



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

(21) **PI0613950-7 A2**

(22) Data de Depósito: 14/07/2006
(43) Data da Publicação: 22/02/2011
(RPI 2094)



* B R P I 0 6 1 3 9 5 0 A 2 *

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

(54) Título: **SISTEMA E MÉTODO PARA SELEÇÃO POR USUÁRIO DE REGRAS DE DETECÇÃO DE FRAUDE**

(30) Prioridade Unionista: 15/07/2005 US 60/709.049

(73) Titular(es): REVOLUTION MONEY, INC.

(72) Inventor(es): JASON JUDE HOGG, PATRICK GRAF

(74) Procurador(es): Alexandre Ferreira

(86) Pedido Internacional: PCT US2006027309 de 14/07/2006

(87) Publicação Internacional: WO 2007/011695 de 25/01/2007

(57) Resumo: SISTEMA E MÉTODO PARA SELEÇÃO POR USUÁRIO DE REGRAS DE DETECÇÃO DE FRAUDE Sistema e método para estabelecer sistema de regras de detecção de fraude inclui um primeiro cartão de transação através do qual acesso a fundos monetários é estendido e uma base de dados associando o dito cartão de transação a uma ou mais regras de detecção de fraude que regem governando acesso aos ditos fundos monetários pelo dito cartão de transação. O sistema também inclui um sistema de computação programado para permitir que um indivíduo proprietário do dito cartão de transação especifique as ditas regras de detecção de fraude governando acesso aos ditos fundos monetários pelo dito cartão de transação.

"SISTEMA E MÉTODO PARA SELEÇÃO POR USUÁRIO DE
REGRAS DE DETECÇÃO DE FRAUDE"

Este pedido está sendo depositado como um pedido
de patente internacional PCT em 14 de julho de 2006 em nome
5 de Gratis Card, Inc., uma corporação nacional dos EUA, re-
querente da nomeação em todos os países, exceto os EUA, e
Jason Jude Hogg e Patrick Graf, ambos cidadãos dos EUA, re-
querentes da designação nos EUA somente, e reivindica prio-
ridade para o pedido US 60/700.049, depositado em 15 de ju-
10 lho de 2005.

CAMPO TÉCNICO

A presente invenção diz respeito, no geral, ao
campo dos sistemas de transação financeira e de dados e,
mais particularmente, a um sistema e método para executar
15 transações financeiras e de dados sobre uma rede aberta.

ANTECEDENTES DA INVENÇÃO

A Figura 1 representa uma típica transação com
cartão de crédito como ela é atualmente realizada. Da forma
representada na Figura 1, o processo começa com o titular do
20 cartão de crédito 100 apresentando seu cartão de crédito pa-
ra um operador localizado em um dispositivo do ponto de ven-
da (por exemplo, máquina registradora) em um ambiente de
venda 102, representado pela operação 101. Em resposta, ti-
picamente, o operador "passa" o cartão por meio de uma lei-
25 tora de fita magnética que fica acoplada no dispositivo do
ponto de venda. Assim, a informação do titular do cartão,
incluindo o nome do titular do cartão e o número do cartão
de crédito, é transferida da mídia de armazenamento no car-

tão até o dispositivo do ponto de venda.

O dispositivo do ponto de venda combina a informação do titular do cartão com informação de transação (incluindo preço de venda total e identificação do comerciante), e
5 transmite o conjunto de dados combinados para um adquirente ou para um terceiro processador 104, representado pela operação 103. O terceiro processador 104 responde encaminhando o conjunto de dados para a rede de transação interna da operadora de cartão 106 (por exemplo, Visa, American Express,
10 etc.) (operação 105), por meio do que, o conjunto de dados é roteado até o banco emitente 108, mostrado pela operação 107.

Mediante a recepção do conjunto de dados, o banco emitente 108 verifica a transação financeira proposta em re-
15 lação a um conjunto de regras de crédito e aprova ou rejeita a transação financeira. Se for aprovada, a aprovação atravessa o caminho idêntico em seqüência inversa (operações 109, 111 e 113) até alcançar o dispositivo do ponto de venda no local de venda 102. Daí em diante, o banco emitente do
20 cartão 108 encaminha uma soma monetária igual ao preço de venda até o banco do comerciante 110 por meio de um conjunto de transações de dados similarmente complexo, como representado pela operação 115 (tipicamente, um processador é usado como um intermediário que encaminha a soma monetária até o
25 banco do comerciante 110). Na expiração do período de tarificação, o titular do cartão 100 paga o preço de venda (mais juros e taxas financeiras) pra o banco emitente do cartão 108 (operação 117).

O esquema supramencionado exhibe certas inconveniências. Por exemplo, em virtude de usar uma rede interna para comunicar dados entre o comerciante 102 e a entidade autorizadora (o banco emitente do cartão 108, neste caso), ocorrem despesas para estabelecimento e manutenção desta rede. Em última análise, esta despesa é paga pelo comerciante 102. Uma outra desvantagem do uso de uma rede interna é que quantidades relativamente pequenas de dados podem ser transmitidas a partir do dispositivo do ponto de venda do comerciante em função das limitações de infra-estrutura e de custos. Isto significa que, por exemplo, não pode ser apresentada ao titular do cartão informação detalhada a respeito de uma dada transação em seu extrato mensal. Em certas circunstâncias, tecnologias existentes de cartão de crédito provêem inclusão ocasional de informação relacionada a conteúdo de uma dada transação. Entretanto, tal informação não é reunida em um momento que é contemporâneo com a execução da transação. Em vez disto, ela é reunida bem depois da execução da transação. Dada esta demora na reunião de dados, certos avanços aqui apresentados não são atualmente possíveis no contexto das tecnologias de cartão de crédito atualmente existentes.

Outros inconvenientes também são inerentes ao esquema supramencionado. Tipicamente, informação de identificação pessoal é tanto impressa quanto modelada em relevo no cartão de crédito e codificada em sua fita magnética. Isto exige uma demora entre o momento em que um requerente de cartão de crédito é aprovado para um cartão de crédito e o

momento em que o requerente pode receber o cartão de crédito (a informação pessoal do requerente é impressa e codificada no cartão no período de intervenção). Adicionalmente, em virtude de o mecanismo de armazenamento usado pelos cartões de crédito ser uma fita magnética, uma leitora de fita magnética deve ter interface com o dispositivo do ponto de venda. Isto gera despesas adicionais, que tem a tendência de desencorajar pequenas empresas a aceitar tais cartões de crédito. Além do mais, atualmente existe um movimento ativo para introduzir dispositivo de identificação por radiofrequência (RFID) nos cartões de crédito. Uma iniciativa como esta também envolve investimento infra-estrutural significativo que, novamente, tem a tendência de desencorajar pequenas empresas a aceitar tais cartões de crédito.

15 SUMÁRIO DA INVENÇÃO

De acordo com uma modalidade, um método computado-rizado inclui associar, na dita base de dados, um cartão de transação com uma ou mais regras de detecção de fraude que governam o acesso aos ditos fundos monetários pelo dito cartão de transação. O método também inclui permitir que um indivíduo que possui o dito cartão de transação especifique as ditas regras de detecção de fraude que governam o acesso aos ditos fundos monetários pelo dito cartão de transação.

De acordo com uma outra modalidade, um sistema inclui um primeiro cartão de transação por meio do qual o acesso aos fundos monetários é estendido e uma base de dados que associa o dito cartão de transação com uma ou mais regras de detecção de fraude que governam o acesso aos ditos

fundos monetários pelo dito cartão de transação. O sistema também inclui um sistema computacional programado para permitir que um indivíduo que possui o dito cartão de transação especifique as ditas regras de detecção de fraude que governam o acesso aos ditos fundos monetários pelo dito cartão de transação.

DESCRIÇÃO RESUMIDA DOS DESENHOS

A Figura 1 representa uma típica transação de cartão de crédito.

10 A Figura 2 representa uma transação de cartão de crédito de acordo com uma modalidade da presente invenção.

A Figura 3 representa um método pelo qual um cartão de transação pode ser ativado quase simultaneamente com o momento no qual uma aplicação associada é aprovada.

15 A Figura 4 representa um ambiente de rede exemplar no qual um núcleo do sistema operacional da Figura 5 pode ser instalado.

A Figura 5 representa uma modalidade exemplar de um núcleo do sistema operacional que pode ser instalado na
20 modalidade de rede exemplar da Figura 4.

A Figura 6 representa uma modalidade exemplar de uma mensagem comunicada do núcleo do sistema operacional da Figura 5 até o sistema do software da Figura 7.

A Figura 7 representa uma modalidade exemplar de
25 um sistema do software que pode ser executado por um ou mais servidores operados por uma plataforma de transação.

A Figura 8 representa uma modalidade exemplar de um esquema implementado pela base de dados da Figura 7.

A Figura 9 representa uma modalidade exemplar de uma mensagem comunicada do sistema do software da Figura 7 até o núcleo do sistema operacional da Figura 5.

5 A Figura 10 representa uma modalidade exemplar de uma mensagem comunicada do núcleo do sistema operacional da Figura 5 até o sistema do software da Figura 7.

A Figura 11 representa uma modalidade exemplar de um método para recompensar um titular do cartão por distribuir cartões anônimos e não atribuídos a possíveis requerentes.
10

A Figura 12 representa uma modalidade exemplar de um método para permitir disputa de um custo associado com um item em uma transação.

A Figura 13 representa uma modalidade exemplar de um método para estabelecer ou modificar regras que governam o uso de um cartão infantil.
15

A Figura 14 representa uma modalidade exemplar de um método para estabelecer ou modificar regras de detecção de fraude selecionáveis pelo usuário.

20 A Figura 15 representa uma modalidade exemplar de um método para estabelecer ou modificar regras de modificação algorítmica de PIN selecionáveis pelo usuário.

A Figura 16 representa uma modalidade exemplar de um esquema para permitir troca intercomerciante de produtos.

25 A Figura 17 representa uma modalidade exemplar de uma troca de fundos pessoa-a-pessoa.

A Figura 18 representa uma outra modalidade exemplar de uma troca de fundos pessoa-a-pessoa.

DESCRIÇÃO DETALHADA

Várias modalidades aqui apresentadas serão descritas com detalhes em relação aos desenhos, em que números de referência iguais representam partes e montagens iguais por todas as diversas vistas. A referência a várias modalidades não deve ser interpretada como limitante do escopo do assunto em questão tratado, que é limitado somente pelo escopo das reivindicações anexas. Adicionalmente, não pretende-se que nenhum exemplo apresentado nesta especificação seja limitante, e eles apresentam algumas das muitas modalidades possíveis.

A Figura 2 representa uma transação financeira, por exemplo, uma transação de cartão de crédito, uma transação de cartão de débito, uma transação de cartão de valor armazenado, uma transação de cartão pré-pago, etc. de acordo com uma modalidade da presente invenção. Da forma mostrada na Figura 2, um titular do cartão 200 inicia a transação apresentando um cartão de crédito a um dispositivo do ponto de venda 202 ou a um operador que opera um dispositivo 202 como este (operação 201). Certamente, a transação pode ser iniciada no curso de uma transação eletrônica ordinária, tal como em virtude da entrada de informação do titular do cartão em uma página da Internet desenhada para comércio eletrônico. A título de ilustração somente, a transação descrita em relação às Figuras aqui expostas é descrita como ocorrendo em um dispositivo do ponto de venda (em uma loja de vendas) manuseado por um operador. Também, o cartão pode ser aqui chamado de "cartão de crédito", "cartão" ou "cartão de

transação" a título de referência rotineira. De fato, como discutido anteriormente, o cartão pode operar como um cartão de crédito, um cartão de débito, um cartão de valor armazenado e/ou um cartão de acesso a dados que permite o acesso a
5 várias formas de dados, tais como dados de assistência médica, dados de associação a clube, etc.

O cartão pode exibir as seguintes características. O próprio cartão pode incluir um substrato (isto é, o corpo do cartão) que pode ser polimérico ou de qualquer material
10 adequado. Uma mídia de armazenamento pode ficar disposta no substrato, ser embutida no substrato e/ou ser impressa sobre ele. A mídia de armazenamento pode ser exclusiva de leitura, tal como um código de barras impresso sobre o substrato, ou pode ser legível e gravável, tal como uma mídia de armazena-
15 mento magnética (por exemplo, fita magnética). De acordo com algumas modalidades, o cartão de crédito pode ter tanto um código de barras quanto uma fita magnética. De acordo com algumas modalidades, um número de cartão que identifica exclusivamente o cartão é codificado na fita magnética e/ou no
20 código de barras. Também, o cartão de crédito pode incluir um dispositivo RFID com um número do cartão nele armazenado. De acordo com uma modalidade, a mídia de armazenamento, seja ela um código de barras, uma fita magnética ou um dispositivo RFID, não contém, não codifica e/ou não armazena nenhuma
25 informação pessoal relacionada ao titular do cartão. De acordo com algumas modalidades, a(s) mídia(s) de armazenamento no cartão codifica, contém e/ou armazena somente um número de cartão que identifica exclusivamente o cartão. De a-

cordo com algumas modalidades, a(s) mídia(s) de armazenamento do cartão não contém, codifica e/ou armazena nenhum número de identificação pessoal (PIN).

Mediante o recebimento do cartão, o operador coloca o cartão em um dispositivo de entrada, tais como um dispositivo de leitura de código de barras, uma leitora de fita magnética ou um transceptor de RFID. Então, a informação codificada na mídia de armazenamento do cartão de crédito é lida. A seguir, o titular do cartão pode ser solicitado a inserir o número de identificação pessoal (PIN), que pode ser inserido no dispositivo do ponto de venda tanto pelo titular do cartão quanto pelo operador por meio de um dispositivo de entrada apropriado, tais como um teclado numérico, um teclado, uma tela sensível ao toque e/ou qualquer dispositivo adequado para a inserção de um PIN. Os dados do cartão de crédito, o PIN e a informação de transação do dispositivo do ponto de venda são usados para preencher uma pluralidade de pacotes de dados que podem ser "empacotados" como uma única unidade que constitui uma solicitação de autorização de uma transação proposta. Os vários pacotes são aqui discutidos com mais detalhes a seguir. A unidade embalada é encriptada de acordo com um esquema descrito, no geral, a seguir e é transmitida através de uma rede aberta, tal como a Internet, até a plataforma de transação 204, como mostrado na operação 203.

Da forma aqui descrita com mais detalhes, a plataforma de transação 204 pode manter um grau de integração com o banco emissor do cartão para que possa autorizar ou re-

jeitar todas, a maioria ou algumas transações (por exemplo, transações inferiores a uma quantidade limite de dólares) sem precisar de comunicação adicional com o banco emitente do cartão para chegar a uma decisão de autorização. Depois
5 de chegar a uma decisão de autorização ou de rejeição, a autorização / rejeição é retornada por meio da rede aberta (por exemplo, a Internet) até o comerciante 202, como mostrado na operação 205.

