(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: SECURE PAYMENT PROCESS FOR ON-LINE TRANSACTIONS
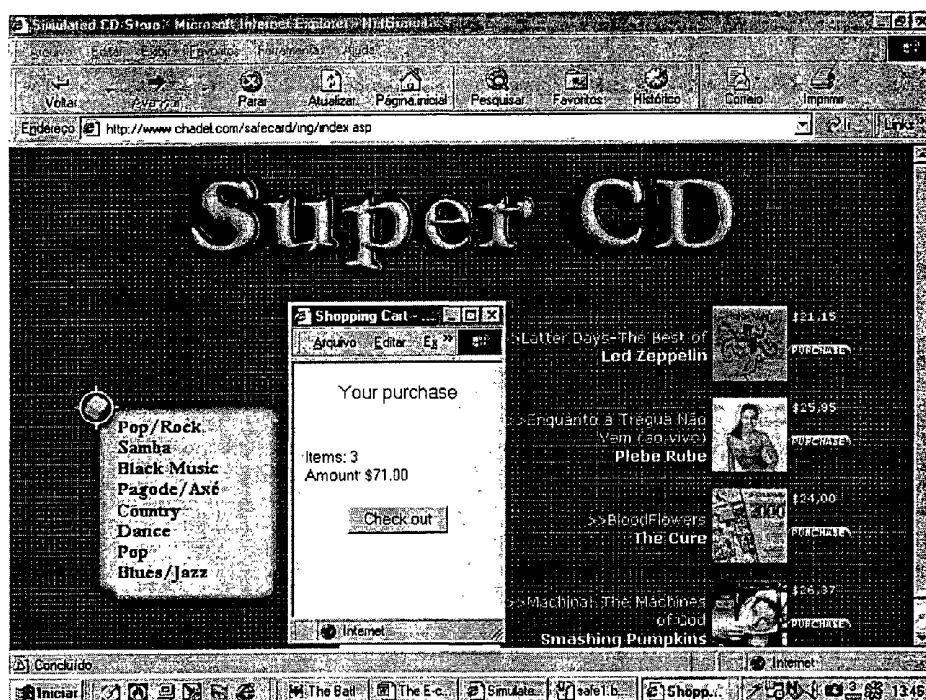
(57) Abstract: There is disclosed a linking process to provide a customer of goods or services on-line a secure payment process without relying upon the security of payment information residing at the retailer. Specifically, there is disclosed an on-line transaction wherein a customer purchases goods from an on-line retailer without providing credit card information to the retailer.

SECURE PAYMENT PROCESS FOR ON-LINE TRANSACTIONS

Technical Field of the Invention

5   The present invention provides a linking process to provide a customer of goods or services on-line a secure payment process without relying upon the security of payment information residing at the retailer. Specifically, the present invention provides an on-line transaction wherein a customer purchases goods from an on-line retailer without providing credit card information to the retailer.

10

Background of the Invention

        The world of e-commerce and on-line transactions are evolving rapidly. Simultaneously, the world of security of financial information is becoming more important as an issue. Internet users often desire to make purchases from merchants by

15   means of an on-line transaction. The most commonly available form of an on-line transaction involving payment or finances is a credit card transaction. This involves the customer supplying to the merchant a valid credit card number, the type of credit card used, the name on the credit card and the expiry date on the credit card. Often a billing address for the credit card is also requested for additional verification. Many Internet

20   users (potential customers) refuse to transmit their credit card information over the Internet due to fears of untrustworthy merchants or of third parties intercepting the information and using it for unapproved purposes.

        Moreover, other Internet users do not want to supply some merchants with their names and other information identifying themselves with either spending habits or other

25   purchases for fear that this information will be used for unsolicited marketing purposes. A credit card facilitates making purchases via telephone or over a network (*i.e.*, the Internet). However, potential customers are justifiably concerned about placing orders for merchandise on networks such as the Internet, for example via E-mail, because of the lack of secure communications. Confidential data (*i.e.*, credit card numbers and

30   associated information) are shared among three entities, the customer, on-line retailer and the credit card company. Several on-line retailers have even been "hacked" and had database files containing customer information, including credit card numbers, accessed by hackers. Security on public networks at the present time is virtually non-existent, making it relatively easy for an unauthorized third party to gain access to credit card data

35   transmitted over the network. Once a dishonest person has the credit card number, thousands of dollars can be improperly charged to the customer's credit card account.

        One solution to this problem is for the customer to enter, for delivery over the network, an order that does not include the customer's credit card number. To complete the order, the customer must then call the merchant (such as on a "toll-free" telephone

number, for example) to provide the credit card number. However, this method does not enable the credit card data to be readily associated with and entered into the order previously placed by the customer. Errors in the order can easily arise. For example, the customer's credit card number can be assigned to the wrong order. In addition, there is

5   usually a considerable delay to further inconvenience the customer while a clerk asks the customer other questions that will help to ensure the correct match between an order that was previously transmitted and the customer's credit card number given over the phone.

