
World Wide Web: Internet and Web Information Systems, 5, 245–256, 2002

Using Trusted Email to Prevent Credit Card Frauds in Multimedia Products

SALEH I. ALFURAIH Alfuraih@usc.edu
Department of Computer Science, Integrated Media Systems Center, University of Southern California, Los Angeles, CA 90089-2561, USA

NIEN T. SUI (ALSAWI) Alsawi@usc.edu
Department of Computer Science, Center for Software Engineering, University of Southern California, Los Angeles, CA 90089-0781, USA

DENNIS MCLEOD McLeod@usc.edu
Department of Computer Science, Integrated Media Systems Center, University of Southern California, Los Angeles, CA 90089-2561, USA

Abstract

This paper focuses on credit card fraud in Multimedia Products, which are soft-products. By soft-products, we mean intangible products that can be used and consumed without having them shipped physically, such as software, music and calling cards (calling time). The demand for soft-products, mainly Multimedia Products, on the Internet has grown in the last few years and is rapidly increasing. Credit card fraudulent transactions on such products are very easy to conduct, while very difficult to recover, compared to the fraud cases in hard-products transactions. This paper classifies the types of products sold on the Internet, and the usual fraud occurred in each type. It summarizes some of the existing best practices to prevent credit card fraud. Finally, it introduces the use of a Trusted Email as a way to authenticate the customer and to simulate his/her physical address (since on these products no actual shipping will happen).

Keywords: multimedia products, e-commerce, credit card, fraud prevention, Trusted Email

1. Introduction

With the huge demand on soft-products that can be delivered via the Internet such as downloadable movies, music, software, and prepaid phone cards, preventing credit card fraudulent transactions becomes more vital. E-commerce allowed customers to transact without physical interactions and the Internet facilities soft-products and services to be acquired via soft delivery methods: email, download or logging in.

The increased number of credit card frauds has many reasons and the most apparent one is that merchants cannot see the customer to verify ID or signature. This problem also existed even before the Internet in both mail orders and telephone orders, which are known to the credit card community as MOTO. MOTO suffered the same problems as Internet orders do. In this paper a new term will be introduced which is MTIO – Mail, Telephone and Internet Orders. Before discussing the proposed solution it is appropriate to explain some important background information about commerce using credit cards.

1.1. Credit card fraud

Credit card fraud is costing merchants and sometimes customers hundreds of millions of dollars each year. Fraud can happen for many reasons. First, stolen cards which represents almost 25% of the total credit card fraud. Second, counterfeit cards, which are the cards that the criminal acquired the technology that allows him to "skim" the data contained in the magnetic strip of the card and then manufacture a fake card, and this constitutes almost 24% of the total credit card fraud. Third, MTIO, which is the fastest increasing fraud, and it represents 21% of the total fraud so far. Fourth, lost cards, and this constitutes only 15%. The remaining 15% is distributed to the rest of credit card fraud [9].

What happens in case of a fraud? Usually credit card fraud is linked with a charge back that refers to the "returned transaction resulting from the lack of adherence to the conditions of the sales agreement, association regulations, or these operation procedures, and result in the debiting of the merchant account" [9]. Charge back is usually a result of the cardholder dispute of the charges in his statement, and according to some statistics, 90% of the disputes end in favor of the customers over the merchants. That is because in many occasions the transaction has suspicious elements, such as shipping to an address that differs from the billing address, which accounts to almost 45% of MTIO credit card fraud cases. When dispute is honored, the merchant is responsible for the charges and some investigation will take place to find out who received the merchandise. But in many cases the investigation will fail especially for the soft products that are not shipped physically.

1.2. Classifying merchandise products

We classify the merchandise products into two main categories: Hard-Products and Soft-Products, and the latter will be further classified.