As modalidades supradescritas exibem certas vantagens
10 gens que devem ser destacadas, mas que não são essenciais para a prática das várias modalidades aqui descritas. Por exemplo, a comunicação entre o comerciante 202 e a plataforma de transação 204 ocorre por meio de uma rede aberta, tal como a Internet. Fazendo uso de uma rede aberta, a necessidade de elementos e/ou linhas de rede interna é eliminada
15 e/ou reduzida, significando que o custo da execução de cada transação é reduzido. Também, em virtude de a comunicação por meio de uma rede aberta, tal como a Internet, ser grátis, uma quantidade relativamente maior de dados pode ser
20 trocada entre o comerciante 202 e a plataforma de transação 204, permitindo maior resolução nas faturas, como descrito a seguir. Além do mais, a administração das regras bancárias definidas por um banco, tais como crédito disponível, taxas de juros e taxas gerais são tratadas pela plataforma, reduzindo a necessidade de comunicação constante entre a operadora de informação 202 e os vários bancos emitentes de cartão 206, que é conduzida por meio de consolidação / sincronização de sistema agendada, que também pode ser conduzida

por meio da rede aberta, desse modo, alcançando os mesmos benefícios.

Também deve-se destacar que, em algumas modalidades, o cartão de crédito não contém nenhuma informação pessoal. Especificamente, nenhuma informação pessoal é impressa, modelada em relevo ou de outra forma apresentada na face do cartão (por exemplo, o cartão não porta o nome do titular do cartão) e nem é codificada, armazenada ou contida na mídia de armazenamento do cartão. Este arranjo permite a colocação quase instantânea de um cartão de transação ativado nas mãos de um provável titular do cartão. Por exemplo, da forma mostrada na Figura 3, um fornecimento de cartões não atribuídos e anônimos pode ser provido, por exemplo, em um dispositivo do ponto de venda em uma loja de venda (operação 300). Por "anônimo", entende-se que o cartão não contém, codifica e/ou armazena nenhuma informação que identifica um indivíduo a quem o cartão pertence. Em outras palavras, ele não porta o nome de um indivíduo em sua superfície nem tem o nome ou outra informação de identificação relacionada a um indivíduo armazenada ou codificada em uma mídia de armazenamento do cartão. A mídia de armazenamento do cartão pode conter somente um número de cartão que identifica exclusivamente o cartão e não o número da conta.

Da forma mostrada na operação 302, um cartão anônimo é distribuído para um operador. Isto pode ocorrer, por exemplo, em um momento em que um cliente está prestes a realizar uma compra de um produto ou serviço. Considerando que uma fonte de cartões não atribuídos e anônimos é mantida em

um dispositivo do ponto de venda, um operador pode perguntar ao cliente se ele gostaria de solicitar um cartão de crédito ou começar a usar um cartão de valor armazenado / cartão pré-pago. Se o cliente responder afirmativamente, então, o
5 operador pode fornecer um cartão ao cliente. Certamente, um provável requerente pode obter um cartão anônimo de qualquer fonte, incluindo amigos ou outros titulares de cartão (discutido a seguir).

A seguir, o servidor da plataforma de transação
10 (discutido com detalhes a seguir) é provido com a informação de requisição do requerente e o número do cartão que identifica exclusivamente o cartão (operação 304). Considerando uma vez mais que o cartão anônimo é distribuído a um cliente em um dispositivo do ponto de venda, a informação de requisi-
15 são do cliente pode ser inserida pelo operador no dispositivo do ponto de venda, em seguida do que, ele se comunica por meio de uma rede, tal como a Internet ou rede telefônica, com o servidor da plataforma de transação. Adicionalmente, a informação de requisição pode ser recebida por um em-
20 pregado da plataforma de transação (por exemplo, por meio de uma chamada telefônica com o requerente) e pode ser inserida no servidor pelo empregado (ou pode ser inserida em um computador em comunicação com o servidor). Ainda adicionalmente, o requerente pode ser direcionado para uma página da In-
25 ternet em um quiosque na loja (por exemplo, o cartão pode portar o endereço de uma página da Internet) que é estruturado para permitir a inserção de informação de requisição. O requerente pode inserir diretamente sua informação de requisi-

sição na página da Internet, desse modo, comunicando sua informação de requisição com o servidor. No geral, a informação de requisição pode ser recebida pelo servidor de qualquer maneira.

5 A própria informação de requisição pode incluir a informação tipicamente necessária para conduzir uma verificação de crédito a fim de determinar a conveniência de crédito de um indivíduo. Por exemplo, tal informação pode incluir informação de identificação, tais como nome, endereço,
10 número de telefone e/ou número da previdência social do requerente, e também pode incluir informação do emprego, tais como local de trabalho, número de anos trabalhados em tal local de trabalho, etc. A informação de requisição pode constituir um conjunto mínimo de informação necessário para
15 o servidor tratar apropriadamente as transações financeiras do requerente. De acordo com algumas modalidades, o servidor tem acesso à base de dados que pode armazenar uma ampla variedade de informação relacionada ao requerente. Tal informação pode incluir informação de saúde, informação de contato de emergência, informação familiar, etc. (estas outras
20 formas de informação são discutidas a seguir). No momento em que a informação de requisição é recebida, as outras formas supramencionadas de informação podem não ser recebidas pelo servidor da plataforma de transação. Assim, o servidor usa a
25 informação de requisição para preencher uma ou mais tabelas na base de dados supramencionada relacionadas à requisição do requerente e, também, para preencher minimamente outras tabelas relacionadas à requisição e a outros assuntos. Se,

no final das contas, a requisição for aprovada, outros tipos de informação podem ser coletados do requerente / titular do cartão em um momento posterior, e as várias tabelas da base de dados podem ser preenchidas mais completamente.

5 Depois de receber a informação de requisição, o servidor insere informação na base de dados para associar o número do cartão do requerente com a informação de requisição do requerente (operação 306). Posteriormente, uma avaliação da requisição é realizada (operação 308). De acordo com
10 algumas modalidades, uma verificação de crédito pode ser realizada em relação ao requerente. A informação de requisição pode incluir uma quantidade suficiente de informação para consultar um serviço de grau de crédito (por exemplo, Fair Issaac Co.) para obter um grau de crédito para o indivíduo
15 (por exemplo, grau FICO). Por exemplo, o servidor da operadora de informação pode comunicar por meio de uma rede, tal como a Internet, com um serviço de grau de crédito para determinar um grau de crédito associado com um indivíduo. Se o grau de crédito exceder um limite em particular, então, a
20 requisição é aprovada, caso contrário, ela é rejeitada. De acordo com outras modalidades, a informação de requisição do requerente é comunicada por meio de uma rede, tal como a Internet, com um ou mais bancos emitentes de cartão. Cada banco emitente do cartão usa individualmente a informação de
25 requisição para realizar sua própria análise e concluir independentemente se rejeita ou aprova a requisição. De acordo com algumas modalidades, o servidor da plataforma de transação compara os termos de crédito oferecidos pelos bancos e-

mitentes do cartão que aprovaram o crédito e seleciona o banco emissor do cartão que oferece os melhores termos de crédito como o banco associado com o número do cartão. De acordo com outras modalidades, cada banco emissor do cartão
5 pode comunicar uma oferta, por exemplo, uma soma monetária que ele está disposto a pagar para a plataforma de transação adquirir a conta, e a plataforma de transação pode selecionar o banco que oferece a melhor oferta, por exemplo. De acordo com outras modalidades, mais de um banco pode estar
10 associado com o número do cartão, e permite-se que o requerente/futuro titular do cartão selecione entre os bancos para extensão de crédito em cada compra.

Independente de como a análise foi conduzida, se a avaliação indicar que a requisição está aprovada, então, o
15 servidor insere a informação na base de dados para associar regras com o cartão do requerente, como mostrado na operação 310. Por exemplo, um limite de gastos determinado com base no grau de crédito pode ser associado com o cartão (ou o banco emissor do cartão pode determinar o limite e comuni-
20 car o limite ao banco da plataforma de transação), dados antifraude genéricos também podem ser associados com o cartão, etc. (operação 312). Posteriormente, o cartão pode ser ativado (operação 314), significando que o cartão pode ser usado para executar uma transação, por exemplo, pode ser usado
25 para comprar um produto ou serviço no crédito (ou, como discutido a seguir, pode ser usado de uma outra maneira, tal como para realizar uma compra como um cartão de débito, um cartão de valor armazenado, etc.). Para facilitar a execução

de uma transação, o PIN atribuído ao cartão de transação é comunicado ao requerente aprovado. Por exemplo, o PIN pode ser comunicado ao titular do cartão por meio de uma mensagem do serviço de mensagens curtas, por meio de um correio eletrônico recebido por um dispositivo sem fio ou outro dispositivo, por meio do dispositivo do ponto de venda, etc. Este PIN pode ser tanto um PIN permanente quanto pode ser ativo somente por um período de tempo em particular, para um número de usos em particular, em um conjunto com transação que tem um valor monetário menor que uma quantidade em particular.

Se, por outro lado, a operação 310 indicar que a requisição está rejeitada, então, o cartão não é ativado (316), significando que o cartão não pode ser usado para executar uma transação.

As operações 300-314 podem ser realizadas quase instantaneamente. Por exemplo, de acordo com algumas modalidades, as operações 300-314 podem ser realizadas em menos de um minuto e, de acordo com outras modalidades, tais operações podem ser realizadas em menos de 30, 15 e/ou 5 segundos. Assim, por exemplo, um requerente pode requisitar um cartão ao mesmo tempo em que inicia uma compra em um dispositivo do ponto de venda em uma loja de venda e pode, na prática, ter o cartão ativado para que o requerente possa usar o cartão para realizar aquela compra (e também outras compras em outros comerciantes). Em virtude de o cartão ser anônimo, não há necessidade de o cartão portar impressão que identifica o titular do cartão, nem é necessário que a mídia

de armazenamento do cartão tenha tal informação de identificação ou PIN nela codificados. Assim, depois do processo de requisição, não existe período de espera para que o cartão seja impresso ou para que sua mídia de armazenamento seja codificada com informação que identifica o requerente.

Da forma descrita em relação à Figura 2, para realizar uma compra usando o cartão de transação aqui descrito, um dispositivo do ponto de venda (por exemplo, máquina registradora) pode ler um dado cartão, e pode comunicar a informação por meio de uma rede aberta até o servidor da plataforma de transação. A Figura 4 representa um ambiente de rede exemplar no qual o dispositivo do ponto de venda 202 da Figura 2 pode ficar residente. Como pode ser visto na Figura 4, uma dada loja de venda pode ter uma pluralidade de dispositivos do ponto de venda 202 ali situados. Cada dispositivo do ponto de venda 202 pode ser acoplado em uma rede de área local (LAN) 400. A LAN da Figura 4 é representada como sendo uma rede Ethernet a título de ilustração somente. A LAN 400 pode ser de qualquer estrutura e utilizar qualquer protocolo.

Os vários dispositivos do ponto de venda 202 comunicam com um servidor 402 por meio da LAN 400. O servidor 402 mantém uma base de dados 404 que armazena informação considerando todas as transações conduzidas por meio de cada um dos dispositivos do ponto de venda 202. (Tipicamente, cada transação é identificada por um identificador de transação discutido a seguir). O servidor 402 pode transferir informação para/de uma rede aberta 408, tal como a Internet,

por meio de um roteador 406.

O ambiente de rede da Figura 4 é exemplar e é apresentado a título de ilustração somente. Existem muitos outros ambientes que são conhecidos pelos versados na técnica. A Figura 5 representa um núcleo de sistema operacional da transação que é instalado, isto é, as várias unidades de software são armazenadas e executadas tanto no dispositivo do ponto de venda 202, quanto no servidor 402, quanto em alguma combinação dos dois quanto em qualquer dispositivo de computação em comunicação tanto com o dispositivo do ponto de venda quanto com o servidor 402. Aqui, o núcleo de sistema operacional da Figura 5 é discutido prosseguindo a partir da consideração de que ele está instalado no ambiente de rede da Figura 4, mas seus módulos são adaptáveis para uso em qualquer ambiente de rede, como é entendido pelos versados na técnica.

Em relação à Figura 5, o dispositivo do ponto de venda 202 é acoplado em um dispositivo de entrada 500, tal como uma fita magnética, uma leitora de código de barras ou um transceptor RFID. Durante a transação de uma compra, a leitora de fita magnética 500 é usada para ler a fita magnética no cartão. Certamente, se a mídia de armazenamento do cartão for um código de barras, então o dispositivo de entrada 500 pode ser incorporado como uma leitora de código de barras. Similarmente, se a mídia de armazenamento do cartão for um chip RFID, então o dispositivo de entrada 500 pode ser incorporado como um transceptor RFID. Quando o dispositivo de entrada 500 lê a mídia de armazenamento do cartão, é

lido um número do cartão que identifica exclusivamente o cartão. O dispositivo de entrada 500 também pode incluir um teclado numérico que pode ser usado pelo titular do cartão para inserir um número de identificação pessoal (PIN). O código PIN e o número do cartão são comunicados a partir do dispositivo de entrada 500 até o dispositivo do ponto de venda 202.

Um dispositivo do ponto de venda 202 tem a estrutura de um dispositivo de computação de uso geral. Em outras palavras, o dispositivo do ponto de venda 202 inclui os componentes tipicamente encontrados em um computador de uso geral, isto é, ele inclui um processador que é acoplado em um ou mais estágios de memória que armazena software e dados. O processador comunica, por meio de um barramento de entrada / saída (I/O), com vários dispositivos de entrada, saída e de comunicação, incluindo uma tela, tal como um monitor, e pode comunicar com um teclado, com um mouse ou outro dispositivo de apontamento, tal como uma plataforma sensível ao toque e/ou alto-falantes, para citar uns poucos tais dispositivos. Vários dispositivos periféricos também podem comunicar com o processador por meio do barramento I/O, incluindo um cartão de interface de rede, uma unidade de disco rígido ou outro dispositivo de armazenamento de dados em massa, unidades de mídia removíveis, tais como uma unidade de CD-ROM ou uma unidade de DVD (que pode ser tanto legível quanto gravável), uma interface sem fio, uma leitora de fita magnética, um leitora de código de barras, um transceptor RFID, etc. Entende-se que computadores empregam atualmente muitos arran-

jos de chips e arquiteturas. O dispositivo do ponto de venda 202 representa amplamente todos tais arranjos de chips e arquiteturas, e as várias modalidades do núcleo do sistema operacional e vários métodos de software aqui descritos podem
5 ser executados em todos os arranjos de chip e arquiteturas.

Um módulo extrator de código PIN e de número do cartão 502 pode ficar residente na memória do dispositivo do ponto de venda 202 ou em qualquer outro dispositivo em comunicação e/ou em rede como ele, e é executado pelo seu pro-
10 cessador. Por "módulo" entende-se uma unidade ou parte de software, tal como uma função, objeto, conjunto de funções e/ou objetos, e/ou um conjunto de instruções de computador (por exemplo, código de máquina) executável pelo processador do dispositivo do ponto de venda 202. Certamente, a funcio-
15 nalidade provida por um módulo também pode ser empregada pelos esforços cooperativos de um ou mais circuitos integrados de aplicação específica (ASICs) ou pelos esforços cooperati- vos de um ou mais ASICs e módulos de software armazenados em um dispositivo de memória e executados por um processador.
20 Mediante o dispositivo de entrada 500 comunicar o código PIN e o número do cartão com o dispositivo do ponto de venda 202, o módulo extrator 502 lê o número do cartão e o código PIN a partir do conjunto de dados comunicado do dispositivo de entrada 500 até o dispositivo do ponto de venda 202. Como
25 discutido a seguir, o módulo extrator 502 comunica o código PIN e a informação do número do cartão com outros módulos de software que podem, de acordo com algumas modalidades, ser armazenados e executados pelo servidor 402.