A similar approach for placing an order in current use is initiated when a customer sends an order, without credit card information, to a merchant over a non-

10   secure network. After receiving the order, the merchant's clerk or an automated system sends an E-mail message to the customer containing an order number that uniquely identifies the order. Upon receiving the E-mail message, the customer dials a telephone number that connects to the merchant's facilities. In response to prompting from an automated attendant, the customer enters the unique order number and correct credit card

15   number for billing the order on a touch-tone telephone (assuming that the customer has placed the call on this type of phone). The order number is used to match the correct order with the customer's credit card number. However, this method requires that the customer retain the unique order number assigned by the merchant for entry during the subsequent phone call.

20   Another approach to solving this problem is to encrypt the credit card information included in an order placed on a public network. Using the encrypted credit card data, an order can be completed in a single transaction. However, virtually all of the encryption schemes thus far developed for protecting such sensitive data have drawbacks. For example, most encryption schemes require the use of an encryption key

25   that is known only to the party encrypting information and to the intended recipient of the information who will decrypt it. The secure distribution and safeguard of such encryption keys adds too much complexity to network shopping transactions and will likely not be readily accepted by customers. While it is possible to embed an encryption key in an application designed to take an order and transmit it over the network, the

30   embedded encryption key can be discovered by others who may then misuse it. Even public key encryption systems require use of a "private" key that should not be disclosed to others. In addition, and perhaps more importantly, the software required for any encryption system must be distributed to prospective customers before the system can be used to transfer credit card data when a customer places an order. The widespread

35   dissemination of such software will likely not occur for some time.

A new method for ordering goods over a network is needed that enables a customer to place an order without concern that others may illicitly gain access to the customer's credit card information. The order entry should be automated for optimum efficiency and to minimize the time required for the customer to complete an order. The

present invention represents a workable solution to this problem that is relatively efficient and foolproof.

Summary of the Invention

5   The present invention provides a process for completing an on-line transaction wherein a customer purchases goods from an on-line retailer, comprising:

(a)   determining the goods to be purchased and the total cost of the goods in an on-line connection between a customer and an on-line retailer;

(b)   linking the customer to a credit card company chosen by the customer,
10   wherein the retailer provides only the amount of the purchase to be authorized by the credit card company;

(c)   identifying the customer to the credit card company by providing credit card information and answers to questions within a designated time frame that only the customer can answer;

15   (d)   providing the customer an authorization code from the credit card company for the purchase of the goods only from the retailer, wherein the authorization code has a limited duration; and

(e)   providing the authorization code to the retailer to complete the sale of the goods.

20   Preferably, the link to the credit card company with the customer is over a secure socket or an encrypted communication. Preferably, in step (a) the identity of the customer or other customer data is not provided to the retailer. Preferably, the customer chooses a link to the credit card company wherein the customer owns an account and identified the credit card account only to the credit card company. Preferably, the
25   process further comprises (f) having the retailer provide the authorization code and a retailer code to the credit card company; and (g) having the credit card company authorize the purchase and bill the customer. If the customer does not identify himself or herself in step (c), then the credit card company cancels the credit card provided.

30   **Brief Description of the Drawings**

Figure 1 is a screen-print from a hypothetical on-line retailer (Super CD) showing a purchase of three items for a total of US$71.00.

Figure 2 shows a screen-print of a form for obtaining customer information to be directed to a credit card company, wherein there are credit card logos for linking
35   available at the bottom of the page.

Figure 3 is a hypothetical first page of a screen showing the first step for an authorization procedure with a customer giving credit card information only to a credit card company (American Express in the Figure).

Figures 4 and 5 show hypothetical screen-prints of an authorization process

3

wherein the customer is given a period of time (30 seconds) to answer a question that the customer should know and provide a password.

Figure 6 shows a screen print of a completed authorization with a credit card company and providing an authorization code "26077" to the customer by the credit card company (American Express).

Figure 7 shows a screen-print of the customer being directed back to the retailer site to enter the authorization code (26077) supplied by the credit card company. It should be noted that the retailer does not have the credit card number of the customer.

Figure 8 shows a hypothetical screen-print of a completed transaction wherein the customer is supplied with an order number (81404) by the retailer.

Figure 9 shows a screen print of a hypothetical situation when a customer does not properly answer questions from the credit card company and the credit card is temporarily canceled.

Detailed Description of the Invention

The present invention addresses the need for greater credit card security so as to allow on-line retailers and on-line customers to more freely conduct business on the Internet without fear or with reduced fear that credit card information will fall into the wrong hands. The present inventive process takes the position that the on-line retailed does not need to know a customer's credit card information in order to conduct (business-to-consumer) business on-line.

