor de proximidade portáteis 102, etc.

É desejável "pré-carregar" o número de conta assegurado em uma memória no dispositivo de consumidor de proximidade portátil 102. Como notado acima, técnicas de criptografia são conhecidas. Porém, tais técnicas de criptografia requerem o uso de programas de computação prolongados que precisam ser armazenados no dispositivo de consumidor de proximidade portátil. Tais programas de computação prolongados ocupam espaço valioso na memória do dispositivo de consumidor de proximidade portátil 102. Usando um número de conta pré-carregado assegurado que parece um número de conta real, uma quantidade relativamente pequena de espaço é usada na memória do dispositivo de consumidor de proximidade portátil 102. Adicionalmente, o software e o hardware associados com o dispositivo de leitor de proximidade 110 e/ou o leitor de cartão de contato 114 não precisam ser alterados desde que o número de conta assegurado tem a mesma forma como o número de conta real.

Em uma concretização operacional, durante uma transação de compra de consumidor, uma mensagem de pedido de autorização incluindo um número de conta assegurado é transmitida por modo sem fio do

dispositivo de consumidor de proximidade portátil 102 para o leitor de dispositivo de proximidade 110. Por exemplo, um consumidor pode comprar um artigo de vestir com um cartão inteligente sem contato. A mensagem de pedido de autorização incluindo o número de conta assegurado e um
5 identificador de tipo de transação de POS (indicativo que a transação era um tipo sem fio de transação de proximidade) é recebido pelo comerciante 112 e é transmitido ao adquirente 116. O adquirente 116 então transmite, entre outra informação, a mensagem de pedido de autorização incluindo o número de conta assegurado, identificador de tipo de transação de POS para o sistema de
10 processamento de pagamento 120 para processamento disso.

Em uma concretização, o identificador de tipo de transação de POS pode ser um indicador alfanumérico, símbolo, e similar. Pode indicar que a transação que era conduzida era uma transação financeira de proximidade, e não era uma transação de tipo de contato. Por exemplo, o
15 identificador de tipo de transação de POS pode ser um número convencional usado na indústria de cartão de crédito tal como "código de entrada de POS 91", ou poderia ser uma versão modificada de um indicador padrão tal como um indicador da organização de padrões internacionais modificados (ISO). Depois um computador de servidor no sistema de processamento de
20 pagamento 120 recebe a mensagem de pedido de autorização, o sistema de processamento de pagamento 120 identifica o número de conta transmitido como um número de conta assegurado e usa o identificador de tipo de transação de POS para identificar a transação como uma transação sem fio. Se o número de conta assegurado for válido e se a transação for identificada
25 como uma transação sem fio, então o sistema de processamento de pagamento 120 converte o número de conta assegurada ao número de conta real do usuário. O número de conta real é então transmitido ao emissor 130 para autorização de pagamento.

O número de conta real inclui o BIN (número de identificação

de banco) do número de conta real, assim o sistema de processamento de transação 120 sabe qual emissor particular é suposto receber a mensagem de pedido de autorização. Geralmente, um BIN corresponde aos primeiros seis dígitos do número de conta real do usuário (por exemplo, o número de conta de crédito ou débito). Estes primeiros seis dígitos identificam com qual rede o dispositivo de consumidor de proximidade portátil 102 está associado como também qual emissor 130 emitiu o dispositivo de consumidor de proximidade portátil 102. Se a transação for autorizada pelo emissor 130, o sistema de processamento de pagamento 120 transmite uma mensagem de resposta de autorização junto com o número de conta assegurado (ou número de conta real) de volta para o adquirente 116. O adquirente 116 envia a mensagem de resposta de autorização para o comerciante 112. Uma impressora (não mostrada) no comerciante 112 pode então imprimir um recibo mostrando só os últimos quatro dígitos do número de conta assegurado, por exemplo, ***** 1214. Como notado acima, desde que os últimos quatro dígitos são os mesmos para o número de conta assegurado e o número de conta real do usuário, o usuário é não ciente de qualquer diferença de número de conta entre o número de conta assegurado e o número de conta real do usuário. Enquanto quatro dígitos são ilustrados, alguém qualificado na arte reconhecerá que qualquer indicador alfanumérico, símbolo, ou indício, comum a ambos o número de conta assegurado e ao número de conta real do usuário pode ser usado dentro da extensão da presente invenção. Por exemplo, em algumas concretizações, o número de conta assegurado e o número de conta real podem ter dois ou mais números comuns.

Duas máquinas de software são ilustradas na Figura 1. Elas incluem uma máquina de conta assegurada 122 e uma máquina de detecção de fraude 124 opcional. Várias outras máquinas de software também podem ser incluídas no sistema para executar os métodos de acordo com concretizações da invenção. Embora as duas máquinas de software 122, 124 sejam mostradas

como sendo diretamente acessíveis ao sistema de processamento de pagamento 120, elas também podem ser ou alternativamente acessíveis diretamente ao dispositivo de leitor de proximidade 110, ao comerciante 112, ao adquirente 116, e ao emissor 130. A máquina de conta assegurada 122 é preferivelmente acessível diretamente ou dentro do sistema de processamento de pagamento 120. Se o número de conta assegurado for convertido no sistema de processamento de pagamento 120, o sistema de processamento de pagamento 120 será capaz de dirigir a mensagem de pedido de autorização ao emissor 130 apropriado. Além disso, se o software para converter o número de conta assegurado no número de conta real estiver no sistema de processamento de pagamento 120, atualizações de equipamento caro não precisam ocorrer no adquirente 116 ou comerciante 112.