O dispositivo do ponto de venda 202 comunica com uma base de dados 404 que é gerenciada pelo servidor 402. Uma interface de aplicação (API) 504 é provida para permitir que o dispositivo do ponto de venda 202 interaja com a base de dados 404. De acordo com algumas modalidades, a base de dados 404 é organizada de acordo com um esquema que inclui uma pluralidade de tabelas estruturadas para armazenar informação relacionada aos itens que foram vendidos na loja. A base de dados 404 também pode armazenar outra informação. Por exemplo, se o comerciante em particular opera muitas lojas, a base de dados 404 pode armazenar informação relacionada aos itens que foram vendidos em todas as lojas de vendas ou em todas as lojas de vendas em uma região. Adicionalmente, a base de dados 404 pode armazenar informação relacionada ao inventário de mercadorias, à informação de fornecedor e a outra informação usada na operação do negócio em particular. Como a estrutura de rede da Figura 4, o esquema da base de dados 404 varia de comerciante para comerciante e pode variar de loja para loja, como é entendido pelos versados na técnica.

Embora o esquema empregado pela base de dados 404 possa variar de comerciante para comerciante, é costumeiro que a base de dados inclua uma tabela que armazena registros que descrevem os detalhes de cada transação. Uma tabela como esta é aqui descrita como uma "tabela de transação" 506. Tipicamente, uma tabela de transação 506 é organizada para identificar exclusivamente cada transação com um identificador de transação 508, isto é, o identificador de transação

508 pode ser a chave primária para a tabela de transação
506. Uma pluralidade de campos 510 pode estar associada com
cada identificador de transação 508. Estes campos 510 provê-
em armazenamento de informação relacionada a cada item in-
5 cluído na transação. Por exemplo, os campos podem incluir um
ou mais dos seguintes: (1) um número de unidade de manuten-
ção de estoque (SKU) de cada item incluído em uma transação;
(2) o preço de cada item incluído na transação; (3) uma des-
crição interna de cada item incluído na transação; (4) uma
10 descrição externa de cada item incluído na transação; (5)
uma descrição geral de cada item incluído na transação; (6)
uma categoria na qual cada item incluído na transação se en-
contra; (7) a taxa de vendas associada com cada item incluí-
do na transação; (8) a data na qual a transação ocorreu; (9)
15 a hora na qual a transação ocorreu; (10) um identificador
que indica a loja em particular na qual a transação ocorreu;
(11) um identificador que indica o dispositivo do ponto de
venda em particular no qual a transação ocorreu; (12) um i-
dentificador que indica o empregado que operou o dispositivo
20 do ponto de venda em particular na data e hora da transação;
(13) uma indicação do método de pagamento usado para reali-
zar a transação em particular, por exemplo, dinheiro em es-
pécie, cartão de crédito, etc.; (14) o preço total da tran-
sação; (15) um indicador do tipo de transação, por exemplo,
25 compra, reembolso, retorno, consulta de dados, etc.; e/ou
(16) qualquer outra informação que descreve os sujeitos e/ou
circunstâncias da transação. No geral, informação da varie-
dade supracitada, isto é, informação que vai além do preço

total, data, hora e/ou local (por exemplo, identificação do comerciante e cidade / estado) da transação, é chamada de "dados de nível três". Depois que um dispositivo do ponto de venda 202 varreu cada item envolvido em uma transação, uma técnica de pagamento pode ser selecionada. O dispositivo do ponto de venda 202 pode apresentar uma tela perguntando qual o tipo de transação será executada por meio do cartão de transação, por exemplo, se o cartão deve ser usado como um cartão de crédito, um cartão de débito e/ou cartão de valor armazenado (como mencionado previamente, o cartão de transação pode ser usado como um cartão de crédito no contexto de uma transação, como um cartão de débito em uma outra transação e como um cartão de valor armazenado no contexto de uma ainda outra transação). O dispositivo do ponto de venda 202 usa a API 504 para criar um novo identificador de transação 508 para fazer referência exclusivamente à transação que ele está executando. Então, o tipo de transação e os dados de nível três relacionados à transação podem ser armazenados na tabela de transação 506 em associação com o identificador de transação 508. De acordo com algumas modalidades, o extrator de PIN e do número do cartão 502 também captura o tipo de transação e distribui os dados do tipo de transação para o segundo módulo de encriptação 522, como discutido a seguir.

Um módulo monitor 512 interage com a API 504 para observar a criação de um novo identificador de transação 508 na tabela de transação 506. Mediante a observação da criação de um novo identificador de transação 508, o módulo monitor 512 chama o módulo de extração de dados 514 para iniciar sua

operação.

De acordo com algumas modalidades, o módulo de extração de dados 514 interage com a API 504 para extrair os dados de nível três, incluindo o identificador de transação associado com a nova transação. De acordo com outras modalidades, o módulo de extração de dados 514 interage com a API 504 para extrair menos que a extensão total dos dados de nível três. Por exemplo, o módulo de extração de dados 514 pode obter somente o identificador de transação e o preço total da transação da base de dados 404. A título de ilustração somente, o presente documento descreve o módulo de extração de dados 514 como obtendo a extensão completa dos dados de nível três da base de dados 404.

Para permitir que o módulo de extração de dados 514 obtenha dados da base de dados 404 no momento da instalação do núcleo do sistema operacional representado na Figura 5, o módulo de extração de dados é suprido com informação que permite tal extração. Por exemplo, o código e/ou espaço de dados do módulo de extração de dados 514 pode ser alterado à luz do nome da tabela de transação 506, e os nomes dos vários campos 510 dos quais devem-se capturar os dados.

À medida que o módulo de extração de dados 514 captura os dados de nível três, ele é inserido em uma região da memória 516 para transferência para o primeiro módulo de encriptação 520. Antes da transferência do primeiro módulo de encriptação 520, um módulo de suficiência 518 examina os dados capturados e interage com o extrator de PIN e número do cartão 502 para garantir que: (1) o módulo de extração de

dados tenha capturado pelo menos um preço total e um identificador de transação; e (2) o extrator de PIN e do número do cartão 502 tenha capturado o número do cartão e o PIN. Se os dados supramencionados não foram capturados, é indicado um erro e a operação do núcleo do sistema operacional em relação à transação é interrompida. Se, por outro lado, os dados supramencionados foram capturados, então, os dados armazenados na memória 516 são passados até a primeira unidade de encriptação 520.

10 A primeira unidade de encriptação 520 encripta os dados de nível três e os dados do tipo da transação (dados do tipo da transação são recebidos do extrator de PIN e número do cartão 502, como mostrado na Figura 5) usando o PIN capturado pelo extrator de PIN e número do cartão 502 como a
15 chave de encriptação, desse modo, criando um primeiro objeto encriptado 600. O primeiro objeto encriptado 600 é representado na Figura 6. O primeiro objeto encriptado 600 passa do primeiro módulo de encriptação 520 para o segundo módulo de encriptação 522.

20 O segundo módulo de encriptação 522 recebe o primeiro objeto encriptado 600 e anexa o número do cartão a ele, criando um conjunto de dados anexado (o número do cartão é recebido do extrator de PIN e número do cartão 502, como mostrado na Figura 5). Então, uma senha do comerciante é usada como uma chave para encriptar o conjunto de dados anexado, desse modo, obtendo um segundo objeto encriptado 602.
25 O segundo objeto encriptado 602 é representado na Figura 6. O segundo objeto encriptado 602 passa do segundo módulo de

encriptação 522 para o terceiro módulo de encriptação 524. De acordo com algumas modalidades, a senha do comerciante é um valor de 64, 128, 256, 512 bits, ou um valor de um outro comprimento apropriado para proteger o segundo objeto encriptado 602 de ser decriptado por um intruso, quando transmitido ao longo de uma rede aberta. Tipicamente, a senha do comerciante permanece um segredo conhecido somente por um conjunto seleto de empregados necessários no comerciante e na plataforma de transação. De acordo com algumas modalidades, a senha do comerciante é inserida no espaço de código e/ou dados do núcleo do sistema operacional no momento da instalação do núcleo do sistema operacional no servidor do comerciante 402.

O terceiro módulo de encriptação 524 recebe o segundo objeto encriptado 600 e anexa um identificador do comerciante, um identificador da loja e um identificador do dispositivo do ponto de venda nele, desse modo, criando um conjunto de dados anexado. O identificador do comerciante é um valor que identifica exclusivamente o comerciante (por exemplo, um valor que indica que a transação ocorreu em uma loja Alvo). O identificador da loja é um valor que indica exclusivamente a loja em particular na qual a transação está ocorrendo (por exemplo, um valor que indica em qual loja Alvo a transação está ocorrendo). O identificador do dispositivo do ponto de venda é um valor que identifica exclusivamente o dispositivo do ponto de venda em particular 202 no qual a transação está ocorrendo (por exemplo, um valor que indica em qual máquina registradora a transação está ocor-

rendo). O identificador do comerciante, um identificador da loja e um identificador do dispositivo do ponto de venda são obtidos a partir da base de dados 404 por meio da API 504. De acordo com algumas modalidades, no momento da instalação do núcleo do sistema operacional da Figura 5 em um servidor do comerciante 402, o nome da(s) tabela(s) e dos campos na base de dados 404 que contêm tal informação é inserido no terceiro módulo de encriptação 524 (por exemplo, inserido no espaço de código e/ou de dados do terceiro módulo de encriptação 524) para que ele possa interagir com a API 504 para obter tal informação. Então, o terceiro módulo de encriptação 524 encripta o conjunto de dados anexado com a chave pública associada com a plataforma de transação 204, produzindo o objeto de transporte 604. O objeto de transporte 604 é representado na Figura 6. De acordo com algumas modalidades, a chave pública é um valor de 64, 128, 256 ou 512 bits ou um valor de um outro comprimento apropriado para proteger o objeto de transporte 604 de ser decriptado por um intruso quando transmitido ao longo de uma rede aberta. O objeto de transporte 604 passa para um módulo de camada de soquete seguro (SSL) 526 junto com uma chave de encriptação SSL para uso pelo módulo SSL 526. De acordo com algumas modalidades, a chave de encriptação SSL supramencionada é gerada por um gerador de número aleatório e a chave pública pode ser diretamente embutida no terceiro módulo de encriptação 524.

O módulo SSL 526 recebe o objeto de dados de transporte 604 e usa a chave de encriptação SSL para encriptar o objeto de transporte, produzindo um objeto de trans-

porte encriptado 606. O objeto de transporte encriptado 606 é representado na Figura 6. Embora a Figura 5 represente a chave de encriptação SSL como sendo gerada por um gerador de número aleatório no terceiro módulo de encriptação 524, de acordo com outras modalidades, a chave de encriptação SSL pode ser gerada pelo módulo SSL 526.

A camada SSL 526 passa o objeto de transporte encriptado para o módulo de protocolo de Controle de transmissão / protocolo de Internet (TCP/IP) 528 para comunicar por meio da rede aberta 408 com o servidor da plataforma de transação (De acordo com o ambiente de rede exemplar da Figura 4, o objeto de transporte é comunicado como um ou mais pacotes roteados por meio do roteador 406 até a rede aberta 408.).

Uma modalidade exemplar de um sistema de software em execução no servidor da plataforma de transação é representada na Figura 7. O servidor da plataforma de transação é estruturado para incluir pelo menos elementos similares como um dispositivo de computação de uso geral. Em outras palavras, o servidor de plataforma de transação inclui os componentes tipicamente encontrados em um computador de uso geral, isto é, ele inclui um processador que é acoplado em um ou mais estágios da memória que armazena software e dados. O processador comunica, por meio de um barramento de entrada / saída (I/O), com vários dispositivos de entrada, saída e de comunicação, incluindo uma tela, tal como um monitor, e pode comunicar com um teclado, um mouse ou outro dispositivo de apontamento, tal como uma plataforma sensível ao toque e/ou

alto-falantes, para citar uns poucos tais dispositivos. Vários dispositivos periféricos também podem comunicar com o processador por meio do barramento I/O, incluindo um cartão de interface de rede, uma unidade de disco rígido ou outro
5 dispositivo de armazenamento de dados em massa, unidades de mídia removíveis, tais como uma unidade de CD-ROM ou uma unidade de DVD (que podem ser tanto legíveis quanto graváveis), uma interface sem fio, uma leitora de fita magnética, uma leitora de código de barras, um transceptor RFID, etc.

10 Entende-se que os servidores empregam atualmente muitos arranjos e arquiteturas de chip. Por todo este documento, o servidor da plataforma de transação é referido no singular, isto é, como se ele fosse uma única máquina. Certamente, na prática, o servidor pode ser composto por uma pluralidade de
15 servidores que cooperam para realizar a funcionalidade aqui descrita. Por exemplo, dois ou mais servidores podem realizar individualmente todas as funcionalidades aqui descritas e eles podem tratar clientes (isto é, vários núcleos do sistema operacional de transação instalados em vários locais),
20 como atribuído por um balanceador de carga. Também, dois ou mais servidores podem cooperar no sentido de que um primeiro servidor pode realizar um subconjunto de operações aqui descrito e pode comunicar com um segundo servidor que realiza um outro subconjunto das operações aqui descritas.

25 A descrição da funcionalidade da Figura 7 é provida em relação a uma transação de crédito a título de ilustração somente. Da forma aqui discutida a seguir, a mesma infra-estrutura pode ser usada para processar transações de

débito, transações de valor armazenado, transações de acesso a dados e combinações destas.

O sistema de software da Figura 7 inclui um módulo TCP/IP 700 que recebe um ou mais pacotes, a carga útil combinada dos quais constitui o objeto de transporte encriptado 606. O módulo TCP/IP 700 reconstitui o objeto de transporte encriptado 606 a partir de um ou mais pacotes e passa o objeto de transporte encriptado 606 para o módulo SSL 702. O módulo SSL 702 usa a chave de encriptação SSL para decriptar o objeto de transporte encriptado, produzindo o objeto de dados de transporte 604 (O módulo SSL 702 tem acesso à chave de encriptação SSL em virtude da negociação que iniciou a sessão SSL segura, como é entendido pelos versados na técnica). Então, o objeto de dados de transporte 604 passa para o primeiro módulo de decrptação 704.

O primeiro módulo de decrptação 704 tem acesso a uma base de dados 706 por meio de uma API 708. A base de dados 706 contém dados financeiros para cada titular do cartão e, também, outros dados, como descrito com mais detalhes a seguir. De acordo com algumas modalidades, o primeiro módulo de decrptação 704 acessa a base de dados 706 para obter a chave privada da plataforma de transação e, então, decrpta o objeto de transporte 604, produzindo o segundo objeto encriptado 602 e o identificador do comerciante, o identificador da loja e o identificador do registro anexados. De acordo com outras modalidades, o primeiro módulo de decrptação 704 tem a supramencionada chave privada embutida no seu espaço de código ou acessa a chave privada a partir de uma re-

gião da memória. Em qualquer caso, o segundo objeto encriptado 602 e o identificador do comerciante, identificador da loja e identificador do registro anexados passam para o segundo módulo de deciptação 710.

5 O segundo módulo de deciptação 710 também tem acesso à base de dados 706 por meio da API 708. O segundo módulo de deciptação 710 usa o identificador do comerciante que é passado para ele pelo primeiro módulo de deciptação 704 para obter a senha do comerciante. Por exemplo, o identificador do comerciante pode ser usado como uma chave para
10 acessar uma tabela na base de dados 706 para encontrar a senha do comerciante. Assim, o segundo módulo de deciptação 710 pode acessar uma tabela que relaciona o identificador do comerciante com a senha do comerciante e pode usar o identificador do comerciante como uma chave para obter a senha do
15 comerciante. Então, a senha do comerciante é usada para deciptar o segundo objeto encriptado 602, produzindo o primeiro objeto encriptado 600 com o número do cartão, o identificador do comerciante, o identificador da loja e o identificador do registro anexados. O primeiro objeto encriptado
20 600 e os supramencionados dados anexados passam para o terceiro módulo de deciptação 712.