Definitions

"**Credit card**" is intended to encompass debit cards and any other form of credit or debit used to make a purchase by providing a reference number that uniquely identifies a purchaser's account from which funds used to pay a seller for goods or services will be transferred.

"**Credit card transactions**" encompass credit cards, debit cards, purchase cards, store cards or any card issued by an "issuing agent."

A "**credit card company**" is a business that provides credit cards, such as VISA or a bank.

A "**customer**" is an individual or business that purchases goods or services.

"**Goods**" include items than can be purchased (*e.g.*, a computer, automobile, or bicycle) or services (*e.g.*, writing a patent application).

"**Issuing Agent**" is a business that issues credit cards. The most common issuing agents are VISA, Mastercard, American Express and Discover.

"**On-line retailer**" or "**retailer**" is a business that offers for sale goods or services on an Internet Web site.

"**On-line transaction**" or "**transaction**" refers to any exchange of goods or services in the normal course of commerce wherein the primary means of

4

communication between a customer and a retailer is via the Internet.

Process

The present invention provides a process for completing an on-line transaction wherein a customer purchases goods from an on-line retailer, comprising:

5 (a) determining the goods to be purchased and the total cost of the goods in an on-line connection between a customer and an on-line retailer;

  (b) linking the customer to a credit card company chosen by the customer, wherein the retailer provides only the amount of the purchase to be authorized by the credit card company;

10 (c) identifying the customer to the credit card company by providing answers to questions within a designated time frame that only the customer can answer;

  (d) providing the customer an authorization code from the credit card company for the purchase of the goods only from the retailer, wherein the authorization code has a limited duration; and

15 (e) providing the authorization code to the retailer to complete the sale of the goods.

A hypothetical transaction is provided in Figures 1-8. In this hypothetical transaction, the customer, Raul Lessa, of São Paulo (Figure 2) desires to purchase three items for a total purchase price of US$71.00 (Figure 1). The hypothetical retailer "Super

20 CD" directs the customer to a credit card company with a choice of credit card companies identified by their logos (Figure 2). This procedure further provides a reduction of risk of fraud to the credit card company, who has the ability to avoid fraud by canceling any credit card that may have been stolen. Selection of a credit card company will automatically link the customer to the secure site of the credit card

25 company without having the retailer have any access to the information. In addition, the link will send the "store code" of the retailer to the credit card company, along with transaction information including the order number and the purchase price amount.

The customer will provide his or her credit card number only to the credit card company (not to the retailer) and there will be no need to include additional information,

30 such as expiration date or the card holder's name (Figure 3). The credit card company will then begin a verification process to identify the credit card holder and not necessarily the person holding the credit card (in case it was physically stolen). The credit card company provides a series of questions that the credit card company knows the credit card holder can answer (Figures 4 and 5). If the credit card company receives

35 the correct answers (within a preset time period), the credit card company provides to the customer an authorization code (Figure 6). Preferably, this code is valid for a period of time and only for the retailer identified to the credit card company. In Figure 6, the authorization code provided by the credit card company (American Express) is 26077. The credit card company links the customer back to the retailer and the customer needed

to have copied down the authorization code. The retailer asks for the authorization code and this code is typed in by the customer (Figure 7).

This completes the on-line transaction with the order number being provided to the customer. Meanwhile the retailer has only the order number and order specifics,

5   along with customer address (for shipping) and email contact. However, the retailer does not have customer credit card information in case any retailed databases are compromised (Figure 8). The credit card company has authorized the transaction, the retailer gets paid and the credit card account is charged the correct amount.

In case the customer does not answer the credit card company questions correctly

10   (Figure 9), the credit card company can cancel, temporarily or permanently, the credit card whose number was provided. The credit card company also provides to the customer (assuming the customer was the valid card holder) a means for reinstating his or her credit card.

The inventive process provides a safe and secure means for facilitating on-line

15   transactions and does not let retailers have credit card information stored in vulnerable databases. There is security provided to the retailer to insure that valid credit hard holders are properly using credit cards to insure payment. There is security to the customer to avoid having his or her credit card numbers stored on a retailer database, having varying levels of security from hackers. Moreover, the foregoing process shifts

20   the verification burden from the retailer to the credit card company, with whom the contract with the customer exists. Therefore, no new infrastructure is needed to implement this process.

25

We claim:

1.   A process for completing an on-line transaction wherein a customer purchases goods from an on-line retailer, comprising:

(a)   determining the goods to be purchased and the total cost of the goods in an on-line connection between a customer and an on-line retailer;

(b)   linking the customer to a credit card company chosen by the customer, wherein the retailer provides only the amount of the purchase to be authorized by the credit card company;

(c)   identifying the customer to the credit card company by providing credit card information and answers to questions within a designated time frame that only the customer can answer;

(d)   providing the customer an authorization code from the credit card company for the purchase of the goods only from the retailer, wherein the authorization code has a limited duration; and

(e)   providing the authorization code to the retailer to complete the sale of the goods.

