

consumer of the purchase, nor does it add security or ease of use to transactions conducted verbally using a cell phone or land based telephone.

**[0009]** Visa's most recent security solution is called "Verified by Visa" and using Three Domain security (3D or 3D-Secure), which operates by the cardholder inputting a personal identification number (PIN) into the merchant's web site when requested. This solution does not work on telephone sales (as the PIN would have to be verbally given to the merchant's call center employee) and is cumbersome to operate on the Internet.

**[0010]** The Verified by Visa process works in the following steps in an Internet transaction:

**[0011]** 1. The cardholder enters payment details using the merchant's web page.

**[0012]** 2. The cardholder is automatically directed to the card issuer's server, who generates a pop-up screen on the consumer's computer.

**[0013]** 3. The issuer authenticates the cardholder via the cardholder inputting his/her PIN number or password.

**[0014]** 4. The issuer then transmits to the cardholder a digitally signed approval, which is then retransmitted to the merchant's server to begin the normal credit approval process.

**[0015]** 5. The normal credit approval process begins after the authentication process in order for the digital authorization from Visa to be included with the authorization request from the Merchant to Visa or, more likely, the authorization service for the card issuer.

**[0016]** Verified by Visa requires that the cardholder send the purchase authorization request from the consumer's computer to the merchant, who then send the request to Visa's server, who then sends the request to the issuer's server. The issuer's server prompts for the password from the consumer, who then inputs the password or PIN, sends it to the issuer's server who then sends it to their (the issuer's) authentication server. The issuer's server then sends the approval to the consumer's computer who then passes the approval to the merchant's server. Then the merchant processes the payment for approval in the normal approval process and includes the authentication data along with the approval request to the card issuer for credit approval. Verified by Visa is cumbersome and will not work on telephone orders, and offers little compensation to consumers while taking more time to complete the transaction. Verified by Visa does not add the functionality of auto-filling forms on the Internet Merchant (or other merchants') customer relationship management (CRM) systems, allow "one-click purchasing", ties up Visa, the merchant and the authorization entity's servers, increases communications between all of these servers, thus increasing the possibility of a communications error or drop, and still exposes the cardholder's data to theft.

**[0017]** Surrogate Card Numbers have been tried by American Express (Private Payments) and by MBNA (ShopSafe). The surrogate card number is basically a system where the consumer uses a software application to generate a one-use credit card number that has a short validity period (normally two months or less) and a fixed charge value. The surrogate card number is tied to the consumer's "real" card number.

This method is cumbersome (the consumer has to obtain the surrogate number and then keep track of it) and prevents the use of one click purchasing. Besides these issues, if surrogate numbers become widespread then, based on the current length of a credit card number (16 digits normally) there would soon be a shortage of numbers available. Of the 16 digits only 10 are available for actual account numbers as the other numbers designate the type of card, etc. With only ten digits available then there would be only ten billion possible card numbers—as there are over 700 million credit cards issued in the United States today that means that there would only be slightly more than 9 numbers available for each card—if just the numbers in the United States were used as a basis for the universe of total numbers. The Nilson Report, in its March, 2004 issue #807, listed total worldwide general purpose credit cards (excluding the store and gas named credit cards) totaled 1.96 billion. Using the worldwide number of bank credit and debit cards would thus leave only eight surrogate numbers per primary card.

**[0018]** None of the above existing methods are an elegant end solution that incorporates additional layers of security for both verbal and Internet transactions. Nor do any of the existing methods solve the combined problems of security, ease of use, and allow for one-click purchasing. Nor do any of the existing methods improve the accuracy and speed of the remote sales (MOTO) type transaction. Several of the above methods require additional hardware to implement and many increase the volume of communications (and thus the possibility for information theft and communications break down).

**[0019]** Currently in a normal MOTO or Internet transaction when there is a chargeback to the merchant the issuing bank and the consumer are fully repaid for the fraud loss. The merchant losses not only the amount of the chargeback, which he/she only received 97% to 98% of to start with (the merchant receives funds from the card issuer after deducting the card company's discount and fees) but also is charged in many instances a fee equal to \$10.00 or more per transaction or more along with any shipping and handling charges that the merchant paid third parties.

**[0020]** On attempt to deal with these issues is with "smart cards" (example U.S. Pat. No. 5,317,636 (Vizcaino) and will increase the security and usability of the smart card. The smart card detailed in this patent generates a "transaction sequence number" that must be verified as correct by the authorizing computer. In order to be verified the transaction sequence number from the smart card must match the number in memory on the authorizing computer. The Vizcaino invention also provides for encryption and decryption of the data stored on the smart card, but the decryption algorithm on the approval computer must match the algorithm on the smart chip. This patent requires a smart card reader, does not allow for the autopopulating of merchant's consumer relationship management system software of the consumer's data and is not readily adaptable to telephone orders.

#### SUMMARY OF THE INVENTION

**[0021]** The invention allows the Purchaser an elegant solution to the above noted problems while increasing the security level in the transaction and decreasing the possibility of fraud to the financial institution.