Quando um número de conta assegurado é recebido pela máquina de conta assegurada 122, a máquina de conta assegurada 122 converte o número de conta assegurado para o número de conta real do usuário. Em uma concretização, a máquina de conta assegurada 122 compara o número de conta assegurado a uma pluralidade de números de conta assegurados para achar o número de conta real do usuário (por exemplo, em uma tabela de consulta). Alternativamente, um ou mais algoritmos podem ser operados para converter o número de conta assegurado ao número de conta real do usuário. Um algoritmo adequado pode ser o programa inverso do algoritmo usado para converter o número de conta real ao número de conta assegurado (como descrito acima).

Se o sistema de processamento de pagamento 120 receber uma mensagem de pedido de autorização incluindo um número de conta assegurado que não tem o identificador de tipo de transação (por exemplo, POS 91), ou outro indicador, indicando uma transação de proximidade, então a máquina de detecção de fraude 124 opcional pode ser capaz de uma ou mais respostas proativas e não proativas. Por exemplo, uma resposta não proativa é

simplesmente negar a transação. Uma mensagem de resposta de autorização pode ser enviada do emissor 130 para o comerciante 112 que indica que a transação não está autorizada. Um exemplo de uma resposta proativa é alertar autoridades legais que uma atividade fraudulenta está acontecendo. Em uma concretização, quando o número de conta assegurado é recebido pelo sistema de processamento de pagamento 120 sem o indicador de transação de proximidade de POS, então o emissor 130 é notificado. O emissor 130 verifica a conta do usuário real para atividade incomum (por exemplo, grandes compras quando um consumidor normalmente não faz grandes compras). Se atividade incomum for detectada, então o sistema de processamento de pagamento 120 e/ou o emissor 130 pode suspender o número de conta assegurado até que verificação seja feita que o número de conta assegurado não era roubado. Neste caso, o uso do número de conta assegurado e/ou o número de conta real pode ser suspenso temporariamente durante uma investigação. Se for determinado que o número de conta assegurado do usuário foi obtido e usado por uma pessoa não autorizada, então o sistema de processamento de pagamento 120 pode re-emitir um novo dispositivo de consumidor de proximidade portátil ao usuário real. Por exemplo, semelhante a procedimentos convencionais para números de conta perdidos ou roubados, parte do processo de verificação pode ser para o sistema de processamento de pagamento 120 emitir um alerta para o comerciante 112 para manter o dispositivo de consumidor de proximidade portátil 102, ou ter o contato de usuário para o emissor 130 verificar a transação não autorizada.

Figura 2 é um diagrama de bloco de alto nível ilustrando uma concretização de um circuito de processamento de dados 104 para uso com um dispositivo de consumidor de proximidade portátil 102. O circuito de processamento de dados 104 pode ser virtualmente qualquer tipo de circuito integrado e/ou sistema de processamento de dados tal como um

microprocessador, arranjo de porta programável em campo (FPGA), circuito integrado específico de aplicação (ASIC), e similar, que pode ser configurado para executar concretizações da presente invenção com vantagem. Em uma concretização, o circuito de processamento de dados 104 inclui uma Unidade de Processamento Central (CPU) 202, um módulo de comunicação sem fio ou circuito de transceptor 206, e uma primeira memória 210, e uma segunda memória opcional 220 em comunicação com isso por um barramento 208. CPU 202 pode estar sob o controle de um sistema operacional que pode ser disposto na primeira memória 210. Virtualmente qualquer sistema operacional ou porção dele suportando as funções de configuração expostas aqui pode ser usado. Em uma concretização, a CPU 202 pode ser circuitos lógicos conectados por fios, e similar, adaptados para operar circuito de processamento de dados 104.

O módulo de comunicação sem fio 206 pode ser projetado para receber sinais de interrogação sem fio e transmitir sinais de comunicação ao dispositivo de leitor de proximidade 110 pelo módulo de transmissão sem fio 106. Qualquer número de dispositivos de comunicação sem fio bem conhecidos na arte pode ser usado para realizar a recepção e transmissão de dados entre o dispositivo de leitor de proximidade 110 e o dispositivo de consumidor de proximidade portátil 102. Por exemplo, o módulo de comunicação sem fio 206 pode ser formado de um receptor sem fio em combinação com um transmissor sem fio. O módulo de comunicação sem fio 206 pode usar qualquer ligação de comunicação viável tal como ISO 14443, Bluetooth, 802.11x, rede celular, RF, e similar. Em outras palavras, virtualmente qualquer sistema de transceptor sem fio que seja dimensionado apropriadamente e capaz de se comunicar com leitor sem contato 110 pode ser usado.

A primeira memória 210 pode ser uma memória não volátil ou volátil tal como uma memória de acesso aleatório que tem espaço suficiente

para conter a programação necessária e estruturas de dados da invenção. Enquanto a primeira memória 210 é mostrada como uma única entidade, deveria ser entendido que a primeira memória 210 pode na realidade incluir uma pluralidade de módulos, e que a primeira memória 210 pode existir a

5 níveis múltiplos de registradores de alta velocidade e 'caches' para abaixar velocidade, mas chips de memória de acesso aleatório direta maiores (DRAM). Em uma concretização, primeiro a memória 210 pode incluir um programa de conta assegurada 212 e armazenamento de número de conta assegurado 214. O programa de conta assegurada 212 pode usar qualquer uma

10 de várias linguagens de programação diferentes. Por exemplo, o código de programa pode ser escrito em código PLC (por exemplo, lógica escalonada), uma linguagem de alto nível tal como C, C++, Java, ou várias outras linguagens. Enquanto o programa de conta assegurada 212 pode ser um programa independente, é contemplado que o programa de conta assegurada

15 212 pode ser combinado com outros programas.