(A) *Hard-Products.* This includes all tangible products that require delivery to a physical address if purchased, clear examples are laptops, printers, house-wares, clothes etc.
(B) *Soft-Products.* This includes all intangible products that can be shipped electronically. Before we further classify soft-products we need to define some terms: *Has-Cost* and *Has-No-Cost. Has-Cost* means that this product costs some money considerably high or really high. An example of this is a prepaid calling card has a real high cost while a piece of music is *Has-No-Cost* since it can be recopied millions of times and the cost of copying is comparably very low to its price. Another term to define is traceability. This means a fraud purchase can be *Traceable* if it can be traced to a phone number or an official IP address, or *Non-Traceable* if otherwise.

    (1) *Has-Cost-Traceable.* The loss in this one is not very high. Often the cost of tracing is higher than the cost of the product itself, as illustrated in the following two examples. Customer service for a laptop company, when the machine is not covered by the warranty, the company usually charges per minutes for customer service by asking for a credit card or a bank account, if a fraud happened in this case then the cost was the time of the customer service representative who answers

the call, which is quite high sometimes, depending on the type of customer service he is providing. The cost of tracing this fraud is low since they have info about the original purchaser, and if not then they can add a note in the system to mark this machine as a stolen machine, and when next time someone calls for a service under the same serial number the company will try to get the machine since it is noted as stolen (there are many ways to trace this item, but this is beyond the scope of this paper). In contrast, if a prepaid calling card is purchased on-line then the loss is the price of minutes in the prepaid card itself, which costs many merchants 70–80% of the actual street price of the card. Here the cost of tracing of the fraud is very high since one has to go and see the log for the calls, and if this card has not expired yet – which is a rare case, since the merchant will not know about the fraud until the real owner of the card reports it, which is typically one month from the time of purchase – then they find out from where that thief was making his call and subsequently knock on his door and catch him. But let us imagine that he was using a pay phone or any public phone. In this case there is no way to trace him unless one tries to call the number he was calling and tries to find out who called them and where he lives. In many cases this is not possible since most of the fraud cases are used in international calls and also there is no one database to look at the called number and see who is else calling it from the area around that pay phone and try to trace him. It is clear here that the cost of tracing is high but one more problem in tracing is that it requires a certain amount of money to be stolen before the FBI or the authorities can help on that, and that amount is around $50,000, which means if one has a fraud of less than $50,000 then one has to deal with it with his lawyer which is really expensive since the cost of many prepaid services is on the average of $50 to $100 maximum.

(2) *Has-Cost-Non-Traceable.* These are almost the same products we mentioned above but the delivery method makes it Non-Traceable. For example, a calling card pin number is sent to a free email and opened from an Internet café, or from an international location, in such case there is absolutely no way to trace it.

(3) *Has-No-Cost-Traceable.* The loss in this kind of fraud is extremely low and there is no need to waste more money in tracing the thief. One example of this is downloading a piece of music or software. This piece of music or software costs money to generate, but the cost of tracing the fraud is much higher since one has to find the IP address of the thief who downloaded it and trace it. In most cases this thief can be in an Internet café or in a different country where the cost of one more copy is only the size of the downloaded file divided by the cost of the bandwidth, and this cost almost equals zero.

(4) *Has-No-Cost-Non-Traceable.* The loss in this one is almost the same as the previous one, but given that it is impossible to trace the thief which is even if it was possible it will not be done. A simple example of this is delivering a picture someone ordered to his email, not by download, in this case with this many free email services and the ease of getting one it is almost non-traceable.

1.3. Types of credit card frauds

There are many kinds of credit card frauds and this paper will concentrate on the type of fraud that can occur with the first type of soft-products which is *Has-Cost-Traceable.* The information needed to charge a credit card is only its number and the expiration date. But merchants usually request more information to avoid fraud. For example, the information required for some on-line systems to approve an order is the following: first and last name, address, phone number, email, credit card number, expiration date and the customer service number of the credit card issuer. Many fraud cases can happen, for example, if someone has your name, credit card number, expiration date and billing address, then the current on-line merchant system is only checking two things: (1) if the credit card number is a valid number, (2) if the first 5 digits of your street address and your zip code match the one in the issuer database. All this information is very easy to obtain even from your home mailbox or any on-line transaction that you had before. So even if the thief does not have your name, he still can get the code "YYY" which means that your address and zip matched. In this case it looks like a non-fraudulent order, but to make sure, the merchant has to call the phone number on the order, so if the thief was smart then he/she will not use his home phone number and he will just use a fake number and in this case a fraud is detected and prevented.