 O terceiro módulo de deciptação 712 recebe os dados supramencionados, incluindo o número do cartão, e acessa
25 a base de dados 706 por meio da API 708. O terceiro módulo de deciptação 712 usa o número do cartão para obter o identificador do cartão e o PIN da base de dados 706. O número do cartão pode ser usado como uma chave para acessar uma ta-

bela que relaciona o número do cartão com um identificador do cartão e, tanto direta quanto indiretamente, com o PIN. Por exemplo, o número do cartão pode ser usado para acessar uma tabela que associa o número do cartão com o identificador do cartão e com um identificador do código PIN. Então, usando o identificador do código PIN, uma tabela que relaciona o identificador do código PIN com o PIN pode ser acessada a fim de obter o PIN. Versados na técnica entendem que o PIN pode ser armazenado em um formato encriptado para que ele não possa ser obtido por fraude. Mediante a restauração da tabela na qual ele está armazenado, o PIN é decryptado, considerando que a tarefa requisitante tem um nível de acesso apropriado para requisitar tal decryptação. Mediante a recepção do PIN, o terceiro módulo de decryptação 712 decrypta o primeiro objeto encriptado 600, produzindo os dados de nível três juntamente com o número do cartão, o identificador do comerciante, o identificador da loja e o identificador do registro (Certamente, como discutido em relação à Figura 5, a carga útil do primeiro objeto encriptado 600 pode, em alguns exemplos, incluir somente o preço total e um identificador da transação.).

Os dados supramencionados passam para o módulo de verificação de balanço 714, que, como os vários módulos de decryptação 704, 710 e 712, tem acesso à base de dados 706 por meio da API 708. Primeiro, o módulo de verificação de balanço 714 obtém o balanço e o limite de crédito atuais associados com o número do cartão da base de dados 706. Por exemplo, o módulo de verificação de balanço 714 pode acessar

uma tabela que contém informação com detalhes do cartão relacionada com um identificador do cartão. Então, usando o identificador do cartão, que foi obtido pelo terceiro módulo de deciptação 712, como uma chave para pesquisar o balanço e o valor de limite de crédito obtidos. A soma do balanço atual e do preço total da transação proposta pode ser rejeitada (discutido posteriormente a seguir). Caso contrário, o fluxo do processo para o módulo de verificação de fraude 716.

O módulo de verificação de fraude 716 tem acesso à base de dados 706 por meio da API 708. O módulo de verificação de fraude 716 obtém regras de indicador de fraude associadas com o número do cartão da base de dados 706. De acordo com algumas modalidades, algumas ou todas as regras podem ser determinadas pelo titular do cartão (isto é discutido a seguir). Também, algumas ou todas as regras podem ser regras do sistema que são geradas sem inserção do titular do cartão. Os parâmetros da transação proposta e de transações recentes podem ser comparados com as regras do indicador de fraude. Se um teste das regras do indicador de fraude der positivo, o titular do cartão pode ser contatado. O titular do cartão pode ser contatado por meio do telefone por um empregado da plataforma de transação (note que a informação de contato do titular do cartão, incluindo o número do telefone do titular do cartão está armazenada em uma tabela associada com a conta principal e o identificador do cartão, como mostrado na Figura 8). O titular do cartão pode ser solicitado a confirmar sua identidade (por exemplo, o indivíduo que a-

tende o telefone pode ser solicitado a identificar-se e pode ser solicitado sobre o PIN associado com o número do cartão) e também é solicitado a confirmar que a transação é legítima. Adicionalmente, o titular do cartão pode ser contatado por meio da operação de um módulo de serviço de mensagens curtas (SMS) 718. Por exemplo, o módulo SMS 718 pode transmitir uma mensagem SMS para o telefone celular do titular do cartão (este número está armazenado na base de dados 706 associada com o número do cartão), solicitando ao titular do cartão a confirmar que a transação proposta deve ser aprovada. Para permitir que transação confirmada seja aprovada, o titular do cartão deve responder afirmativamente e também deve inserir seu código PIN. O módulo SMS 718 recebe a mensagem de resposta e a retorna para o módulo de verificação de fraude 716. Se a mensagem de retorno indicar que a transação proposta não deve ser aprovada, então, a transação proposta é rejeitada (discutido posteriormente) e o cartão é congelado (também discutido posteriormente). Se a mensagem de retorno indicar que a transação é legítima e também contiver o PIN associado com o cartão, o fluxo de execução passa para o módulo de verificação de perfil 720.

O módulo de verificação de perfil 720 opera em cartões infantis. Um cartão "infantil" é um cartão que está associado com a mesma conta principal (discutido em relação à Figura 8) à qual um cartão do pai está associado. O efeito de tal associação é que o pai e qualquer número de cartões infantis associados que exploram os mesmos fundos, isto é, exploram a mesma linha de crédito, exploram o mesmo valor

armazenado, exploram o mesmo balanço de serviços ou produtos pré-pagos e/ou exploram a mesma conta de cheques ou conta bancária. O titular do cartão associado com o cartão do pai recebe um extrato que apresenta as transações de todas as

5 contas associadas com a conta principal, significando que o titular do cartão do cartão do pai recebe um extrato que apresenta as transações executadas por meio tanto do cartão do pai quanto de qualquer cartão infantil. O cartão do pai pode impor regras sobre as permissões de gastos do cartão

10 infantil, como discutido com mais detalhes a seguir. Por exemplo, considere a circunstância na qual um pai é um titular do cartão. O pai pode criar uma conta infantil para uso por seus filhos. A tarifa gerada pela conta infantil é acumulada na tarifa da conta do pai. O pai pode atribuir regras

15 para a conta infantil. Por exemplo, o pai pode associar uma regra com a conta infantil que permite que a conta infantil incorra em até um nível de débito escolhido por uma unidade de tempo escolhida (por exemplo, \$ 250 por mês). Outras regras incluem, mas sem limitações: (1) não permitir compras

20 de certos SKUs ou classes de SKUs (por exemplo, não permitir compras de SKUs que indicam que o item comprado é bebida alcoólica); (2) não permitir compras que ocorram em certos comerciantes, tipos de comerciantes e/ou categorias de comerciantes; (3) permitir somente compras que ocorram em certos

25 comerciantes, tipos de comerciantes e/ou categorias de comerciantes. Para este fim, de acordo com algumas modalidades, a base de dados 706 armazena uma ou mais tabelas que associam um tipo de comerciante e/ou categoria de comercian-

te para os vários identificadores de comerciante ali armazenados. O módulo de verificação de perfil 720 opera recuperando as regras (se houver) associadas com um número do cartão e testando a transação proposta em relação às regras. Se
5 alguma das regras for violada, o titular do cartão do cartão do pai pode ser contatado, como descrito com referência ao módulo de verificação de fraude 716, para permitir a transação.

Por exemplo, o módulo de verificação de perfil 720
10 pode operar acessando uma tabela que associa o identificador do cartão do(s) cartão(s) infantil(s) com o cartão do pai que o(s) controla. O módulo de verificação de perfil 720 pode examinar a tabela para determinar se o identificador do cartão (recuperado inicialmente pela terceira unidade de decriptação 712) é ali apresentado correspondendo a um cartão
15 do pai. Se ele não for ali encontrado, o cartão não é um cartão infantil e nenhuma regra imposta por um cartão do pai está associada com ele. Alternativamente, se ele for ali encontrado, ele é um cartão infantil e pode ter regras associadas com ele. Em uma circunstância como esta, a supramencionada tabela pode associar o cartão infantil com o valor que
20 pode ser usado como uma chave para uma ainda outra tabela que associa o valor supramencionado com um apontador que aponta para código executável que implementa as regras escolhidas para o cartão. Então, o código executável é executado
25 para determinar se alguma das regras está violada, como descrito anteriormente.

Se tanto o módulo de verificação de balanço 714,

quanto o módulo de verificação de fraude 716 quanto o módulo de verificação de perfil 720 indicar que a transação não deve ser permitida, então o controle passa para o módulo de rejeição/congelamento 722. O módulo de rejeição/congelamento 722 rejeita a transação e transmite uma mensagem para o dispositivo do ponto de venda indicando que a transação proposta foi rejeitada (detalhes considerando a estrutura de uma mensagem de retorno como esta até o dispositivo do ponto de venda são apresentados a seguir). Adicionalmente, se o módulo de verificação de fraude 716 indicar que a compra é fraudulenta, então, a conta associada com o cartão é congelada, significando que nenhuma transação futura será permitida até que o cartão seja reativado.

Se cada um do módulo de verificação de balanço 714, do módulo de verificação de fraude 716 e do módulo de verificação de perfil indicar que a transação deve ser permitida, então, o controle passa para o módulo de registro de transação 724. O módulo de registro de transação 724 insere os dados recuperados pelos três módulos de deciptação 704, 710 e 712, incluindo os dados de nível três, na base de dados 706. Por exemplo, um identificador de transação - diferente daquele atribuído pelo comerciante - é atribuído às transações. Um novo registro, identificado pelo identificador de transação recém-atribuído, é criado em uma tabela que relaciona detalhes relacionados a uma transação com o identificador de transação recém-atribuído. Posteriormente, os vários campos do novo registro são preenchidos usando os dados recuperados pelos três módulos de deciptação 704, 710 e

712, incluindo os dados de nível três (O identificador de transação do comerciante também é armazenado na supramencionada tabela em conjunto com o identificador de transação recém-atribuído, desse modo, preservando a associação entre o
5 identificador de transação da plataforma de transação e o identificador de transação do comerciante).

Da forma mencionada anteriormente, o dispositivo do ponto de venda localizado no comerciante é notificado da rejeição / aprovação da transação. De acordo com algumas modalidades, uma mensagem estruturada como mostrado na Figura
10 9 é transmitida por meio do módulo SSL 702 e do módulo TCP/IP 700 até o núcleo do sistema operacional previamente discutido em execução no servidor do comerciante 402. Como
15 a transação proposta foi aprovada ou rejeitada 900, se o identificador de transação é atribuído pela base de dados do comerciante 902, e pelo identificador do comerciante, pelo identificador da loja e pelo identificador do registro 904.

A mensagem da Figura 9 é recebida pelo módulo
20 TCP/IP 528 do núcleo do sistema operacional (Figura 5) e é passada para o módulo SSL 526, em seguida do que, ela é decriptada. A sua carga útil é transferida para o módulo de reconhecimento 530 que usa a API 504 para atualizar a base de dados 404 com a informação que considera a aprovação ou
25 rejeição (A indicação 900 se a transação proposta foi aprovada ou rejeitada é associada com o identificador de transação 902 do comerciante, que é incluído na mensagem da Figura 9). De acordo com algumas modalidades, no momento em que o

núcleo do sistema operacional é instalado no servidor do comerciante 402, o módulo de reconhecimento 530 é alterado para incluir a tabela apropriada e o nome do campo para a inserção de tal informação (por exemplo, o espaço de código e/ou de dados do módulo de reconhecimento 530 é alterado para incluir o nome da tabela e o nome do campo do local apropriado para a inserção de tal informação). Posteriormente, o identificador do comerciante, o identificador da loja e o identificador do registro 904 são usados para determinar como rotear a informação que considera a rejeição/aprovação até o dispositivo do ponto de venda apropriado 202, e o identificador de transação é usado para rejeitar/aprovar a transação apropriada.

Da forma descrita na discussão exposta, de acordo com algumas modalidades, os dados de nível três que são o sujeito de uma dada transação são coletados, comunicados com o sistema de software da Figura 7 e armazenados na base de dados 706 em um momento que é contemporâneo com a execução da transação. Isto provê certas vantagens que, embora notáveis, não são essenciais para a prática da invenção. Por exemplo, em virtude de os dados de nível três ser capturados e inseridos na base de dados 706 durante a execução da transação (em oposição a depois da execução da transação), o sistema do software pode examinar os dados de nível três e comparar tais dados de nível três em relação a várias regras para determinar se uma transação proposta deve ser aprovada ou rejeitada. Como discutido a seguir, um titular do cartão pode selecionar regras de detecção de fraude que, por exem-

plo, identificam uma transação proposta como sendo potencialmente fraudulenta se um produto ou classe ou categorias de produtos em particular forem o sujeito da transação. Evidentemente, tais regras não podem ser impostas se dados relacionados à identidade dos produtos que são o sujeito da transação estiverem tanto ausentes quanto não reunidos até depois que a transação tenha sido executada. Como também é discutido a seguir, um titular do cartão pode customizar regras que governam gastos admissíveis para um "cartão infantil". Por exemplo, um titular do cartão pode especificar que um cartão infantil está impedido de executar uma transação em que um produto ou classe de produto em particular é um sujeito desta. Novamente, tais regras não podem ser impostas se dados que consideram a identidade dos produtos que são o sujeito de uma dada transação estiverem ausentes ou não reunidos até depois que a transação tenha sido executada. Finalmente, em virtude de os dados de nível três ser reunidos e armazenados de forma contemporânea com a transação, pode ser apresentada a um titular do cartão informação que considera a identidade dos itens vendidos com qualquer cartão associado com seu cartão (incluindo, por exemplo, itens comprados por meio de um cartão infantil) e a identidade do número do cartão que conduziu tais transações. Tal informação pode ser provida em tempo real ou quase em tempo real, tal como por meio de uma página da Internet ou de uma central de atendimento.

De acordo com algumas modalidades, a base de dados 706 pode ser organizada da forma mostrada na Figura 8. Como

pode-se ver na Figura 8, a base de dados pode ser organizada para associar um número do cartão 800, isto é, um conjunto de dados que é codificado/armazenado/contido em uma mídia de armazenamento de um cartão de transação e que identifica exclusivamente este cartão com identificador de cartão 802. Um identificador do cartão 802 é um conjunto de dados (por exemplo, um número inteiro) que é associado exclusivamente com um número do cartão 800 na base de dados 706. Por sua vez, o identificador do cartão é associado com um número de conta principal 804.

O número de conta principal 804 é um conjunto de dados que é associado exclusivamente com todas as informações de conta 806 de cada conta que pode ser acessada por meio do cartão de transação e que também é associado com todas as informações do titular do cartão 808 que podem ser acessadas por meio do cartão. Por exemplo, o número de conta principal é associado com o balanço de cada conta que pode ser acessada por meio do cartão. Assim, ele pode ser associado com um balanço de crédito (como quando o cartão for usado como um cartão de crédito), um balanço de conta bancária (como quando o cartão for usado como um cartão de débito) e/ou um balanço de valor armazenado (como quando o cartão for usado como um cartão de valor armazenado, por exemplo, cartão presente, cartão de produtos e/ou serviços pré-pago, etc.). O número de conta principal 804 também é associado com todos os detalhes, por exemplo, dados de nível três, de todas as transações executadas por meio de cada conta que pode ser acessada por meio do cartão. Adicionalmente, o nú-

mero de conta principal 804 é associado com cada regra que governa o cartão, por exemplo, regras de juros, regras de pagamento com atraso, regras de detecção de fraude, regras de gastos de despesa infantil, etc. Ainda adicionalmente, o

5 número de conta principal 804 é associado com informação relacionada à instituição financeira amarrada a cada conta que pode ser acessada por meio do cartão, por exemplo, o banco que estende a linha de crédito por trás do uso do cartão como um cartão de crédito, etc. No geral, cada unidade de da-

10 dos exigida e/ou associada com a capacidade do cartão como um cartão de crédito, cartão de débito e/ou cartão de valor armazenado é associada com o número de conta principal, tanto direta quanto indiretamente.