O programa de conta assegurada 212 quando executado na CPU 202, provê um número de conta assegurado ao dispositivo de leitor de proximidade 110 do armazenamento de número de conta assegurado 214. Em uma concretização, o programa de conta assegurada 212 é configurado para

20 recuperar um número de conta assegurado do armazenamento de conta assegurada 214. O programa de conta assegurada 212 instrui a CPU 202 para transmitir por modo sem fio o número de conta assegurado, entre outros dados tais como crédito disponível, dados de usuário, e similar, para o dispositivo de leitor de proximidade 110 pelo módulo de comunicação sem

25 fio 206.

Em uma concretização, o circuito de processamento de dados 104 pode opcionalmente incluir uma segunda memória 220. A segunda memória 220 é capaz de armazenar o número de conta real do usuário em um armazenamento de número de conta real 222. Preferivelmente, no caso onde o

circuito de processamento de dados 104 armazena ambos o número de conta assegurado e o número de conta real do usuário, o número de conta real do usuário só é acessível por uma conexão de contato físico. Por exemplo, o número de conta real do usuário pode ser acessado por uma conexão elétrica com circuito de processamento de dados 104. Em uma concretização alternada, semelhante a cartões de crédito/débito convencionais, o número de conta real do usuário pode ser codificado sobre a faixa magnética 108. O número de conta real do usuário é acessível usando leitores de contato convencionais 114 capazes de ler faixas magnéticas.

10 Em concretizações preferidas, a primeira e segunda memórias usam tecnologias de armazenamento de dados diferentes. Por exemplo, a primeira e segunda memórias podem ser selecionadas de meio de armazenamento óptico, magnético, ou eletrônico, e podem ser diferentes. Por exemplo, a primeira memória pode usar um meio de armazenamento eletrônico (por exemplo, um chip de memória), enquanto a segunda memória
15 pode usar um meio de armazenamento magnético (por exemplo, uma faixa magnética 108).

Figura 3 é um fluxograma de alto nível ilustrando uma concretização de um método 300 de executar um processo de transação de número de conta assegurado. No método 300 pode ser entrado na etapa 301 quando, por exemplo, um dispositivo de leitor de proximidade 110 interroga por modo sem fio um dispositivo de consumidor de proximidade portátil 102. Na etapa 302, um usuário inicia a criação de uma mensagem de pedido de autorização para, por exemplo, comprar bens ou serviços de um comerciante
20 112 (por exemplo, o usuário está tentando comprar uma peça de roupa usando o dispositivo de consumidor de proximidade portátil 102), passando o dispositivo de consumidor de proximidade portátil 102 perto do dispositivo de leitor de proximidade 110. O dispositivo de leitor de proximidade 110 interroga por modo sem fio o dispositivo de consumidor de proximidade
25

portátil 102. Na etapa 304, o dispositivo de consumidor de proximidade portátil 102 responde a protocolos de interrogação válidos (por exemplo, buscar instruções de número de conta, buscar instruções de ID de usuário, etc.) transmitindo por modo sem fio informação ao dispositivo de leitor de proximidade 110. A informação pode incluir um número de conta assegurado 5 junto com outros dados, tal como uma data de expiração da conta do usuário. O leitor de dispositivo de proximidade 110 então cria uma mensagem de pedido de autorização incluindo o número de conta assegurado, ID de comerciante, identificador de tipo de transação de POS, e a quantia de compra, e é transmitida do comerciante 112 para o adquirente 116 na etapa 10 304. Por exemplo, o comerciante 112 pode transmitir o número de conta assegurado, o ID de comerciante, o tipo de transação de POS, a identificação do usuário, a data de expiração, e similar ao adquirente 116. Na etapa 306, o adquirente 116 transmite a informação recebida do adquirente 116 ao sistema 15 de processamento de pagamento 120.

Na etapa 308, o número de conta assegurado é convertido ao número de conta real do usuário. Por exemplo, como descrito acima, quando um número de conta assegurado é recebido pelo sistema de processamento de pagamento 120, uma máquina de conta assegurada 122 converte o número de 20 conta assegurado para o número de conta real do usuário. Em uma concretização, a máquina de conta assegurada 122 pode pesquisar um banco de dados de números de conta assegurada para achar o número de conta real do usuário. Alternativamente, um algoritmo de conversão pode ser usado para converter o número de conta assegurado ao número de conta real do usuário.

25 Se o número de conta real não for achado, na etapa 309, o método 300 procede à etapa 316 e, por exemplo, emite um protocolo inválido de transação para o sistema de processamento de pagamento 120. Por exemplo, se o número de conta real não for achado, o sistema de processamento de pagamento 120 pode alertar o emissor 130, o adquirente

116, e/ou o comerciante 112 que a transação não está autorizada. Concebivelmente, depois de tentar usar a autorização sem contato, o usuário, estando desavisado do número de conta assegurado, pode tentar a transação usando o número de conta real do usuário por entrada por um operador ou usando um leitor de contato 114.