2.   The process for completing an on-line transaction of claim 1 wherein the link to the credit card company with the customer is over a secure socket or an encrypted communication.

3.   The process for completing an on-line transaction of claim 1 wherein in step (a) the identity of the customer or other customer data is not provided to the retailer.

4.   The process for completing an on-line transaction of claim 1 wherein the customer chooses a link to the credit card company wherein the customer owns an account and identified the credit card account only to the credit card company.

5.   The process for completing an on-line transaction of claim 1 wherein the process further comprises (f) having the retailer provide the authorization code and a retailer code to the credit card company; and (g) having the credit card company authorize the purchase and bill the customer.

6.   The process for completing an on-line transaction of claim 1 wherein if the customer does not identify himself or herself in step (c), then the credit card company cancels the credit card provided.
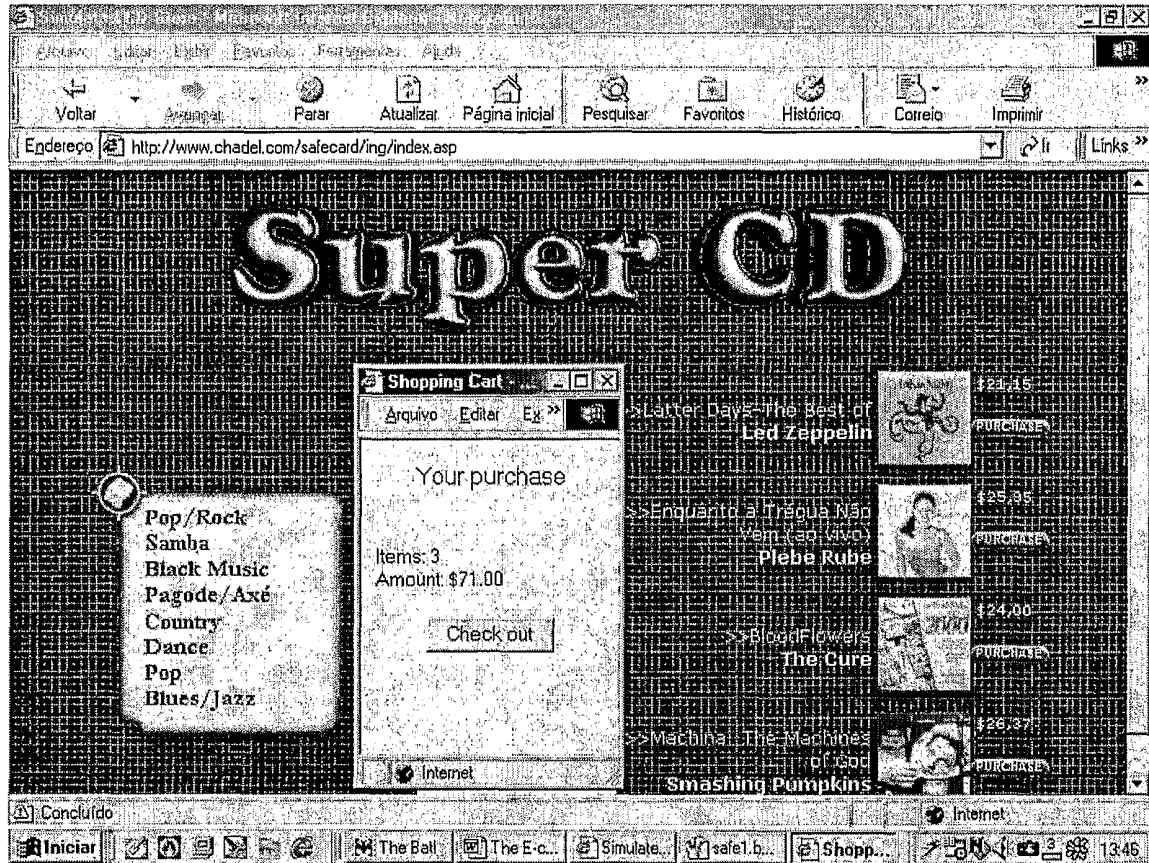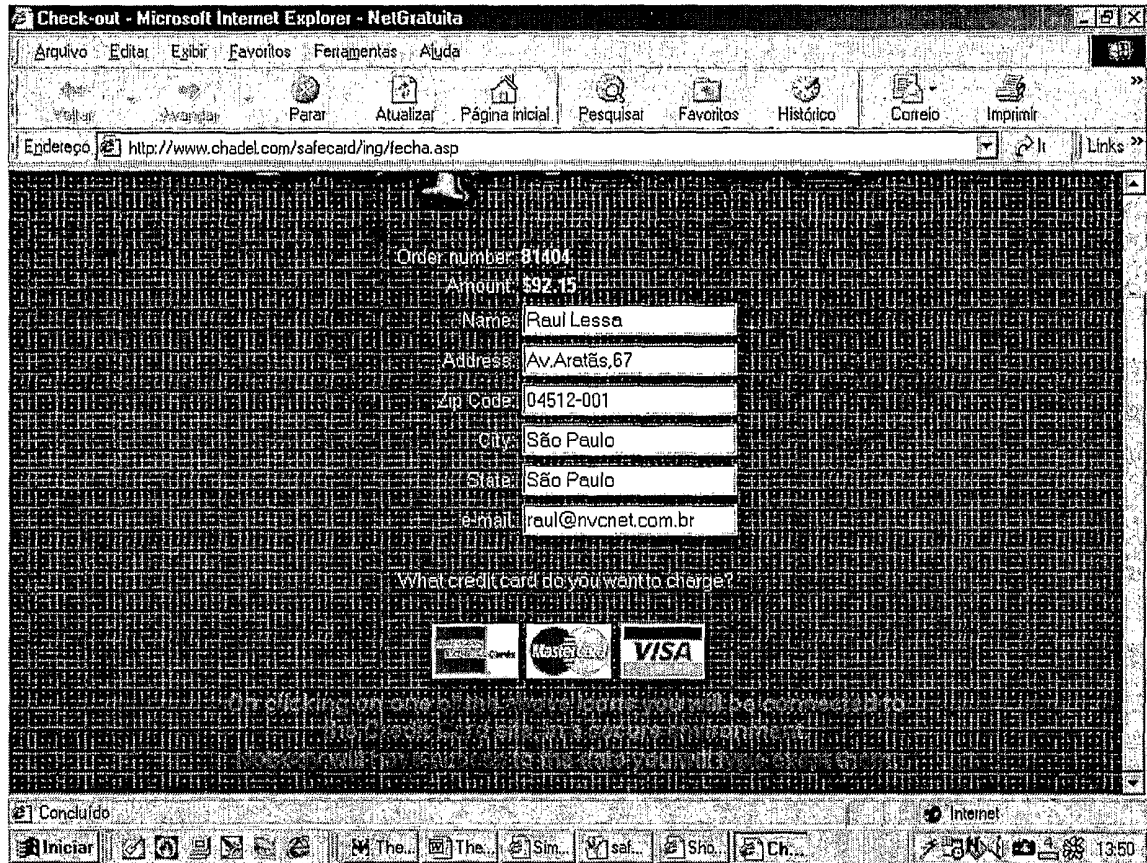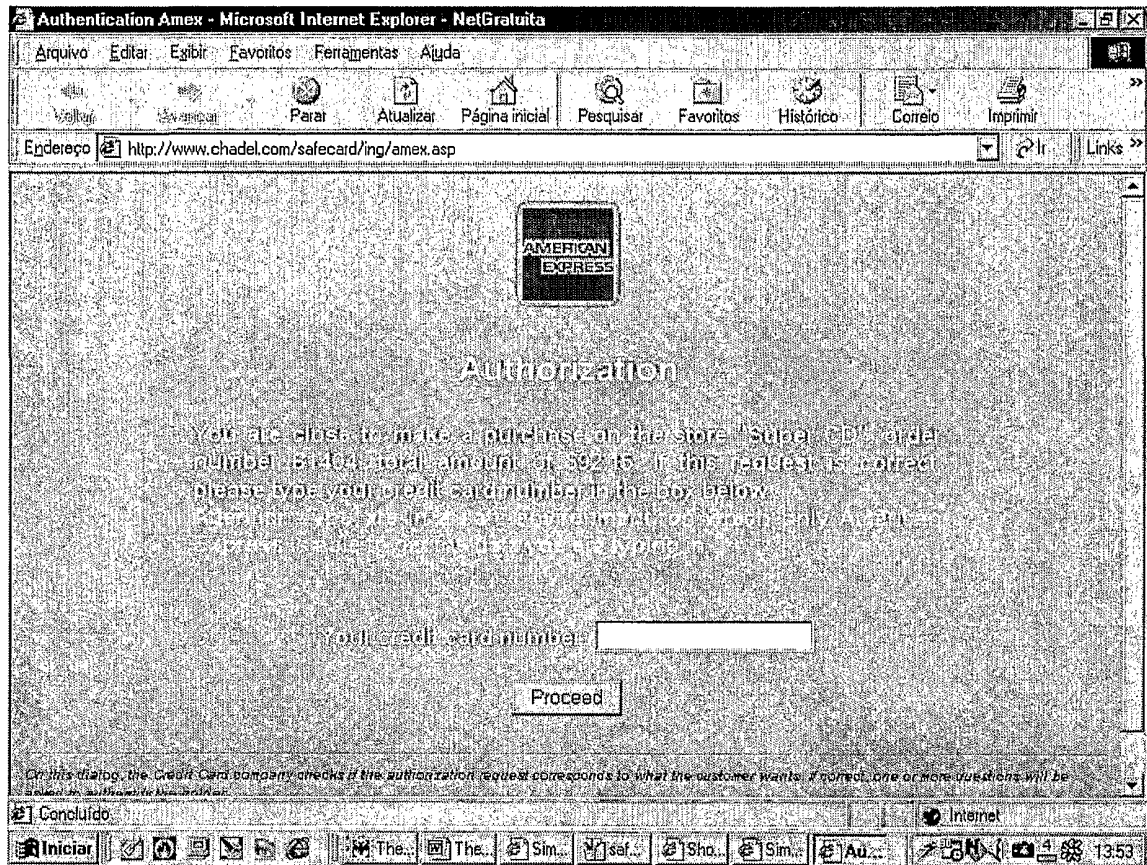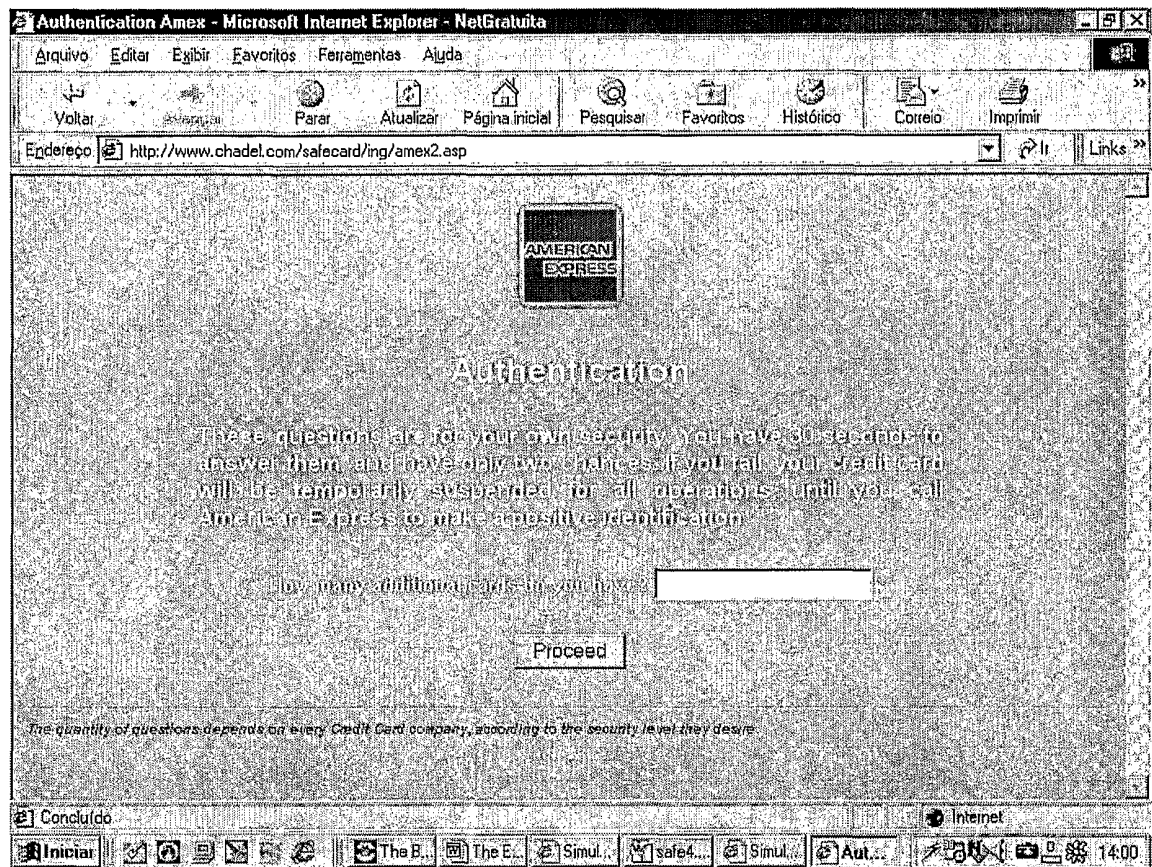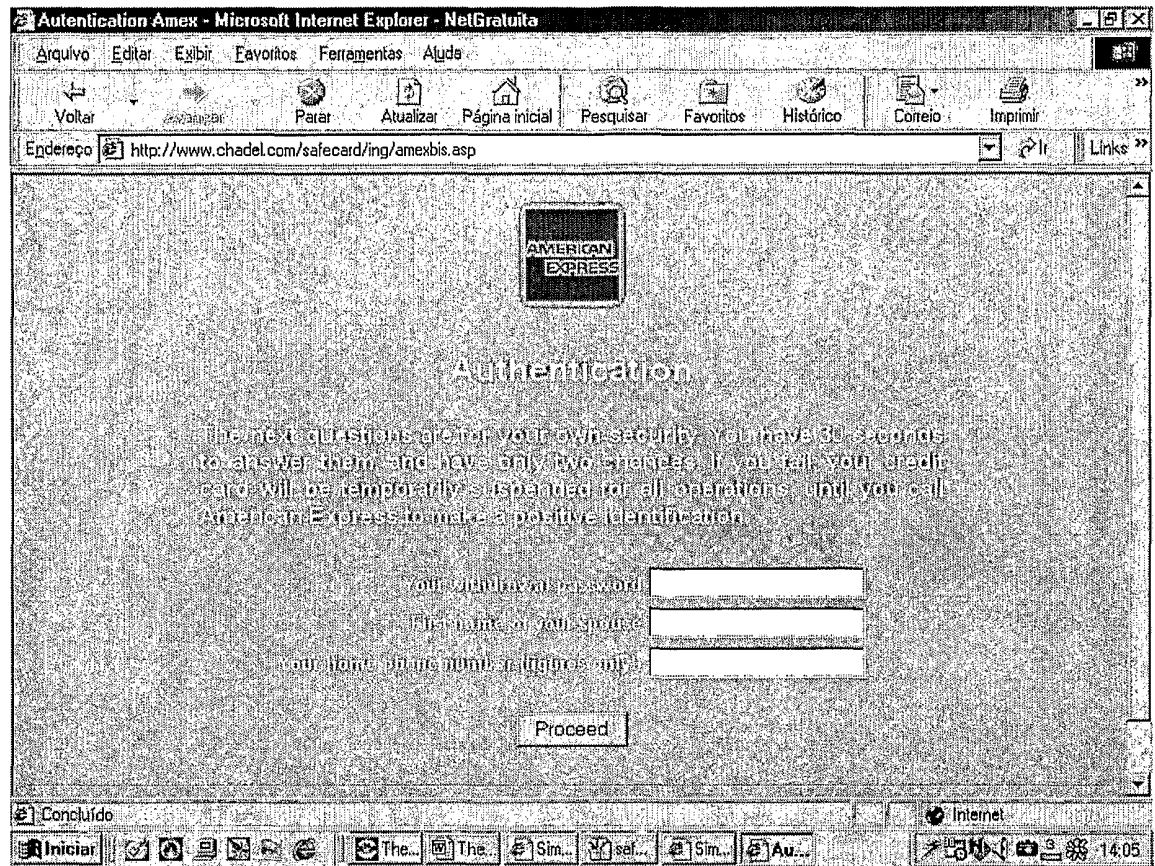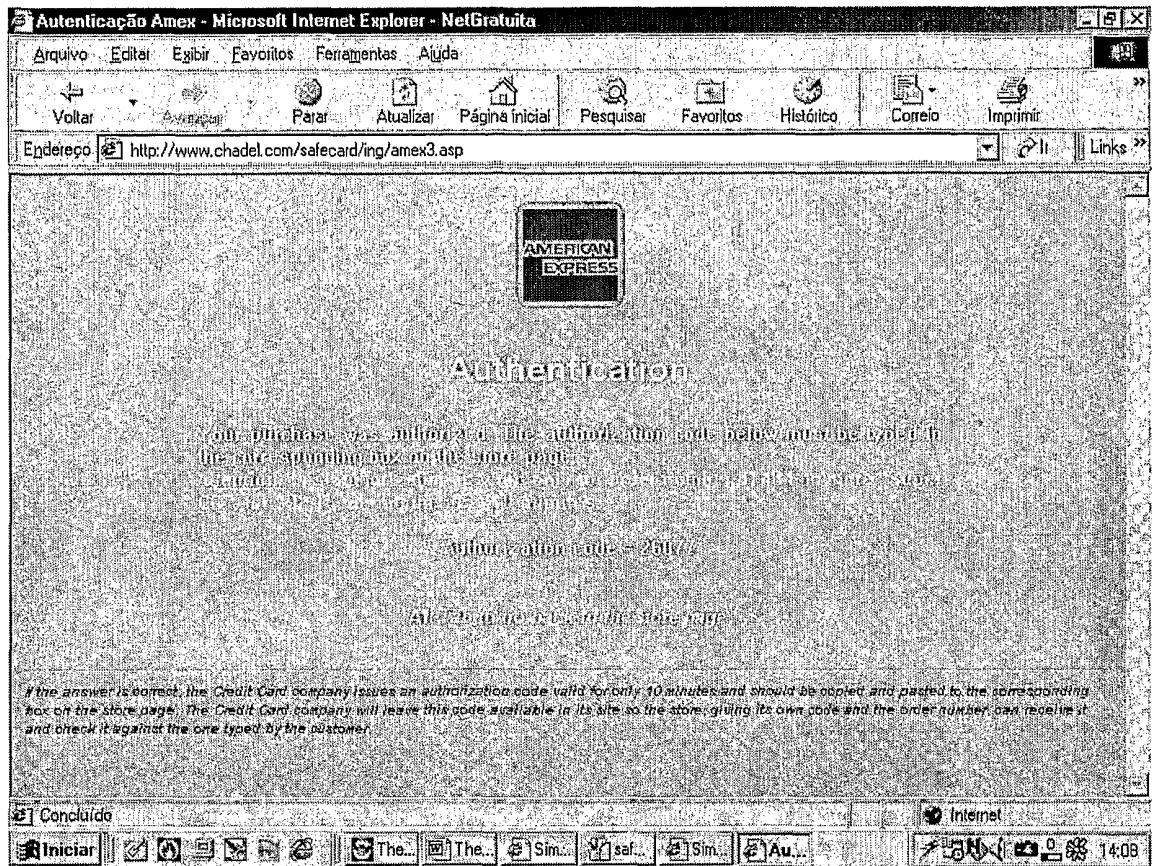
Fig. 1