O arranjo supramencionado apresenta certas vantagens que são notáveis, mas não são essenciais para a prática da invenção. Por exemplo, considerando que o cartão de transação associado com o número do cartão 800 foi roubado, um

15 outro cartão, com um outro número do cartão, tal como o número do cartão 810, pode ser ré-associado com o número de

20 conta principal (por meio de um novo identificador do cartão 812). Fazendo isto, todas as informações de conta 806 e informações de titular do cartão 808 permanece no local e nenhuma tal informação é perdida.

Uma outra vantagem que é inerente no arranjo da

25 Figura 8 é notável, mas não é essencial para a prática da invenção. Da forma mostrada na Figura 8, mais de um número do cartão 800 e 810 pode ser associado com o mesmo número de conta principal 804. Conseqüentemente, um titular do cartão

pode eleger possuir dois cartões de transação - um para uso pessoal e um para uso corporativo, por exemplo (Embora este exemplo descreva dois números do cartão 800 e 810 associados com um número de conta principal 804, inúmeros números do cartão 800 e 810 podem estar associados com o mesmo número de conta principal 804.). Assim, um único extrato ou página da Internet pode apresentar uma decomposição da conta 814 ao titular do cartão mostrando, por exemplo, os gastos totais para cada carta ou, ainda, apresentando, em uma base transação por transação, todos os dados de nível três (por exemplo, cada item e custo associado) para cada cartão.

De acordo com algumas modalidades, uma transação pode ser conduzida sem o uso de um cartão de transação e, em vez disto, ser conduzida por meio de um dispositivo sem fio, tais como um telefone celular e/ou um assistente digital pessoal. A título de ilustração somente, a seguinte modalidade exemplar é descrita em relação a um telefone celular. Da forma previamente descrita, a transação pode ser iniciada em um dispositivo do ponto de venda 202, onde os códigos de barras associados com os itens a ser adquiridos são varridos por um operador. Neste ponto, o operador pergunta ao titular do cartão seu número de telefone celular (ou, de outra forma, consegue o número do telefone celular, por exemplo, o titular do cartão faz uma chamada para um número específico que captura o número do telefone celular do titular do cartão e o comunica para o dispositivo do ponto de venda 202, para o servidor do comerciante 402 ou para um sistema computacional em comunicação tanto com o dispositivo do ponto de

venda 202 quanto como servidor do comerciante 402), e o número do telefone é inserido no dispositivo do ponto de venda 202.

Então, o dispositivo do ponto de venda 202 insere
5 os dados de nível três na base de dados 404, como descrito
previamente em relação à Figura 5. Novamente, isto faz com
que o módulo monitor 512 observe a criação de um novo identificador de transação 508 na tabela de transação 506, desse
modo, propagando o conjunto de eventos supradescrito com as
10 seguintes exceções. O primeiro módulo de encriptação 520 é
instruído a usar o número de telefone do telefone celular do
titular do cartão para encriptar os dados de nível três,
produzindo um primeiro objeto encriptado 1000, como mostrado
na Figura 10. Então, o segundo módulo de encriptação 522 a-
15 nexa o número do telefone celular no primeiro objeto encrip-
tado (em vez de ali colocar o número do cartão), e encripta
o conjunto de dados anexado com a senha do comerciante, como
supradescrito, produzindo o segundo conjunto de dados en-
criptado 1002. O restante das funções do núcleo do sistema
20 operacional funciona como supradescrito.

No servidor da plataforma de transação, a maior
parte do tratamento é similar àquele supradescrito em rela-
ção à Figura 7, com as seguintes exceções. Quando passou o
primeiro objeto encriptado e dados anexos, a terceira unida-
25 de de decríptação 712 detecta que um número de telefone ce-
lular foi inserido no lugar do número do cartão (por exem-
plo, tal como uma detecção pode ser feita em virtude do fato
de que um número de telefone celular e um número do cartão

de transação têm comprimentos diferentes). Mediante a detecção que um número de telefone celular foi inserido no lugar do número do cartão, a terceira unidade de decriptação 712 usa o número de telefone celular como a chave de decriptação para decriptar o primeiro objeto decriptado. Posteriormente, a terceira unidade de decriptação 712 invoca o módulo SMS 728 com o número de telefone celular. O módulo SMS 728 transmite uma mensagem SMS para o número de telefone provido. A mensagem SMS indica o preço total da transação e o nome da loja de venda na qual a transação proposta está sendo conduzida. A mensagem solicita ao usuário que confirme ou rejeite a transação. Se o usuário confirmar a transação, ele insere seu PIN no telefone e um pequeno aplicativo e/ou outra forma de código executável empacota o PIN com o número do cartão do usuário (o pequeno aplicativo e/ou outra forma de código executável é previamente alterado para incluir o número do cartão em seu espaço de código ou de dados), gerando uma resposta que indica que a transação proposta deve ser confirmada e incluindo o número do cartão do usuário e o PIN associado. De acordo com algumas modalidades, a mensagem de resposta que confirma ou rejeita a transação é comunicada por meio de uma conexão sem fio com a Internet estabelecida pelo dispositivo e é encriptada por meio do protocolo SSL. A mensagem de resposta é retornada para a terceira unidade de decriptação 712. Se a mensagem de resposta rejeitar a transação, então, a transação é recusada, como supradescrito em relação à Figura 7. Por outro lado, se a mensagem de resposta aprovar a transação, então, o terceiro módulo de decript-

tação 712 acessa a base de dados 706 para recuperar o PIN do usuário com base no número do cartão, como supradescrito. Se o PIN recuperado casar com o PIN inserido no telefone celular e for passado para o terceiro módulo de deciptação 712 por meio do módulo SMS 728, então, o processo continua como descrito previamente em relação à Figura 7 (isto é, a verificação de balanço, a verificação de fraude e a verificação de perfil são realizadas como usual).

O efeito do exposto é que um titular do cartão pode realizar uma compra simplesmente provendo seu número de telefone celular para um operador em um dispositivo do ponto de venda 202. Depois que o(s) item(s) a ser comprado(s) foi(s) varrido(s) pelo operador, o titular do cartão recebe uma SMS, pedindo ao titular do cartão para confirmar se o preço total está correto. O titular do cartão confirma respondendo ao SMS de maneira afirmativa e inserindo seu PIN.

De acordo com algumas modalidades, um titular do cartão pode utilizar um dispositivo sem fio, tal como um telefone celular, para realizar uma compra de um produto ou serviço de um vendedor que não tem um ponto de venda conectado arranjado para interagir com o núcleo do sistema operacional da Figura 5. O dispositivo sem fio é programado com um pequeno aplicativo que permite a inserção de uma soma monetária total da transação, de um identificador do comerciante e do número PIN associado com o cartão de transação do titular do cartão. De acordo com algumas modalidades, o pequeno aplicativo é configurado na instalação para ter acesso ao número do cartão do titular do cartão. Então, o pequeno

aplicativo combina o número do cartão, o identificador do comerciante, a quantidade total da transação e uma unidade de dados do tipo de transação que descreve o tipo de transação em um pacote que é encriptado primeiro usando o PIN como
5 uma chave de encriptação e, então, é encriptado usando SSL. No sistema do software da Figura 7, o pacote é decryptado, primeiro pelo módulo SSL 702 e, então, pelo terceiro módulo de decryptação 712. Posteriormente, o processo prossegue como previamente descrito.

10 Da forma previamente mencionada, o núcleo do sistema operacional da Figura 5 e o sistema de software da Figura 7 podem cooperar para executar várias espécies de transações e podem realizar tal variedade de transações variando os dados portados no objeto de transporte encriptado da Fi-
15 gura 6. Por exemplo, a infra-estrutura supramencionada pode cooperar para realizar uma "compra de clube privado". Uma compra de clube privado é uma compra conduzida em um comerciante que exige uma associação (por exemplo, Sam's Club, uma locadora de vídeo, etc.). Por exemplo, considere o cenário
20 em que um indivíduo deseja alugar um filme de uma locadora de vídeo. Tipicamente, uma locadora como esta exige a apresentação de um cartão de associação a fim de conduzir a compra. Tipicamente, o cartão de associação porta uma mídia de armazenamento (código de barras, fita magnética, etc.)
25 que codifica um número associado com uma conta de associação. Um cartão de associação como este fica obsoleto em vista da infra-estrutura aqui descrita.

Como uma etapa inicial, um titular do cartão pode

associar seu número de conta de associação (ou outro número de identificação associado, tal como o número codificado na mídia de armazenamento do seu cartão de associação) com sua conta principal. Quando está alugando o filme, o titular do
5 cartão apresenta um cartão de transação da espécie aqui divulgada tanto para realizar o aluguel do filme quanto para apresentar sua conta de associação. O empregado pode "passar" o cartão da forma supradescrita, colocando em funcionamento os eventos supradescritos. Entretanto, neste contexto,
10 os dados do tipo de transação são ajustados em um valor que indica que uma compra de clube privado está sendo realizada (Os dados de nível três portam dados que descrevem o título do filme que está sendo alugado, etc.). Assim, um objeto de transporte encriptado com um identificador do comerciante
15 que identifica o comerciante locador de filme, um identificador da loja que identifica a loja em particular, um identificador do ponto de venda que identifica o dispositivo do ponto de venda em particular, o número do cartão do cartão de transação, os dados de nível três supradescritos e os dados
20 do tipo de transação supradescritos são comunicados ao sistema de software da Figura 7.

Mediante recepção, o objeto de transporte encriptado que porta o sistema comporta-se da forma supradescrita, com a seguinte exceção: o sistema acessa uma tabela na base
25 de dados 706 que relaciona o número de associação do clube privado (ou outro número associado) com a conta principal e o identificador do cartão. O sistema adquire o número de associação supramencionado e retorna este número no pacote de

resposta da Figura 9, além dos elementos mostrados a esse respeito. Portanto, o dispositivo do ponto de venda é provido com informação de aprovação/rejeição que considera a transação financeira e também é provido com o número de associação do titular do cartão. Assim, a necessidade de completar uma transação de clube privado com dois cartões é eliminada.

A infra-estrutura supramencionada também pode ser usada para conduzir uma transação de aquisição de dados. Uma transação de aquisição de dados é uma transação na qual o cartão é usado para obter informação associada com o identificador do cartão e com a conta principal. Tal informação recuperada pode ser simples. Por exemplo, a informação recuperada pode apresentar uma indicação se um indivíduo é, de fato, um membro de uma organização (por exemplo, se um indivíduo é um membro de um plano de saúde). Alternativamente, a informação pode ser complexa, tal como indicando a informação de saúde do titular do cartão. No contexto de uma transação de aquisição de dados, a infra-estrutura se comporta da forma supradescrita, com as seguintes exceções que são descritas em relação a um titular do cartão que usa seu cartão para prover assistência médica a uma instituição de assistência médica (hospital, clínica, etc.).

Como uma questão inicial, o titular do cartão estabelece um conjunto de regras na base de dados 706 que identifica qual espécie de dados pode ser recuperada. Por exemplo, as regras descrevem a espécie de dados de assistência médica que pode ser recuperada do cartão pelas várias

instituições identificadas por seus respectivos identificadores do comerciante.

Na instalação de assistência médica, o cartão é “passado” para ler a sua mídia de armazenamento e a série de eventos previamente descrita ocorre. Entretanto, neste contexto, o titular do cartão pode não estar ciente, então o PIN a ser inserido pode ser “911” ou algum outro PIN pré-definido. Os dados do tipo de transação são ajustados em um valor para indicar que a transação de aquisição de dados está sendo realizada (Os dados de nível três podem ser nulos ou podem ser preenchidos com dados fictícios, como podem ser o identificador da loja e o identificador do ponto de venda. Entretanto, em alguns exemplos, estes campos são preenchidos para que uma mensagem de resposta possa ser roteada até o dispositivo de execução de transação apropriado na instalação de assistência médica.). Assim, o objeto de transporte encriptado com um identificador do comerciante que identifica a instalação de assistência médica, o número do cartão e os dados do tipo de transação supradescritos são comunicados com o sistema do software da Figura 7 (Novamente, em certos exemplos, o identificador da loja e o identificador do ponto de venda podem ser preenchidos.).

Mediante a recepção do objeto de transporte encriptado, o sistema comporta-se da forma supradescrita, com as seguintes exceções. Mediante a identificação de que o identificador do comerciante corresponde a uma instalação de assistência médica e de que os dados do tipo de transação correspondem a uma transação de aquisição de dados, o ter-

ceiro módulo de deciptação é evitado, já que os dados de nível três são nulos. Então, o sistema do software acessa a base de dados 706 para obter as regras que governam o acesso aos dados associados com o identificador do comerciante. Por exemplo, a base de dados 706 pode conter uma tabela que relaciona cada identificador do comerciante, conta principal e identificador do cartão com os dados do titular do cartão que podem ser retornados em resposta a uma transação de aquisição de dados. Então, o sistema do software implementa as regras, retornando os dados que são permitidos ser retornados à instalação de assistência médica, dadas as regras. Assim, o cartão de transação aqui descrito pode ser usado para prover qualquer variedade de informação a qualquer variedade de organização.

Para permitir as transações expostas, o módulo de interface inicial da Figura 7 pode prover uma página da Internet na qual um titular do cartão pode conectar-se. A página da Internet pode apresentar uma ou mais páginas da Internet estruturadas para permitir que o titular do cartão associe todos os dados com seu cartão, incluindo dados de assistência médica, dados de seguro, dados de associação em clube ou quaisquer outros dados, incluindo dados específicos de usuário. A página da Internet também pode apresentar uma ou mais estruturas de páginas da Internet para permitir que o titular do cartão associe regras que governam acesso a tais dados, por exemplo, em uma base comerciante-a-comerciante (entidade-a-entidade).

Alguns recursos do sistema descritos em relação às

Figuras 2-10 devem ser destacados, mas não são essenciais para a prática da invenção. Como pode-se ver na Figura 2, por exemplo, o sistema de transação não inclui nenhum ator de intercâmbio e, portanto, elimina componentes do sistema e
5 taxas financeiras a ele relacionadas. Por exemplo, se comparado com o sistema da Figura 1, pode-se ver que o sistema da Figura 2 não exige linhas ou elementos de rede privada. Assim, os atores de intercâmbio responsáveis pela criação e manutenção de tais linhas e elementos de rede são eliminados
10 do processo de execução de uma transação. Portanto, os custos ordinariamente pagos pelos comerciantes para a provisão de seus serviços de intercâmbio são eliminados. Entretanto, de acordo com algumas modalidades, um número mínimo de linhas e/ou elementos de rede pode ser utilizado.