Na etapa 310, se o número de conta assegurado for válido, a mensagem de pedido de autorização incluindo o número de conta real do usuário, o ID de comerciante, o tipo de transação de POS, e a quantia de compra junto com outros dados de transação ao emissor 130. Por exemplo, o sistema de processamento de pagamento 120 pode transmitir o número de conta real do usuário, o número de conta assegurado, e o tipo de transação de POS, junto com outros dados de transação para o emissor 130. Na etapa 312, se a transação não estiver autorizada, por exemplo o usuário não tem crédito suficiente para a compra, o método 300 procede à etapa 316. Porém, se a transação estiver autorizada, por exemplo, o emissor 130 autorizou a transação, o método 300 procede à etapa 313. Então na etapa 313, uma mensagem de resposta de autorização é enviada ao comerciante 112 informando o comerciante 112 e o usuário se ou não a transação está autorizada. Na etapa 314, é a transação compensada e paga usando procedimentos convencionais. Por exemplo, ao término do dia, um processo de compensação e pagamento normal pode acontecer na etapa 314. Na etapa 318, o método 300 termina.

Figura 4 é um fluxograma de alto nível ilustrando uma concretização de um método 400 de executar uma transação financeira envolvendo um número de conta assegurado. O método 400 pode ser entrado na etapa 401 quando, por exemplo, um comerciante 112 transmite um pedido de autorização de compra a um sistema de processamento de pagamento 120. Na etapa 402, um número de conta assegurado é recebido. Por exemplo, um sistema de processamento de pagamento 120 recebe um número de conta

assegurado e tipo de transação de POS de um adquirente 116. Na etapa 404, o método 400 determina se o número de conta assegurado foi recebido de um dispositivo de consumidor de proximidade portátil 102 comunicando por modo sem fio com um dispositivo de leitor de proximidade 110. Em uma concretização, o método 400 usa um identificador de tipo de transação de POS para determinar se o número de conta assegurado foi recebido tanto usando uma transação de proximidade, ou foi recebido por outro meio, tal como um portal de comerciante da Internet, ou entrada manual no terminal de um dispositivo de leitor de proximidade 110 ou um leitor de contato 114, e similar. Se o número de conta assegurado não foi recebido por um dispositivo de leitor de proximidade 110, então o método 400 procede à etapa 406 e inicia um protocolo de fraude. Por exemplo, o protocolo de fraude pode ser usado para rastrear a transação por autoridades, instruir o sistema de processamento de pagamento 120 para negar a transação, e/ou enviar um relatório de estado ao emissor indicativo do fato que o número de conta assegurado foi adquirido por usuários não autorizados. Se na etapa 404 o método 400 determinar que o número de conta assegurado e o tipo de transação de POS estão corretos, o método 400 procede à etapa 408. O método 400 converte o número de conta assegurado para o número de conta real do usuário na etapa 408. Por exemplo, o sistema de processamento de pagamento 120 pode executar algoritmos para converter o número de conta assegurado ao número de conta real do usuário alguns dos quais são descritos aqui. Na etapa 410, o número de conta real do usuário e outros dados de verificação tais como data de expiração e identificação de cliente são transmitidos a um emissor 130 para autorização. Opcionalmente, na etapa 410, o número de conta assegurado também é transmitido ao emissor 130. O método 400 termina na etapa 414.

O método mostrado na Figura 4 pode ser combinado com quaisquer das etapas no método mostrado na Figura 3. O método também pode ser conduzido pela máquina de conta assegurada 122, pelo sistema de

processamento de pagamento 120, ou qualquer outra entidade adequada.

Qualquer das etapas descritas acima pode ser concretizada como código de computador em um meio legível por computador. O meio legível por computador pode residir em um ou mais aparelhos computacionais e pode usar qualquer tecnologia de memória de dados adequada.

A presente invenção pode ser implementada na forma de lógica de controle em software ou hardware ou uma combinação de ambas. A lógica de controle pode ser armazenada em um meio de armazenamento de informação tal como uma pluralidade de instruções adaptadas para dirigir um dispositivo de processamento de informação para executar um conjunto de etapas expostas na concretização da presente invenção. Baseado na exposição e ensinos providos aqui, uma pessoa de habilidade ordinária na arte apreciará outros modos e/ou métodos para implementar a presente invenção.

A descrição anterior é ilustrativa, mas não restritiva. Muitas variações da invenção se tornarão aparentes àqueles qualificados na arte na revisão da exposição. A extensão da invenção, portanto, não deveria ser dada com referência à descrição anterior, mas ao invés deveria ser dada com referência às reivindicações pendentes junto com sua extensão completa ou equivalentes.

Uma recitação de "um" "uma" ou "o" é pretendido que significar "um ou mais", a menos que especificamente indicado o contrário.

Todas as patentes, pedidos de patente, publicações, e descrições mencionadas acima estão incorporados aqui por referência na sua totalidade para todos os propósitos. Nenhum é admitido ser arte anterior.

REIVINDICAÇÕES

1. Método para usar um número de conta assegurado para processar tipos de proximidade de transações financeiras sem fio, caracterizado pelo fato de incluir:

5 receber uma mensagem de pedido de autorização, em que a mensagem de pedido de autorização inclui um número de conta assegurado, em que a mensagem de pedido de autorização se originou de uma interação sem fio entre um dispositivo de consumidor de proximidade portátil incluindo um número de conta real, um módulo de transmissão sem fio, e uma memória
10 pré-carregada com o número de conta assegurado, e um dispositivo de leitor de proximidade incluindo um segundo módulo de transmissão sem fio, em que o número de conta assegurado está associado com o número de conta real, e em que o número de conta assegurado era transmitido por modo sem fio do primeiro módulo de transmissão sem fio no dispositivo de consumidor de
15 proximidade portátil para o segundo módulo de transmissão sem fio no dispositivo de leitor de proximidade; e

 determinar o número de conta real usando o número de conta assegurado depois de receber a mensagem de pedido de autorização incluindo o número de conta assegurado.