Fig. 2

Fig. 3

Example of ONE question :

Fig. 4

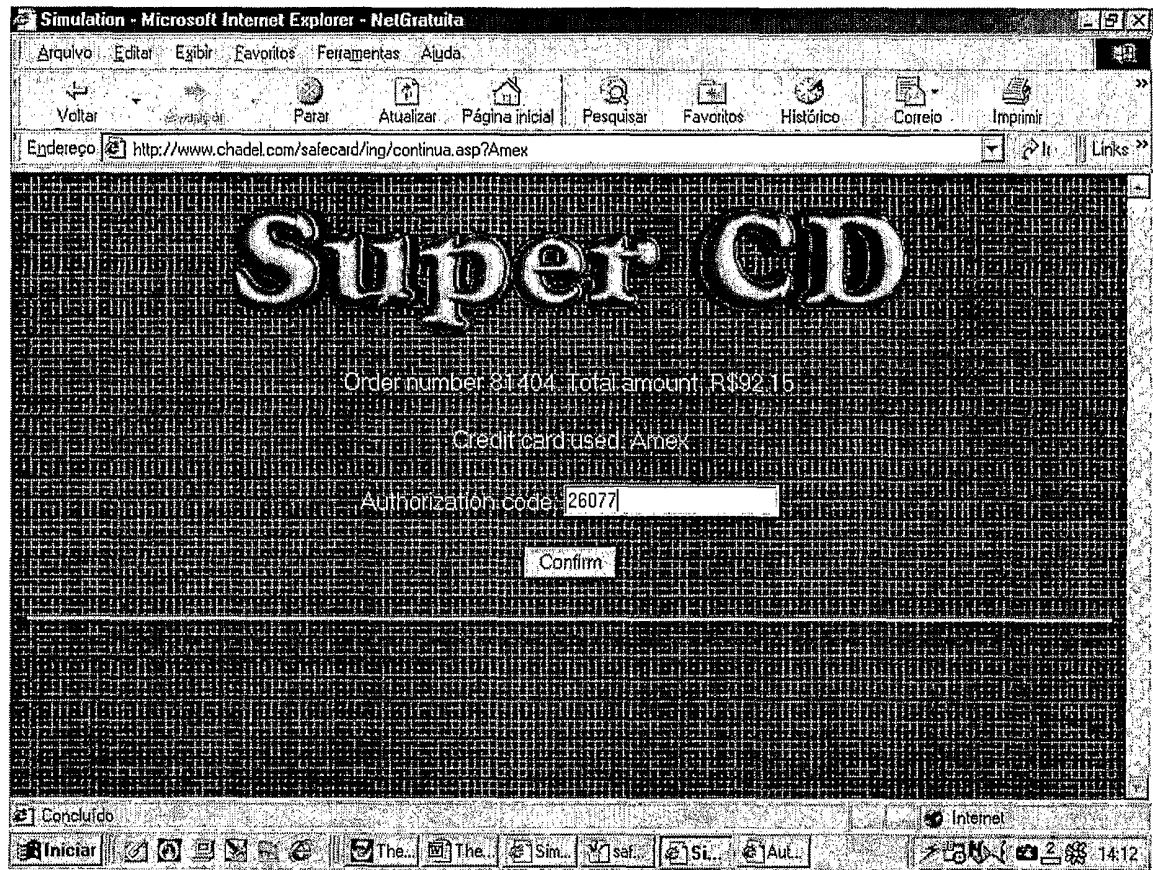5. Example of THREE random questions :

Fig. 5

6.

Fig. 6

7.

Fig. 7

Fig. 8

Fig. 9