15 A base de dados mantida pela plataforma de transação inclui tabelas com campos para a inclusão de limites de crédito, regras de fraude e outras regras ordinariamente impostas em uma base banco-a-banco ou operadora-a-operadora. O sistema do software da Figura 7 inclui uma interface inicial
20 726 que permite o acesso à base de dados pelos titulares de cartão e bancos emitentes de cartão. Um banco emitente de cartão pode estabelecer regras, por exemplo, regras de limite de crédito, regras de detecção de fraude, etc. associadas com um dado número do cartão por meio do módulo de interface
25 inicial 726. As regras estabelecidas pelo banco emitente do cartão ficam residentes na base de dados 706 em conjunto com o número do cartão ao qual as regras se aplicam. Portanto, o servidor da plataforma de transação não precisa comunicar

com os sistemas de informação do banco emissor de cartão com cada transação proposta a fim de rejeitar ou aprovar a transação. Em vez disto, o servidor da plataforma de transação pode atualizar periodicamente o sistema de informação do banco emissor de cartão (por exemplo, em uma base diária) depois de ter aprovado independentemente uma ou mais transações durante o período.

Também merece destaque, mas não é essencial para a prática da invenção, o fato de que a base de dados 706 pode conter uma tabela que relaciona o identificador do cartão com um identificador do banco. O identificador do banco indica a identidade da instituição financeira que corresponde a um dado cartão. Simplesmente trocando o identificador do banco na tabela supramencionada, o banco associado com um dado cartão é alterado. Assim, um titular do cartão pode transferir efetivamente seu balanço de um banco para um outro sem precisar trocar cartões de crédito (a plataforma de transação simplesmente muda o identificador do banco).

Similarmente, a base de dados 706 pode incluir uma tabela que associa um identificador de tipo de cartão com um identificador do cartão. O identificador de tipo de cartão identifica a(s) espécie(s) de transação(s) financeira(s) que é(s) suportada(s) pelo cartão. Em outras palavras, o identificador de tipo de cartão indica se o cartão é um cartão de crédito, um cartão de débito, um cartão de valor armazenado, um cartão de gerenciamento de assistência médica, outra forma de cartão ou uma combinação de algum ou de todos os expostos. Assim, um único cartão de transação pode ser usado

como um cartão de crédito em um contexto e como um cartão de débito em um outro contexto, por exemplo. Dito de uma outra forma, o esquema da base de dados apresenta um mecanismo pelo qual um número do cartão armazenado em uma mídia de armazenamento de um cartão e inserido na base de dados 706 diz respeito a um identificador do cartão. Por sua vez, o identificador do cartão diz respeito a um identificador de tipo de cartão que identifica o tipo de transação a ser suportado pelo cartão ou informação a ser acessada por meio do cartão.

10 O identificador de tipo de cartão e o identificador do cartão cooperam para dizer respeito a um conjunto de tabelas organizado e preenchido para permitir que o cartão aja como um cartão de crédito, como um cartão de débito, como um cartão de valor armazenado, como um cartão de informação de saúde, etc.

Por exemplo, da forma exposta, a base de dados inclui um conjunto de tabelas que contém informação suficiente para permitir que o cartão aja como um cartão de crédito. Estas tabelas incluem, entre outras informações, informação

20 que considera o limite de crédito do cartão, as regras de juros relacionadas ao cartão, as regras de taxas por atraso relacionadas ao cartão, a identidade do banco emissor do cartão relacionado ao cartão, informação de endereço que permite contato com os sistemas de informação do banco emissor do cartão (por exemplo, endereço IP, informação de porta, endereço físico, etc.) e informações semelhantes. Os dados nestas tabelas podem estar associados com um dado cartão pelo uso de um identificador do cartão, isto é, o iden-

25

tificador do cartão pode ser usado como uma chave nestas tabelas.

Um segundo conjunto de tabelas permite que o cartão aja como um cartão de débito. Estas tabelas incluem, entre outras informações, informação que considera o número da
5 conta de cheques e o número de roteamento da conta associada com o cartão, o balanço da conta de cheques e informações semelhantes. Novamente, os dados nestas tabelas podem ser associados com um dado cartão pelo uso de um identificador
10 do cartão, isto é, o identificador do cartão pode ser usado como uma chave nestas tabelas.

Um terceiro conjunto de tabelas permite que o cartão aja como um cartão de valor armazenado. Um cartão de valor armazenado é um cartão que provê acesso a um produto ou
15 serviço pré-pago (por exemplo, um cartão de chamadas telefônicas pré-pagas, um cartão presente, etc.). Estas tabelas incluem, entre outras informações, informação que considera a disponibilidade de balanço, a(s) loja(s) de venda na qual o balanço pode ser gasto, regras que consideram todas as
20 restrições de gastos do balanço e informações semelhantes. Novamente, os dados nestas tabelas podem ser associados com um dado cartão pelo uso de um identificador do cartão, isto é, o identificador do cartão pode ser usado como uma chave nestas tabelas. Um ainda outro conjunto de tabelas permite
25 que o cartão aja como um cartão de acesso ao registro de saúde. Um cartão de acesso ao registro de saúde é um cartão que permite acesso à informação de saúde armazenada em uma base de dados, tal como a base de dados 706 da Figura 7. Es-

tas tabelas incluem, entre outras informações, informação que considera seguro de saúde possuído pelo titular do cartão, seguro dentário possuído pelo titular do cartão, estatísticas vitais do titular do cartão, medicamentos tomados pelo titular do cartão, alergias do titular do cartão, procedimentos cirúrgicos submetidos ao titular do cartão, informação que considera o médico e os outros provedores de assistência médica do titular do cartão, registro de saúde pessoal, registro eletrônico médico, adjudicação de pagamento, cálculo e liquidação de copagamento e informações semelhantes. Novamente, os dados nestas tabelas podem ser associados com um dado cartão pelo uso de um identificador do cartão, isto é, o identificador do cartão pode ser usado como uma chave nestas tabelas.

Da forma discutida em relação à Figura 3, um esquema para a colocação rápida de um cartão de transação ativado na posse de um requerente foi descrita anteriormente. A Figura 11 apresenta um método pelo qual os atuais titulares do cartão podem distribuir cartões de transação em nome da plataforma de transação, e pode receber um incentivo para fazê-lo. Um titular do cartão que deseja agir como um distribuidor de cartões de transação pode solicitar um fornecimento de cartões de transação anônimos e não atribuídos. Em resposta, a plataforma de transação provê ao titular do cartão um fornecimento de cartões não atribuídos e anônimos como este (operação 1100). O titular do cartão distribui um dos cartões anônimos a uma pessoa que ele tem motivos para acreditar que gostaria de ser um titular do cartão (por e-

xemplo, um amigo, colega de trabalho, etc.), da forma mostrada na operação 1102. Tanto antes quanto depois de tal distribuição, o cartão distribuído é associado com o titular do cartão na base de dados 706 (operação 1104). Por exemplo,

5 uma tabela pode ser preenchida para associar os números de cartão de cada um dos cartões anônimos distribuídos e o identificador do cartão correspondente ao titular do cartão com a pessoa a quem os cartões foram distribuídos. A tabela também pode ser preenchida para incluir informação que identifica a pessoa a quem o titular do cartão distribuiu o cartão de transação não atribuído (isto é, o potencial requerente). A operação 1104 pode ser conduzida, por exemplo, pelo titular do cartão em uma página da Internet apresentada pelo módulo de interface inicial 726.

15 Depois da operação 1104, o procedimento para requisição prossegue como descrito em relação à Figura 3. Entretanto, da forma mostrada na operação 1106, no caso em que a pessoa a quem o titular do cartão forneceu um cartão anônimo é aprovada, pontos de incentivo são adicionados à conta do titular do cartão que fez a distribuição, considerando

20 que a informação de identificação do requerente casa com a informação de identificação fornecida pelo titular do cartão na operação 1104 (isto impede que o titular do cartão solicite um grande número de cartões de transação não atribuídos e deixe uma pilha deles, por exemplo, um centro de compras na esperança de ser creditado em relação a todas as requisições resultantes). Também, além do mais, ou como uma alternativa a pontos de incentivo, a conta do titular do cartão

pode ser creditada com uma soma monetária. A operação da operadora realizada na operação 1102 permite que o servidor da plataforma de transação identifique o cartão apropriado ao qual adicionar pontos de incentivo. Mediante aprovação de
5 um cartão de requerente, o sistema do software da plataforma de transação pode examinar uma tabela que relaciona os números de cartão não atribuídos aos identificadores do cartão dos titulares do cartão que receberam e distribuíram os cartões a fim de determinar se o número do cartão do cartão recém-aprovado está associado com o identificador do cartão de
10 um titular do cartão como este. Se ele estiver associado, então, o identificador do cartão correspondente é obtido. A seguir, uma tabela que associa o identificador do cartão com uma conta principal pode ser acessada para obter a conta principal do titular do cartão que distribuiu o cartão. Posteriormente, é acessada uma tabela que relaciona um balanço de pontos de incentivo com o número da conta principal e o balanço dos pontos de incentivo é atualizado para refletir os pontos de incentivo adicionados.

20 De acordo com algumas modalidades, a conta do titular do cartão que fez a distribuição é suprida com pontos, mesmo se a pessoa a quem o titular do cartão forneceu o cartão seja rejeitada (operação 1108). De acordo com algumas modalidades, os pontos de incentivo podem ser gastos em itens determinados para tal uso pelos comerciantes ou podem
25 ser usados no contexto de um programa de recompensas genérico. Se uma soma monetária for concedida à conta do titular do cartão, então, a soma monetária pode ser gasta em qual-

quer produto ou serviço.

Da forma discutida em relação à Figura 6, algumas modalidades do sistema de transação permitem comunicação de dados de nível três que descreve uma dada transação. Por exemplo, considerando que um titular do cartão realizou uma compra de sabonete, bebida gasosa e papel toalha por um total de \$ 15, a informação comunicada do núcleo do sistema operacional da Figura 5 até o sistema do software da Figura 7 inclui informação que identifica a transação incluindo sabonete a um custo de \$ 8, bebida gasosa a um custo de \$ 4 e papel toalha a um custo de \$ 3, perfazendo um total de \$ 15. O sistema do software da Figura 7 recebe a informação e, da forma descrita anteriormente, cria um identificador de transação que identifica a transação de \$ 15. Cada item comprado (e o custo associado com ele) é associado com o identificador de transação. Assim, de acordo com tais modalidades, a base de dados 706 contém dados que associam um comerciante em particular, loja de venda, registro, cada item comprado, o custo de cada item comprado e o custo total da transação. A preservação de tais dados de nível três permite certas funcionalidades até aqui impossíveis.

Um exemplo de funcionalidade permitida pela preservação de dados de nível três diz respeito a melhores resoluções de disputas. Atualmente, se um titular de um cartão de crédito revisar seu extrato e acreditar que uma taxa em particular está muito alta, o titular do cartão pode disputar a taxa. Continuando com o exemplo anterior, considerando que o extrato recebido pelo titular do cartão apresentou a-

quela transação totalizando \$ 25 em vez de \$ 15, o titular do cartão entrará em contato com sua operadora de cartão de crédito e declarará que aquela transação deve totalizar \$ 15 e não \$ 25. Conseqüentemente, toda a transação de \$ 25 será
5 identificada como sendo disputada, apesar do fato de que somente \$ 10 de \$ 25 esteja em desacordo, isto é, o titular do cartão reconhece que ele deve \$ 15, mas não acredita que ele deve \$ 25. Toda a transação deve ser disputada, em alguns casos, em virtude de uma operadora de cartão de crédito tradicional não receber informação detalhada relacionada aos
10 conteúdos de uma transação e, em outros casos, em virtude de o sistema do software empregado pela operadora de cartão de crédito tradicional não permitir disputa de um custo associado com o item em particular. Em resposta à disputa, o banco
15 emitente de cartão remove a transação de \$ 25 do balanço do titular do cartão (até que a disputa seja resolvida) e não transfere nenhum fundo para o banco do comerciante para a transação - nem mesmo os \$ 15 que o titular do cartão reconhece que ele de fato deve. Assim, o comerciante deixa de
20 receber os \$ 15 que ambas partes reconhecem ser devido ao comerciante, até que a quantidade de \$ 10 disputada seja resolvida.

De acordo com o método da Figura 12, disputas podem ser gravadas em uma base item-a-item, em oposição a meramente uma base transação-a-transação. Da forma mostrada na
25 Figura 12, informação que considera o item disputado pode ser obtida do titular do cartão (operação 1200). Por exemplo, o titular do cartão pode ligar para um empregado da

plataforma de transação e descrever o item disputado. Por exemplo, o titular do cartão pode descrever a data, o comerciante e o item disputado. No geral, o titular do cartão pode citar qualquer quantidade dos dados de nível três para
5 identificar exclusivamente o item disputado. O empregado acessa a base de dados usando a informação de nível provida até que a transação específica e o seu item disputado sejam identificados (O processo de identificação do custo em particular associado com um item em particular que é o sujeito
10 de uma transação pode ser realizado por meio de uma página da Internet apresentada pelo módulo de interface inicial 726. Por exemplo, depois de conectar-se, um titular do cartão pode selecionar uma opção para disputar um item em uma transação. Então, a página da Internet pode apresentar uma
15 série de campos, permitindo que o titular do cartão identifique o item em particular a ser disputado. Por exemplo, a página da Internet pode apresentar um primeiro campo que permite que o titular do cartão visualize todas as transações em um período de tempo em particular, por exemplo, que
20 ocorrem em um dado dia. Em resposta, pode ser apresentado ao usuário um conjunto de sumários de transação, por exemplo, uma lista de transações identificadas pela data, comerciante e quantidade total. A seleção de um sumário em particular faz com que a lista de cada item que é um sujeito da transação e os custos associados com eles sejam apresentados. Para
25 disputar um custo em particular, o titular do cartão pode selecionar o item a disputar e pode inserir uma explicação da disputa em um campo associado a ele.). Retornando ao e-

xemplo por meio do qual a disputa é inserida por meio de uma conversa o telef nica com um empregado, o identificador de transa o, da transa o da qual o item disputado   um constituinte,   encontrado (opera o 1202). A seguir,   criado
5 um registro em uma ou mais tabelas a fim de disputar o custo associado com um item identificado da transa o identificada (opera o 1204). Por exemplo, o registro pode disputar o custo associado com um item em virtude de o extrato refletir um pre o de compra de um item em um custo diferente daquele
10 que o titular do cart o acredita ser o custo verdadeiro. Tamb m, o registro pode disputar o custo associado com um item em virtude de o titular do cart o negar ter comprado o item. O registro que descreve a disputa pode incluir campos de dados para a descri o do item disputado e os motivos do
15 titular do cart o para disputar o custo associado com um dado item. O custo associado com o item disputado   removido do balan o associado com o cart o (opera o 1206), at  que tal tempo de disputa seja resolvido. Mediante a resolu o da disputa (al m do escopo desta divulga o, mas entendida pe-
20 los versados na t cnica), uma soma monet ria pode ser devolvida ao balan o associado com o cart o. Finalmente, como mostrado na opera o 1208, uma refer ncia ao registro criado na opera o 1204 pode ser inserida em uma tabela de disputas a ser resolvida.