20 2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o número de conta assegurado só é transmitido por modo sem fio ao dispositivo de leitor de proximidade quando há uma transação financeira sem fio e em que o número de conta real é usado para transações não financeiras não sem fio.

25 3. Método de acordo com a reivindicação 1, caracterizado pelo fato de enviar uma mensagem de resposta de autorização depois que o número de conta real é determinado usando o número de conta assegurado.

 4. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o número de conta real é o número de conta de cartão de crédito

de um usuário, número de conta bancária, ou número de conta de cartão de débito.

5 5. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a mensagem de pedido de autorização inclui um identificador de tipo de transação sem fio.

6. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a mensagem de pedido de autorização foi criptografada previamente.

10 7. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o dispositivo de consumidor de proximidade portátil está na forma de um cartão, e em que o cartão tem uma faixa magnética incluindo o número de conta real.

8. Meio legível por computador, caracterizado pelo fato de incluir código para executar o método como definido na reivindicação 1.

15 9. Computador de servidor, caracterizado pelo fato de ser adaptado para executar o método como definido na reivindicação 1.

20 10. Método de acordo com a reivindicação 1, caracterizado pelo fato de pré-carregar o número de conta assegurado na memória e pré-carregar o número de conta real em um meio de armazenamento magnético no dispositivo de consumidor de proximidade portátil.

11. Dispositivo de consumidor de proximidade portátil para executar transações sem contato, caracterizado pelo fato de incluir:

um módulo de transmissão sem fio;

25 uma primeira memória incluindo um número de conta assegurado acoplada ao primeiro módulo de transmissão sem fio; e

uma segunda memória, em que a segunda memória inclui um número de conta real, em que o número de conta real está associado com o número de conta assegurado.

12. Dispositivo de consumidor de proximidade portátil de

acordo com a reivindicação 11, caracterizado pelo fato de que a primeira e segunda memórias usam tecnologias de memória de dados diferentes.

13. Dispositivo de consumidor de proximidade portátil de acordo com a reivindicação 11, caracterizado pelo fato de que a primeira
5 memória inclui uma chip de memória e em que a segunda memória inclui uma faixa magnética, e em que o dispositivo de consumidor de proximidade portátil está na forma de um cartão.

14. Dispositivo de consumidor de proximidade portátil de acordo com a reivindicação 11, caracterizado pelo fato de que o dispositivo de
10 consumidor de proximidade portátil é um cartão de transação financeira.

15. Dispositivo de consumidor de proximidade portátil de acordo com a reivindicação 11, caracterizado pelo fato de que a transação sem contato inclui uma transação financeira sem contato.

16. Sistema para executar transações de pagamento, caracterizado pelo fato de incluir:
15

um sistema de processamento de pagamento capaz de converter um número de conta assegurado ao número de conta real de um usuário, em que em resposta ao sistema de processamento de pagamento receber um pedido de autorização de transação incluindo o número de conta
20 assegurado, o sistema de processamento de pagamento determina o número de conta real do usuário associado com o número de conta assegurado, e verifica que o pedido de autorização de transação era associado com um tipo de proximidade de transação sem fio.

17. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de que a transação sem fio inclui um tipo de proximidade de transação financeira.
25

18. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de que a transação sem fio é recebida por modo sem fio de um dispositivo de consumidor de proximidade portátil incluindo o número de

conta assegurado e o número de conta real do usuário.

19. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de que o sistema de processamento de pagamento inclui código para converter o número de conta assegurado ao número de conta real do usuário.

5 20. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de que o pedido de autorização de transação inclui um indicador de transação indicativo de se o pedido de autorização de transação foi recebido pelo tipo de proximidade de transação sem fio.

10 21. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de que o sistema de processamento de pagamento inclui código para emitir um alerta se o número de conta assegurado não foi recebido por um tipo de proximidade de transação sem fio com um dispositivo de consumidor de proximidade portátil incluindo o número de conta assegurado.

15 22. Método para conduzir transações financeiras sem fio, caracterizado pelo fato de incluir:

receber uma mensagem de pedido de autorização que inclui um número de conta assegurado e um identificador de transação, em que a mensagem de pedido de autorização se originou de um dispositivo de consumidor portátil incluindo o número de conta assegurado e um número de conta real; e

20 determinar o número de conta real usando o número de conta assegurado quando o identificador de transação é indicativo que o número de conta assegurado se originou de uma transação sem fio com o dispositivo de consumidor portátil.

25 23. Método de acordo com a reivindicação 22, caracterizado pelo fato de que o número de conta real é utilizável para transações financeiras não sem fio.

24. Método de acordo com a reivindicação 22, caracterizado pelo fato de gerar um alerta quando o identificador de transação é indicativo que o número de conta assegurado se originou de um transação não sem fio.

25. Método de acordo com a reivindicação 22, caracterizado pelo fato de incluir :

gerar uma saída alfanumérica que inclui uma sequência predeterminada de caracteres alfanuméricos designados para serem comuns a ambos o número de conta assegurado e o número de conta real; e mascarar ou eliminar outros caracteres alfanuméricos da saída alfanumérica não designada a sequência predeterminada.

26. Método de acordo com a reivindicação 22, caracterizado pelo fato de receber uma mensagem de pedido de autorização inclui:

transmitir a mensagem de pedido de autorização para um adquirente;

transmitir a mensagem de pedido de autorização do adquirente para um sistema de processamento de pagamento;

verificar com o sistema de processamento de pagamento que o número de conta assegurado está associado com uma transação sem fio;

quando verificado que o número de conta assegurado está associado com a transação sem fio, enviar a mensagem de pedido de autorização junto com o número de conta real para um emissor para autorização; e

quando a transação financeira está autorizada, transmitir uma mensagem de autorização do emissor para o sistema de processamento de pagamento, adquirente e comerciante.