But if the thief uses someone's phone number or a public phone number and asks the merchant to call him at a specific time since he will leave home after that time, then there is no way for the merchant to tell if this is a home phone, a pay phone or public phone, unless the merchant asks the customer at the time of order to use the phone number he listed with the credit card company when he applied for the credit card, and in many cases customers forget which number they used. So if the merchant calls the bank and finds out that the number does not match the number provided by the customer then he has to send an email to the customer asking him for his correct phone number. The real problem here is that bank intends not to give any clue to the merchants about the customer's phone number not even the last 4 digits.

Even when a correct phone number is sent to the merchants and they try to call, most of the time they will get an answering machine and in this case the merchants will leave a message or try to call later, so if the customer answers the phone and says, "Yes, I did buy calling cards and this is my credit card" since sometimes small teens use their parents' credit cards and the parents do not approve that. After all this process a fraud is very simple and that can happen if the guy who answers the phone was a fraudulent himself so someone visiting or, as mentioned before, a teenager, or the worst case is when the real owner of the credit card disputes the charge and claims that he did not order it. In this case there is absolutely no way for the merchants to convince the credit card company that their customer is not telling the truth. At this point the credit card company will ask for his signature on the receipt which the merchants never actually received or asked for since it is soft delivery.

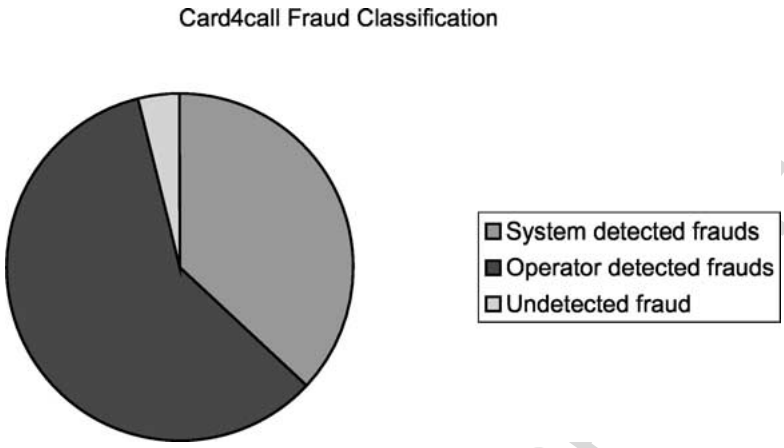

Figure 1. Site 1, Card4Call.com statistics since 10/10/2000 for 1 year.

Table 1. Site 1, Card4Call.com statistics since 10/10/2000 for 1 year

System detected frauds	65
Operator detected frauds	104
Undetected frauds	7
Fraud (sum of above)	169
Total orders	2136
Fraud percentage	7.9%

Obvious suspects. Some transactions have many suspicious symptoms that make them easy to be flagged out, such as:

1. Random orders of big amount.
2. Garbage information (funny names, addresses, incomplete phone or zip codes).
3. Incomplete information, such as no credit card customer service number.

1.4. Case study

We have conducted two case studies with soft-product e-commerce sites, namely, Card4Call and 123CallingCards. Both sites sell calling cards and deliver to customers email addresses. Both sites have experienced quite a number of fraudulent transactions, and are actively applying automatic and manual fraud prevention methods, such as verifying address, or calling the bank and customer. Table 1 and figure 1 show the statistics of fraud transactions occurred with Card4Call.com. Similarly, table 2 and figure 2 show statistics for 123CallingCards.com.