25 Uma outra fun o que resulta da cole o dos dados de n vel tr s   a resolu o de faturas que podem ser alcan adas. De acordo com algumas modalidades, alguns ou todos os dados de n vel tr s podem ser inclu dos nas faturas. De a-

cordo com algumas modalidades, um titular do cartão pode se-
 lecionar a quantidade de dados de nível três apresentados no
 extrato associado com seu cartão. Por exemplo, a interface
 inicial 726 (Figura 7) pode apresentar uma página da Inter-
 5 net que permite que um titular do cartão selecione o nível
 de detalhes a ser apresentado no seu extrato. A página da
 Internet pode permitir, por exemplo, que o titular do cartão
 indique que todos os dados de nível três disponíveis sejam
 apresentados. Neste caso, o extrato apresenta todos os dados
 10 de nível três coletados para cada transação apresentada no
 extrato. A página da Internet também pode permitir que o u-
 suário selecione somente certos tipos de dados de nível três
 a ser apresentados, por exemplo, somente descrição dos pro-
 dutos/serviços, ou classificação de produtos/serviços, ou
 15 SKUs de produtos/serviços, etc. Assim, um extrato pode apre-
 sentar, para cada transação, uma descrição de cada um dos
 produtos/serviços que constitui cada transação, uma classi-
 ficação de cada produto/serviço que constitui cada transa-
 ção, a SKU de cada produto/serviço que constitui cada tran-
 20 sação, etc. Certamente, a página da Internet também pode
 permitir que o usuário eleja não ter dados de nível três a-
 presentados em seu extrato, em cujo caso, o extrato apresen-
 ta informação de transação típica (comerciante, data, quan-
 tidade total da transação).

25 A Figura 13 representa um método para estabelecer
 uma ou mais regras que governam um cartão infantil. Da forma
 mencionada anteriormente, um cartão infantil corresponde a
 uma conta que é uma sub-conta de um cartão do pai. Um titu-

lar do cartão de um cartão do pai pode estabelecer uma ou mais regras para um cartão infantil, por exemplo, conectando em uma página da Internet apresentada pelo módulo de interface inicial 726 do sistema do software da Figura 7 (operação 1300). Por exemplo, de acordo com algumas modalidades, a

5 página da Internet apresenta um campo para inserção do número do cartão do titular do cartão que está se conectando na página da Internet. A página da Internet também apresenta um campo para a inserção de uma senha e/ou PIN correspondentes

10 ao número do cartão. O titular do cartão insere seu número do cartão, senha e/ou PIN para se conectar. Desse modo, o sistema do software da Figura 7 identifica o usuário em particular da página da Internet correspondente a um número do cartão em particular. Alternativamente, a página da Internet

15 pode apresentar um campo para inserção de um nome de usuário associado com o titular do cartão (e, portanto, associado com seu número do cartão, etc.) e um outro campo para inserção de uma senha. O procedimento de conexão é executado mediante a inserção de dados nestes campos.

20 Mediante a conexão, é apresentado ao titular do cartão um menu que permite que o titular do cartão analise uma apresentação em tempo real do seu extrato, incluindo seu balanço, analise transações recentes relacionadas com qualquer conta que, por sua vez, é relacionada com seu número do

25 cartão, analise e/ou insira informação, tais como informação médica, informação de seguro, etc., relacionada com seu número do cartão, ajuste regras de fraude personalizadas para governar seu número do cartão, ajuste regras para alterar

automaticamente seu PIN de tempos em tempos, e/ou ajuste regras que governam uma conta infantil que corresponde à sua conta do pai. Da forma mostrada na operação 1302, o titular do cartão seleciona uma opção para ajustar regras que governam uma conta infantil. Em resposta a uma seleção como esta, da forma mostrada na operação 1304, a página da Internet apresenta uma lista de números de conta infantil correspondentes ao número do cartão do pai inserido na operação 1300. Por exemplo, o sistema do software da Figura 7 examina uma tabela em particular na base de dados 706 que associa, tanto direta quanto indiretamente, números do cartão infantis com números do cartão do pai. Todos os números de cartão infantil associados com o número do cartão do pai inseridos durante a operação 1300 são identificados e apresentados. De acordo com algumas modalidades, o nome do titular do cartão associado com o cartão infantil também é apresentado. Então, o titular do cartão do pai seleciona um número do cartão a partir da lista (operação 1306).

Posteriormente, a página da Internet apresenta campos para customização de regras que podem ser aplicadas ao cartão infantil. Por exemplo, a página da Internet pode apresentar campos que permitem que o pai associe uma regra com a conta infantil que permite que a conta infantil incorra até um nível de débito escolhido por uma unidade escolhida de tempo (por exemplo, \$ 250 por mês). Outras regras incluem, mas sem limitações: (1) não permitir compras de certos SKUs ou classes ou categorias de SKUs (por exemplo, não permitir compras de SKUs que indicam que o item comprado é

bebida alcoólica); (2) não permitir compras que ocorram em certos comerciantes, tipos de comerciantes e/ou categorias de comerciantes; e/ou (3) permitir somente compras que ocorram em certos comerciantes. O titular do cartão seleciona a
5 regra para aplicação ao cartão infantil e insere os dados de regra pertinentes (por exemplo, se o titular do cartão desejar limitar o cartão infantil a um limite de \$ 250 por mês, então, "250" é inserido em um campo de limite de despesa, e "mês" é inserido em um campo de unidade de tempo, por exem-
10 plo, pode ser selecionado a partir de um menu suspenso de frequência) (operação 1310). Finalmente, da forma mostrada na operação 1312, as regras selecionadas durante a operação 1310 são associadas com o cartão infantil.

Da forma mencionada em relação à Figura 13, um ti-
15 tular do cartão pode selecionar disparadores de fraude para ser atribuídos ao seu cartão e/ou a um cartão infantil. Como foi o caso com o estabelecimento de regras para um cartão infantil, os disparadores de fraude podem ser estabelecidos, por exemplo, por meio da conexão em uma página da Internet
20 apresentada pelo módulo de interface inicial 726 do sistema de software da Figura 7 (operação 1400, Figura 14). Da forma descrita anteriormente, de acordo com algumas modalidades, a página da Internet apresenta um campo para a inserção do número do cartão do titular do cartão que está se conectando
25 na página da Internet. A página da Internet também apresenta um campo para inserção de um nome de usuário, senha e/ou PIN correspondente ao número do cartão. O titular do cartão insere seu número do cartão, senha e/ou PIN para se conectar.

Desse modo, o sistema do software da Figura 7 identifica o usuário em particular da página da Internet correspondente a um número do cartão em particular.

Da forma discutida em relação à Figura 13, depois da conexão, o usuário seleciona uma opção para permitir a customização de disparadores de fraude. Posteriormente, a página da Internet responde apresentando ao titular do cartão várias categorizações de disparadores de fraude que podem ser aplicados no cartão (operação 1402). Por exemplo, da forma mostrada na caixa 1404, a presente invenção pode apresentar ao titular do cartão um conjunto de campos que permite a inserção de dados para a designação de: (1) um número máximo de dólares que pode ser gasto por unidade de tempo, com qualquer despesa acima do limite sendo considerada fraudulenta, por exemplo, qualquer despesa acima de \$ 5.000 em um dia é considerada fraudulenta; (2) um preço de compra máximo para uma única transação, com qualquer despesa acima do preço de compra máximo sendo considerada fraudulenta, por exemplo, qualquer despesa acima de \$ 5.000 é considerada fraudulenta; (3) classes em particular de produtos que são consideradas fraudulentas, por exemplo, uma transação que inclui dados de nível três com um SKU que indica que estão tentando comprar jóias é considerada fraudulenta; (4) um aumento nas despesas que excede um dado percentual, por exemplo, o sistema do software da Figura 7 pode rastrear as despesas de um dado titular do cartão durante os últimos N dias ($N = 30, 60, 90$, etc.) e pode calcular a quantidade mediana ou média gasta por dia, com despesas em um dia que excedem

as despesas médias e/ou medianas em um percentual maior que o selecionado sendo consideradas fraudulentas; (5) uma classe de comerciantes pode ser designada, por exemplo, qualquer compra em uma joalheria é considerada fraudulenta; (6) comerciantes em particular podem ser designados, por exemplo, qualquer transação com um identificador do comerciante correspondente a um comerciante selecionado é considerada fraudulenta; (7) produtos ou serviços em particular podem ser designados, por exemplo, qualquer transação que inclui dados de nível três com uma SKU que corresponde a um produto e/ou serviço é considerada fraudulenta; (8) regiões geográficas podem ser designadas, por exemplo, qualquer transação com dados de nível três indicando que a loja de vendas fica localizada em uma dada região (estado, país, continente, etc.) é considerada fraudulenta.

O titular do cartão pode inserir dados em qualquer dos campos correspondentes às regras de fraude que ele deseja que sejam aplicadas no cartão (operação 1406). Por exemplo, para estabelecer que uma despesa que excede \$ 5.000 deve ser considerada fraudulenta o titular do cartão pode inserir "5.000" em um campo rotulado "despesa máxima admissível (em dólares)". Finalmente, da forma mostrada na operação 1408, o sistema do software da Figura 7 associa as regras selecionadas com o número do cartão inserido durante a operação 1400.

Da forma também mencionada em relação à Figura 13, um titular do cartão pode selecionar um esquema pelo qual um PIN associado com seu cartão é modificado. Da forma descrita

em relação às Figuras 13 e 14, o titular do cartão pode começar a seleção do esquema de modificação do PIN se conectando à página da Internet (operação 1500). Desse modo, o sistema do software da Figura 7 identifica o usuário em particular da página da Internet como correspondente a um número do cartão em particular.

Da forma discutida em relação às Figuras 13 e 14, depois da conexão, o usuário seleciona uma opção para permitir modificação automática do PIN associado com seu cartão.

10 Posteriormente, a página da Internet responde apresentando ao titular do cartão vários esquemas de modificação que podem ser aplicados ao cartão (operação 1502). Por exemplo, da forma mostrada na caixa 1504, a página da Internet pode apresentar ao titular do cartão um conjunto de campos que

15 permite a inserção de dados para a designação de: (1) uma quantidade selecionada pela qual incrementar o PIN por uma unidade de tempo selecionada, por exemplo, incrementar o PIN em uma quantidade de 5 a cada semana; (2) uma quantidade selecionada pela qual decrementar o PIN por uma unidade selecionada de tempo, por exemplo, decrementar o PIN em uma

20 quantidade de 5 a cada semana; (3) um conjunto selecionado de PINs, cada um dos quais fica ativo por um período de tempo selecionado, por exemplo, um conjunto selecionado de 5 PINs, com o primeiro PIN do conjunto ficando ativo por uma

25 semana, o segundo PIN do conjunto ficando ativo pela próxima semana, e assim por diante; (4) a opção de realizar uma operação de rotacionar à direita em um PIN em cada unidade de tempo, por exemplo, depois de uma semana o PIN 4305 se

transforma em 5430, depois da próxima semana ele se transforma em 0543, e assim por diante; (5) a opção de realizar uma operação de rotacionar à esquerda em um PIN a cada unidade de tempo, por exemplo, depois de uma semana o PIN 4305
5 se transforma em 3054, depois da próxima semana, ele se transforma em 0543, e assim por diante; (6) uma seleção de um período de tempo para o qual um PIN fica ativo, depois da expiração de um tempo como este, um novo PIN é aleatoriamente selecionado, por exemplo, selecionar aleatoriamente um
10 novo PIN a cada semana (o titular do cartão pode conectar-se na página da Internet para descobrir o novo PIN, ou pode ligar para um número de telefone e descobrir o novo número PIN por meio de reconhecimento interativo de voz, e/ou ter o PIN enviado a ele por correio eletrônico, por exemplo); (7) uma
15 quantidade selecionada pela qual o PIN é multiplicado com a passagem de um período de tempo selecionado, por exemplo, multiplicar o PIN por 2 a cada dia; (8) uma quantidade selecionada pela qual o PIN é dividido com a passagem de um período de tempo selecionado, por exemplo, dividir o PIN por 2
20 a cada dia; e/ou (9) selecionar uma parte estática de um PIN que deve ser anexado ou incluído no início de uma parte dinâmica de um PIN que muda de acordo com algum algoritmo, incluindo os supramencionados algoritmos, por exemplo, uma parte estática, 12345, na qual uma parte dinâmica, 99, é a-
25 nexada, produzindo um PIN de 1234599, que pode mudar para ser 12345100, se a parte dinâmica for selecionada para ser alterada pelo incremento em um. Onde uma operação matemática for realizada sobre um PIN, por exemplo, multiplicando o PIN

por uma quantidade selecionada, N, entende-se que a quantidade resultante pode ser truncada ou, de outra forma, ser operada para chegar em inúmeros números apropriados de dígitos. Entretanto, deve-se perceber que, de acordo com algumas
5 modalidades, o PIN não é de um comprimento prescrito, mas, em vez disto, pode ser de qualquer comprimento em uma faixa pré-determinada, por exemplo, entre quatro e cinquenta e seis dígitos. Também, onde uma operação matemática for realizada sobre o PIN, por exemplo, dividindo o PIN por uma
10 quantidade selecionada, N, entende-se que a quantidade resultante pode ser arredondada para um número mais próximo ou, de outra forma, operada para chegar em uma quantidade de número inteiro.

O titular do cartão pode inserir dados em qualquer
15 um dos campos correspondentes ao esquema de modificação de PIN que ele deseja que seja aplicado no cartão (operação 1506). Por exemplo, estabelecer que o PIN associado com seu cartão deve ser incrementado em 5 a cada semana, o titular do cartão pode inserir "5" em um campo rotulado "quantidade
20 na qual incrementar PIN" e "semanalmente" em um campo rotulado "período no qual incrementar PIN". Finalmente, da forma mostrada na operação 1508, o sistema do software da Figura 7 associa as regras selecionadas com o número do cartão inserido durante a operação 1500.

25 De acordo com uma outra modalidade, o sistema de software da Figura 7 pode suportar a seleção de um PIN que é usado somente uma vez. Por exemplo, o titular do cartão pode selecionar um PIN que está sempre associado com seu número

do cartão (pelo uso de uma página da Internet provida pelo módulo de interface inicial 726, da forma supradescrita). Além do mais, o titular do cartão pode selecionar um PIN que pode ser usado mais de uma vez (novamente, pelo uso de uma

5 página da Internet provida pelo módulo de interface inicial 726, como descrito anteriormente). Quando, no contexto da execução de uma transação, o sistema do software da Figura 7 recebe um objeto de transporte encriptado, tal como um da Figura 6, o terceiro módulo de deciptação 712 pode, inicialmente,

10 almente, tentar sua deciptação usando o PIN "ordinário", como descrito em relação à Figura 7. Considerando que a deciptação falhou, o terceiro módulo de deciptação 712 tenta a deciptação com o PIN de "uma vez" associado com o número do cartão. Se obtiver sucesso, a transação é realizada da

15 forma supradescrita, e o PIN de uma vez é desabilitado para uso adicional. Um PIN de uma vez como este é usado para ajustes nos quais o titular do cartão é hesitante sobre prover seu PIN "ordinário" a um comerciante, tal como quando o titular do cartão pode estar usando uma página de comércio

20 eletrônico não familiar ou quando ele acredita que a inserção do seu PIN pode estar sob observação. Uma vez que o PIN somente pode ser usado uma vez, não importa se a inserção do PIN é observada ou capturada por uma página da Internet.

De acordo com uma outra modalidade da invenção, o

25 esquema de transação supramencionado pode ser utilizado para permitir retorno de produtos intercomerciante, como ilustrado em relação às Figuras 16A e 16B. Por exemplo, a Figura 16A representa um arranjo típico de compra eletrônica, por

meio do qual o titular do cartão 1600 encomenda um item de um comerciante eletrônico 1602. O titular do cartão 1600 recebe o item do comerciante eletrônico (operação 1601). Em resposta, o banco emitente do cartão 1604 encaminha o preço do item para o banco do comerciante eletrônico (operação 1603). Então, na expiração do período de tarifação, o titular do cartão 1600 paga uma soma monetária igual ao preço do item ao banco 1604 (operação 1605).