27. Método de acordo com a reivindicação 22, caracterizado pelo fato de determinar o número de conta real inclui examinar um banco de dados de números de conta assegurados, em que cada um dos números de conta assegurados está associado com um número de conta real respectivo.

28. Método de acordo com a reivindicação 22, caracterizado pelo fato de determinar o número de conta real inclui processar o número de conta assegurado com um algoritmo configurado para converter o número de conta assegurado ao número de conta real.

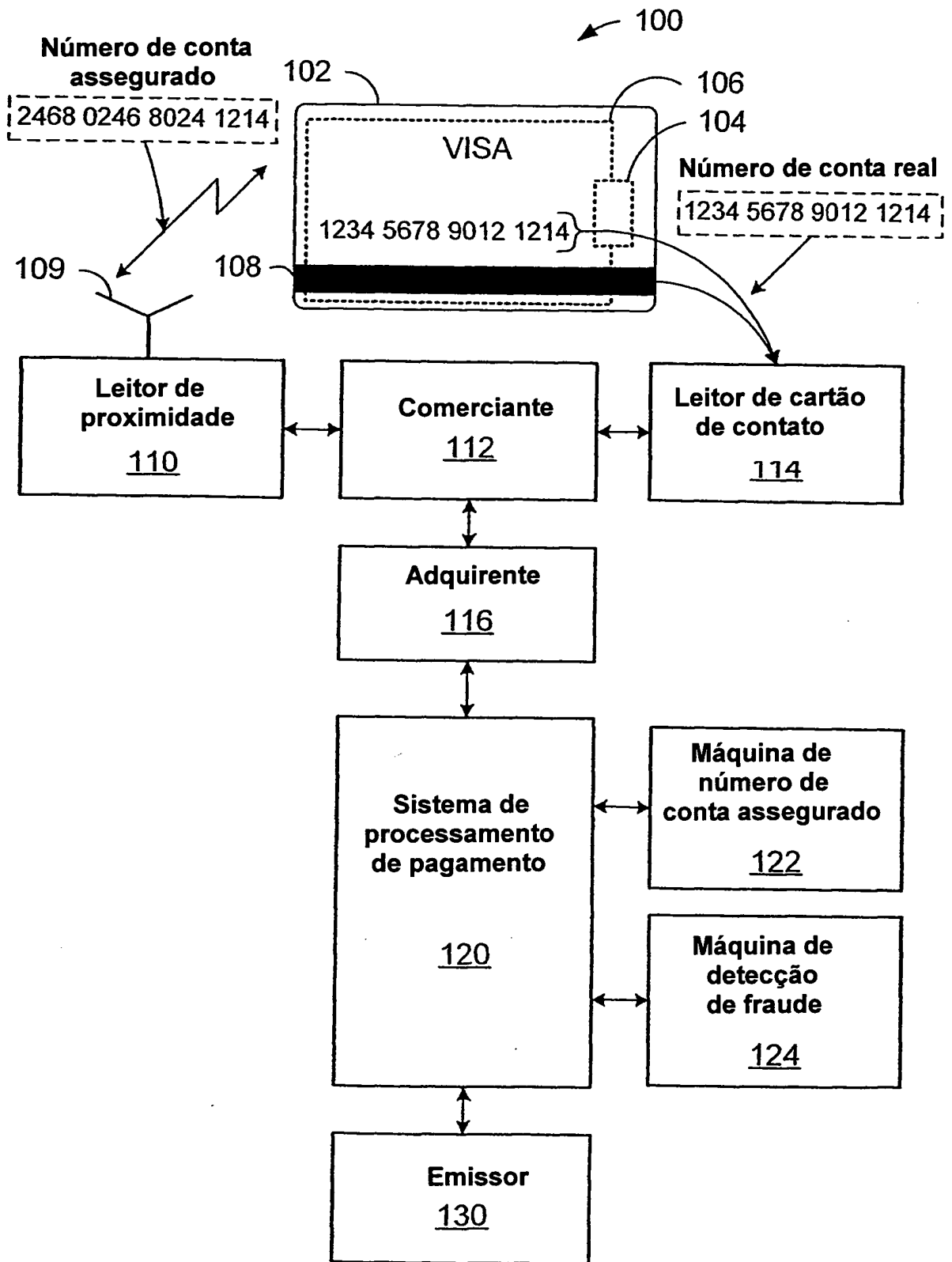


FIG. 1

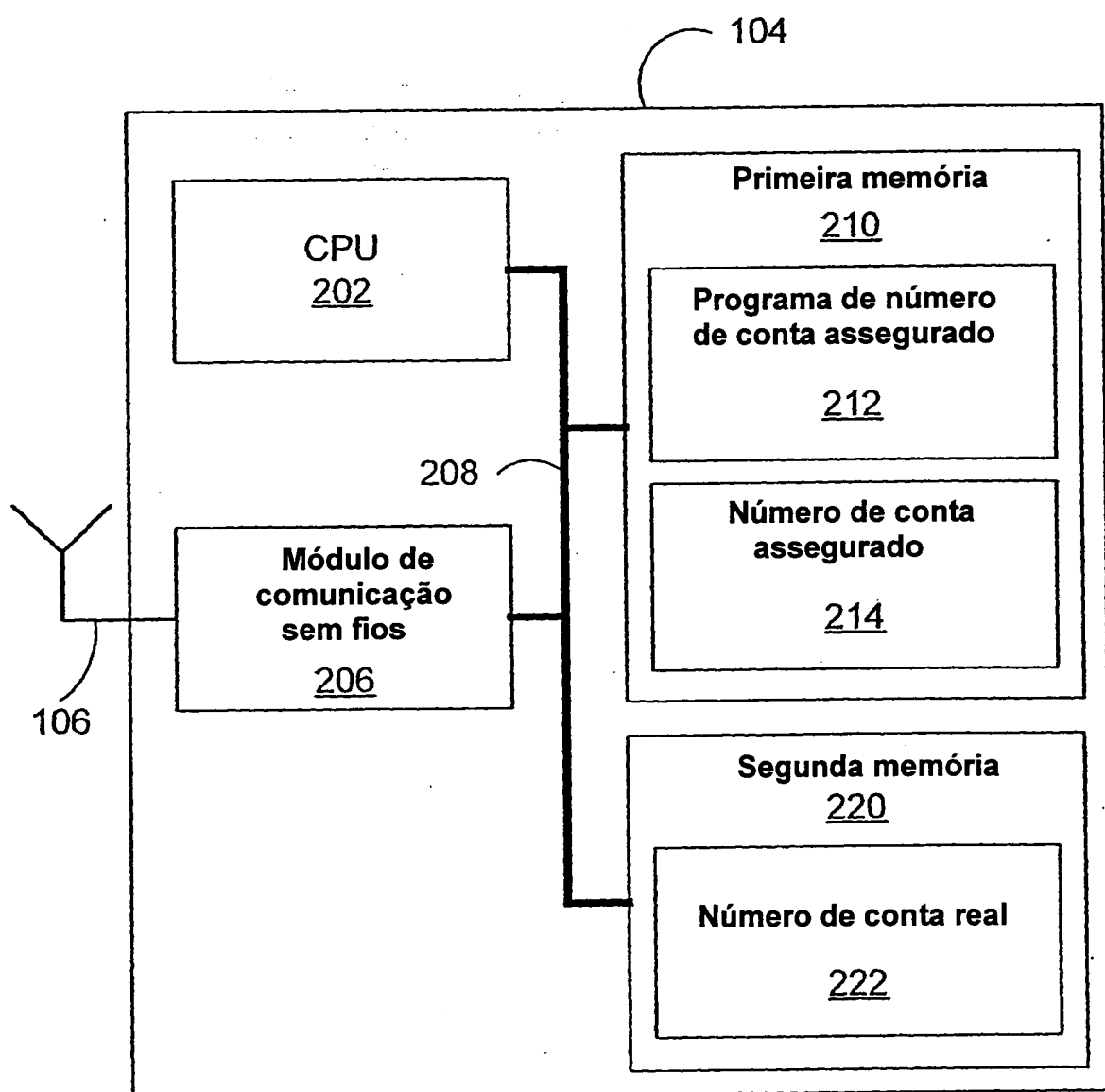


FIG. 2

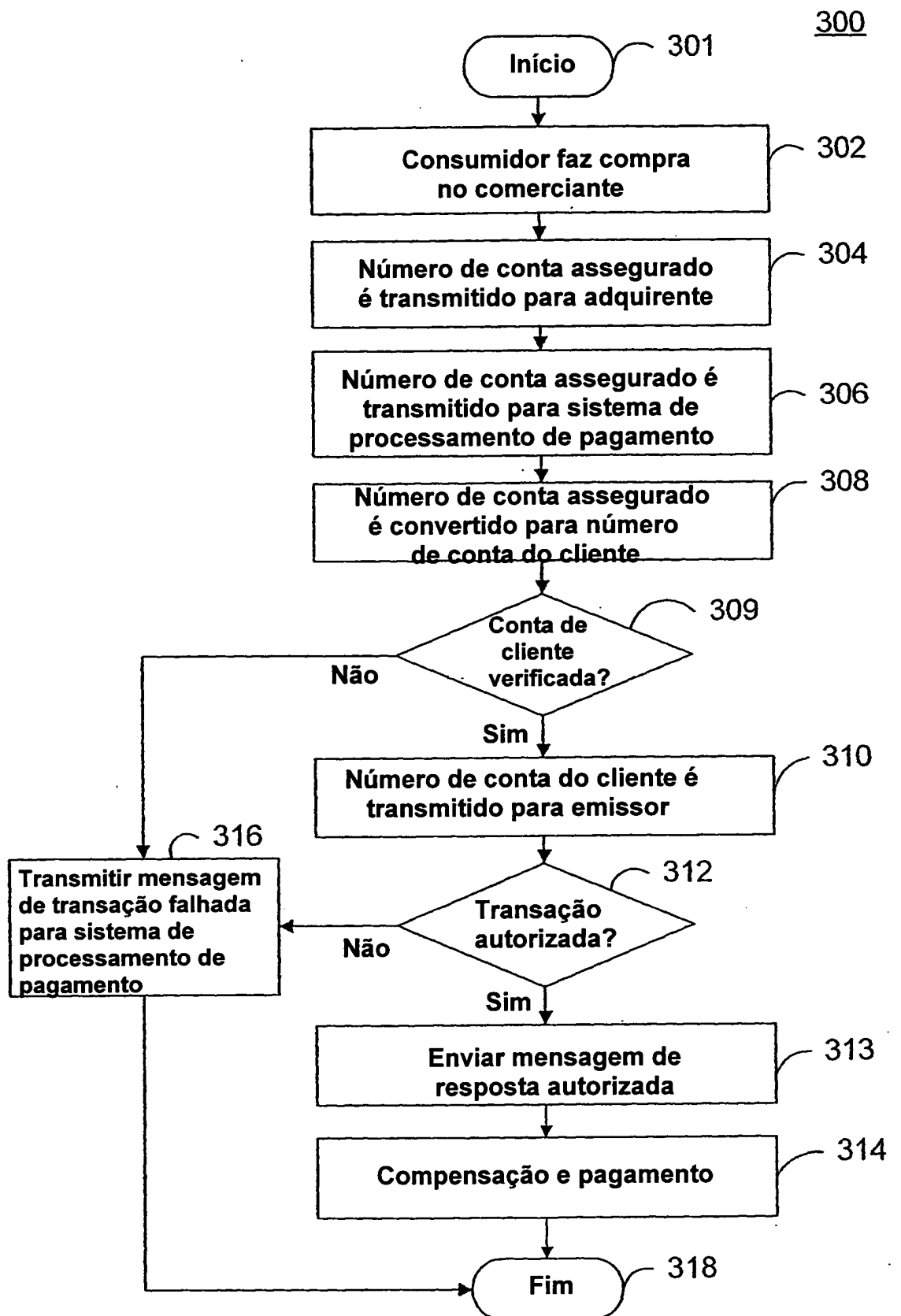


FIG. 3

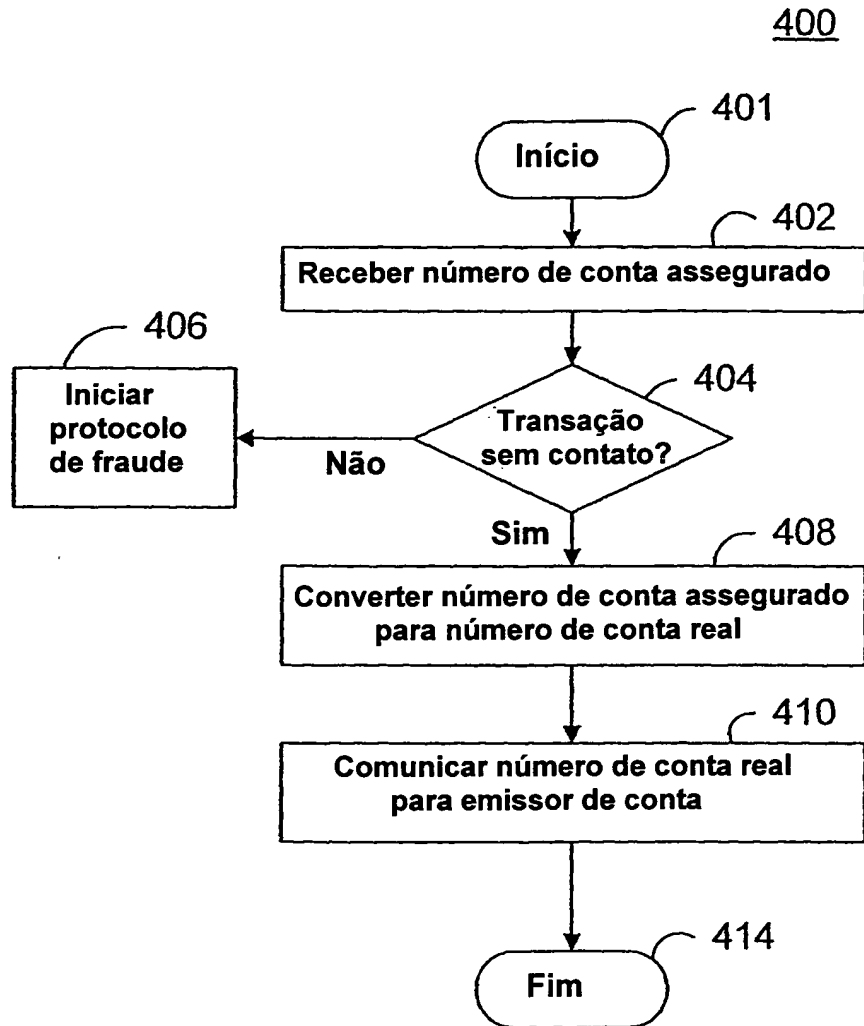


FIG. 4

RESUMO

“MÉTODO PARA USAR UM NÚMERO DE CONTA ASSEGURADO PARA PROCESSAR TIPOS DE PROXIMIDADE DE TRANSAÇÕES FINANCEIRAS SEM FIO, MEIO LEGÍVEL POR COMPUTADOR, COMPUTADOR DE SERVIDOR, DISPOSITIVO DE CONSUMIDOR DE PROXIMIDADE PORTÁTIL PARA EXECUTAR TRANSAÇÕES SEM CONTATO, SISTEMA PARA EXECUTAR TRANSAÇÕES DE PAGAMENTO, E, MÉTODO PARA CONDUZIR TRANSAÇÕES FINANCEIRAS SEM FIO”

Um método e sistema para usar um número de conta assegurado para processar tipos de proximidade de transações financeiras sem fio associadas com dispositivos de proximidade de consumidor portáteis são expostos. Em uma concretização, o método inclui receber um tipo de proximidade de pedido de transação financeira sem fio junto com um número de conta assegurado de um dispositivo de consumidor de proximidade portátil, tal como um cartão inteligente sem contato, converter o número de conta assegurado ao número de conta real do usuário, e transmitir o pedido de transação financeira junto com o número de conta real do usuário para o emissor do número de conta real do usuário para autorização e processamento.