A Figura 16B apresenta um exemplo de um arranjo de retorno intermercado de produtos. Conforme o arranjo da Figura 16B, o titular do cartão 1600 retorna o item a um comerciante de tijolos e cimento 1606 (operação 1607). No momento do retorno, o titular do cartão 1600 apresenta seu recibo ao comerciante de tijolos e cimento 1606 que usa a informação para indicar à plataforma de transação que um retorno de bens em particular proveniente de um comerciante em particular por um titular do cartão em particular deve ser realizado na loja de vendas de tijolo e cimento 1606. Usando a supramencionada informação, a plataforma de transação acessa a base de dados de regras para determinar uma soma monetária a ser transferida do comerciante de tijolos e cimento até o comerciante eletrônico. Então, o servidor da plataforma de transação inicia uma transferência de fundos do banco do comerciante de tijolos e cimento para o banco do comerciante eletrônico igual à soma determinada (operação 1609). A soma baseada em regras supramencionada pode ser combinada antecipadamente pelos comerciantes individuais e pode ser em função do produto em particular a ser trocado ou

classe de produtos a ser trocada, e pode ser adicionalmente em função de dois comerciantes em particular envolvidos na troca intercomerciante.

Posteriormente, o comerciante eletrônico 1602 transfere uma soma monetária igual ao preço do item para o banco emissor do cartão 1604 (operação 1611), e o banco emissor do cartão 1604 credita a conta do titular do cartão com uma soma monetária igual ao preço do item (operação 1613). Assim, o titular do cartão 1600 pode conduzir uma compra em um comerciante (tal como um comerciante eletrônico 1602) e retornar o produto para um segundo comerciante (tal como comerciante de tijolos e cimento 1606). Este arranjo de retorno torna-se possível em virtude de uma combinação sobre a soma a ser transferida de um comerciante para um outro comerciante, no caso de uma troca de um produto em particular ou classe de produtos, estar armazenada em uma base de dados em comunicação com o servidor da plataforma de transação.

A Figura 17 representa um esquema de troca de fundos sem fio entre titulares do cartão. O esquema envolve um pequeno aplicativo que executa em um processador em um telefone celular. O pequeno aplicativo inclui um módulo de solicitação 1700 que pede para um titular do cartão inserir os seguintes dados: (1) a quantidade de dinheiro que ele deseja transferir para um outro titular do cartão; (2) o código PIN do titular do cartão; e (3) o número de telefone celular do receptor. Os dados supramencionados são aglomerados em um conjunto de dados e são encriptados pela unidade de encriptação 1702 que pode operar de acordo com os princípios su-

pradescritos. Então, o conjunto de dados encriptados é comunicado por meio da plataforma de transação conectada à Internet com SSL da Figura 7.

Na interface inicial, o número de telefone a partir do qual a transação originada é extraída e é usada para consultar uma base de dados 1704 que associou os números de telefone do titular do cartão com os códigos PIN. Portanto, o código PIN correspondente é retornado para o módulo 1706 e é provido para o módulo de deciptação 1708, que usa o código PIN como uma chave de deciptação.

Posteriormente, é verificada a disponibilidade de fundos na conta correspondente ao PIN. De acordo com uma modalidade, o PIN ou número de telefone pode ser usado para acessar uma base de dados 1710 que relaciona um número de identificação de cartão com um PIN ou módulo 1712, que determina se a conta correspondente ao PIN / número de telefone tem fundos suficientes para permitir a troca proposta. Se for o caso, a troca é realizada e uma SMS é transmitida pelo módulo 114 para o número de telefone do receptor, informando-o sobre a troca de fundos.

Uma troca de fundos pessoa-a-pessoa também pode ser conduzida on-line por meio de uma página da Internet apresentada a partir do módulo de interface inicial 726, no geral, prosseguindo como descrito em relação à Figura 17.

A Figura 18 representa uma modalidade exemplar de uma transação pessoa-a-pessoa, da forma supradescrita. Da forma mostrada na Figura 18, a plataforma de transação 1800 estende o acesso aos fundos monetários (linha de crédito,

conta de débito, conta de cheques, conta de poupança, valor armazenado e/ou conta pré-paga) por meio de cada um dos dois bancos 1802 e 1804. Em princípio, a plataforma 1800 pode entender acesso aos fundos por meio de qualquer número de bancos. A título de ilustração, uma transferência pessoa-a-pessoa de fundos é descrita em relação à transferência de um cartão de crédito. A transferência de fundos pode ser executada de qualquer tipo de conta para qualquer tipo de conta. Novamente, a título de ilustração somente, considera-se que a plataforma de transação trata oito partes, cada uma das quais possui um cartão de transação que funciona como um cartão de crédito. Quatro dos titulares do cartão acessam uma linha de crédito por meio do banco 1802, enquanto que os outros quatro acessam uma linha de crédito por meio do banco 1804. Assim, da forma mostrada na Figura 18, uma conta é mantida para cada titular do cartão por cada banco emissor do cartão 1802 e 1804. Uma tal conta é identificada pelo número de referência 1806 e uma outra tal conta é identificada pelo número de referência 1808.

Considerando que o titular do cartão associado com a conta de crédito 1806 deseja transferir fundos para a parte associada com a conta 1808, tais fundos podem se tornar disponíveis de forma instantânea à parte associada com a conta 1808. A plataforma de transação mantém uma conta 1810 e 1812 em cada banco 1802 e 1804. Todos os titulares do cartão com contas no banco 1802 têm os fundos de suas contas pré-pagas armazenadas na conta 1810, enquanto que todos os titulares do cartão com contas no banco 1804 têm os fundos

de suas contas pré-pagas armazenados na conta 1812. A plataforma mantém uma base de dados 706 que mantém vestígio da quota de cada titular do cartão dos fundos mantidos nas contas pré-pagas 1810 e 1812. Uma transferência de uma conta de crédito 1806 para o titular do cartão associado com a conta de crédito 1808 é feita da conta de crédito 1806 para a conta pré-paga 1812, e a base de dados 706 é imediatamente atualizada para: (1) refletir que a conta 1812 é incrementada pela soma monetária que está sendo transferida; e (2) refletir que o titular do cartão associado com a conta de crédito 1808 tem uma quota da conta pré-paga que é incrementada pela soma monetária que está sendo transferida. Assim, o titular do cartão associado com a conta monetária 1808 pode sacar imediatamente sua parte da conta pré-paga 1812, por exemplo, pode conduzir uma compra de um produto ou serviço realizando tal compra com uma transação pré-paga, significando que os fundos foram sacados daquela conta pré-paga 1812, e a base de dados 706 é imediatamente atualizada para refletir tal transação. Alternativamente, o titular do cartão associado com a conta de crédito 1808 pode especificar que os fundos recebidos sejam transferidos para sua conta de crédito 1808 ou qualquer outra conta. Então, tal transferência é completada, por exemplo, no fim do dia quando a base de dados 706 e o sistema computacional do banco 1804 estiverem sincronizados, a fim de refletir que a soma monetária deve ser sacada da conta pré-paga 1812 e depositada na conta de crédito 1808.

As várias modalidades supradescritas são providas

a título de ilustração somente e não devem ser interpretadas limitando a invenção. Versados na técnica reconhecerão prontamente várias modificações e mudanças que podem ser feitas na presente invenção sem seguir as modalidades e aplicações de exemplo aqui ilustradas e descritas e sem fugir do verdadeiro espírito e escopo da presente invenção, que é apresentada nas seguintes reivindicações.

REIVINDICAÇÕES

1. Método computadorizado, **CARACTERIZADO** pelo fato de que compreende:

associar, na dita base de dados, um cartão de transação com uma ou mais regras de detecção de fraude governando acesso a fundos monetários pelo dito cartão de transação; e

permitir que um indivíduo proprietário do dito cartão de transação especifique as ditas regras de detecção de fraude governando acesso aos ditos fundos monetários pelo dito cartão de transação.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que ao dito indivíduo é permitido especificar uma regra de detecção de fraude na qual um gasto de mais de um número especificado de dólares por período especificado de tempo dos ditos fundos monetários pelo dito cartão de transação é identificado como potencialmente fraudulento.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que ao dito indivíduo é permitido especificar uma regra de detecção de fraude na qual um gasto de mais de um número especificado de dólares em um único produto ou serviço dos ditos fundos monetários pelo dito cartão de transação é identificado como potencialmente fraudulento.

4. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que ao dito indivíduo é permitido especificar uma regra de detecção de fraude na qual uma a-

quisição de uma classe especificada de produtos dos ditos fundos monetários com o dito cartão de transação é identificada como potencialmente fraudulenta.

5 5. Método, de acordo com a reivindicação 1,
5 **CARACTERIZADO** pelo fato de que ao dito indivíduo é permitido especificar uma regra de detecção de fraude na qual um gasto causando uma conferência em execução de número de dólares gastos dos ditos fundos monetários pelo dito cartão de transação por um período de tempo especificado para exceder um
10 número médio ou mediano de dólares gastos dos ditos fundos monetários pelo dito cartão de transação pelo dito período de tempo por mais que uma quantidade especificada é identificado como sendo potencialmente fraudulento.

15 6. Método, de acordo com a reivindicação 1,
15 **CARACTERIZADO** pelo fato de que ao dito indivíduo é permitido especificar uma regra de detecção de fraude na qual um gasto a partir dos ditos fundos monetários pelo dito cartão de transação em uma classe, um tipo ou uma categoria especificados de comerciantes é identificado como sendo potencial-
20 mente fraudulento.

7. Método, de acordo com a reivindicação 1,
CARACTERIZADO pelo fato de que ao dito indivíduo é permitido especificar uma regra de detecção de fraude na qual um gasto a partir dos ditos fundos monetários pelo dito cartão de
25 transação para um produto ou serviço especificado é identificado como sendo potencialmente fraudulento.

8. Método, de acordo com a reivindicação 1,
CARACTERIZADO pelo fato de que ao dito indivíduo é permitido

especificar uma regra de detecção de fraude na qual um gasto a partir dos ditos fundos monetários pelo dito cartão de transação dentro de uma região geográfica especificada é identificado como sendo potencialmente fraudulento.

5 9. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dito cartão de transação compreende um cartão de crédito.

 10. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dito cartão de transação
10 compreende um cartão de débito.

 11. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dito cartão de transação compreende um cartão de valor armazenado.

 12. Método, de acordo com a reivindicação 1,
15 **CARACTERIZADO** pelo fato de que o acesso aos ditos fundos monetários é governado pelas ditas regras de detecção de fraude substancialmente imediatamente quando da especificação das ditas regras de detecção de fraude pelo dito indivíduo.

 13. Método, de acordo com a reivindicação 1,
20 **CARACTERIZADO** pelo fato de que compreende adicionalmente:

 receber uma solicitação para acessar os ditos fundos monetários via o dito cartão de transação;

 testar a dita solicitação contra as ditas regras de detecção de fraude;

25 determinar que a dita solicitação é potencialmente fraudulenta, com base no dito teste contra as ditas regras de detecção de fraude;

contatar o dito indivíduo para confirmar a dita solicitação, antes de autorizar a dita solicitação para acessar os ditos fundos monetários.

14. Método, de acordo com a reivindicação 13,
5 **CARACTERIZADO** pelo fato de que o dito ato de contatar o dito indivíduo é conduzido via um serviço de mensagem curta (SMS).

15. Método, de acordo com a reivindicação 13,
CARACTERIZADO pelo fato de que o dito ato de contatar o dito
10 indivíduo é conduzido via uma mensagem de Internet.

16. Método, de acordo com a reivindicação 13,
CARACTERIZADO pelo fato de que o dito ato de contatar o dito indivíduo é conduzido via uma chamada de telefone.

17. Sistema, **CARACTERIZADO** pelo fato de que com-
15 preende:

um primeiro cartão de transação através do qual acesso a fundos monetários é estendido;

uma base de dados associando o dito cartão de transação a uma ou mais regras de detecção de fraude gover-
20 nando acesso aos ditos fundos monetários pelo dito cartão de transação; e

um sistema de computação programado para permitir que um indivíduo proprietário do dito cartão de transação especifique as ditas regras de detecção de fraude governando
25 acesso aos ditos fundos monetários pelo dito cartão de transação.

18. Sistema, de acordo com a reivindicação 17,
CARACTERIZADO pelo fato de que o dito sistema de computação

é programado para permitir que o dito indivíduo especifique uma regra de detecção de fraude na qual um gasto de mais de um número especificado de dólares por período especificado de tempo dos ditos fundos monetários pelo dito cartão de transação é identificado como potencialmente fraudulento.

19. Sistema, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o dito sistema de computação é programado para permitir que o dito indivíduo especifique uma regra de detecção de fraude na qual um gasto de mais de um número especificado de dólares em um único produto ou serviço dos ditos fundos monetários pelo dito cartão de transação é identificado como potencialmente fraudulento.

20. Sistema, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o dito sistema de computação é programado para permitir que o dito indivíduo especifique uma regra de detecção de fraude na qual uma aquisição de uma classe especificada de produtos dos ditos fundos monetários com o dito cartão de transação é identificada como potencialmente fraudulenta.

21. Sistema, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o dito sistema de computação é programado para permitir que o dito indivíduo especifique uma regra de detecção de fraude na qual um gasto causando uma conferência em execução de número de dólares gastos dos ditos fundos monetários pelo dito cartão de transação por um período de tempo especificado para exceder um número médio ou mediano de dólares gastos dos ditos fundos monetários pelo dito cartão de transação pelo dito período de tempo por

mais que uma quantidade especificada é identificado como sendo potencialmente fraudulento.

22. Sistema, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o dito sistema de computação é programado para permitir que o dito indivíduo especifique uma regra de detecção de fraude na qual um gasto a partir dos ditos fundos monetários pelo dito cartão de transação em uma classe especificada de comerciantes é identificado como sendo potencialmente fraudulento.

10 23. Sistema, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o dito sistema de computação é programado para permitir que o dito indivíduo especifique uma regra de detecção de fraude na qual um gasto a partir dos ditos fundos monetários pelo dito cartão de transação para um produto ou serviço especificado é identificado como sendo potencialmente fraudulento.

24. Sistema, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o dito sistema de computação é programado para permitir que o dito indivíduo especifique uma regra de detecção de fraude na qual um gasto a partir dos ditos fundos monetários pelo dito cartão de transação dentro de uma região geográfica especificada é identificado como potencialmente fraudulento.

25. Sistema, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o dito cartão de transação compreende um cartão de crédito.

26. Sistema, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o dito cartão de transação compreende um cartão de débito.

27. Sistema, de acordo com a reivindicação 17,
5 **CARACTERIZADO** pelo fato de que o dito cartão de transação compreende um cartão de valor armazenado.

RESUMO

"SISTEMA E MÉTODO PARA SELEÇÃO POR USUÁRIO DE REGRAS DE DETECÇÃO DE FRAUDE"

Sistema e método para estabelecer sistema de regras de detecção de fraude inclui um primeiro cartão de transação através do qual acesso a fundos monetários é estendido e uma base de dados associando o dito cartão de transação a uma ou mais regras de detecção de fraude que regem governando acesso aos ditos fundos monetários pelo dito cartão de transação. O sistema também inclui um sistema de computação programado para permitir que um indivíduo proprietário do dito cartão de transação especifique as ditas regras de detecção de fraude governando acesso aos ditos fundos monetários pelo dito cartão de transação.