One important thing to point out when looking at these data sets is the fact that the losses are not limited to undetected fraud cases. Although, often these cases cost the most in terms of charge back penalty. We have to look at the loss in terms of the fees charged by

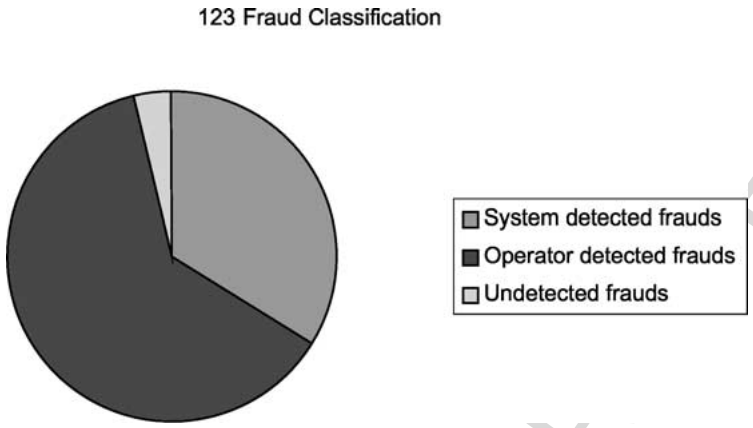

Figure 2. Site 2, 123CallingCards.com statistics since 11/23/2000 for 1 year.

Table 2. Site 2, 123CallingCards.com statistics since 11/23/2000 for 1 year

System detected frauds	74
Operator detected frauds	136
Undetected frauds	8
Fraud (sum of above)	210
Total orders	2124
Fraud percentage	around 9.8%

the credit card company for charging and refunding the detected fraud, time spent for the operator to detect and prevent the fraud cases, and on top of that the loss of opportunities due to time wasted and customer satisfaction's concerns (as explained in the next section).

1.5. Hassles and inconvenience faced in e-commerce

This section will identify some of the inconveniences faced by merchants and customers. They can be summarized as follows:

- Merchants need to trade off between fraud transactions and processing delay and cost.
- Customers need to trade off between information privacy and shopping on-line.
- New trends that may be considered as anomalies, for example, customer let a bill payment company to handle his bills. This in turns makes his billing address the address of the company, and raises various anomalies in contact information and billing information.
- To avoid fraud, merchants need to call both bank and customer:
  - Problems with calling banks: sometimes no toll free numbers, sometimes not 24×7, sometimes system not available, sometimes the bank does not verify customer name and phone number.

  - Problems with calling customers: calling customer costs money and time, customer may not be available and no perfect time to call, sometimes it is too early, sometimes too late.

- Inconvenient for customer to wait for merchant phone calls.

These inconveniences and fraud cases jeopardize e-commerce mass acceptance, as many customers are reluctant to shop on-line [8].

2. Other solutions related to credit card fraud

Credit card fraud problem has been a concerned topic in the area of business, IT industry and academia, and regulatory authorities. Various ways of detecting and preventing credit card frauds has been proposed. Each solution comes to target certain aspect of this multi-faced problem.

In [4], a distributed data mining approach for credit card fraud detection is proposed. In [1,2,6], various types of neural network solutions and neural data mining are proposed for credit card fraud detection. In [7] a density-based clustering and radial basis function modeling is propoced to generate credit card fraud scores.

As an example of IT vendor solution, Microsoft and other vendors, Orbiscom Inc. and Cyota, have come up with credit card surrogate number that can be used for only one on-line transaction [3]. American express has a similar "proxy/filter" service that shields users' credit card information from being exposed on the net. Visa has its Verified solution, similarly, MasterCard and Discover have their own fraud prevention methods [8].

Tradecraft has obtained a patent for its Internet Payments solution. The proposed solution is a system of payment where a cable company or ISP acts as a trusted authority for billing subscribers when they purchase from on-line third parties. This consortium of ISPs and/or vendors will act as the intermediary to facilitate Internet payment, somehow similar to Visa International [5].

Often, these solutions either require customers to download some software (as in MasterCard and Discover solutions), or that the bank and merchants need to modify their system or checkout procedure (as in Visa Verified). All these solutions cost money for merchants or banks to be compliant with, and need mass acceptance before they can be declared success.

3. Current identification and authentication protocols

3.1. Cardholder Verification Value 2 (CVV2)

It is a unique three or four digits number on the credit card itself, and most of the credit cards are required to have this number. This number can be verified on a real time by almost all MTIO merchants. This number is supposed to help merchants verify that the customer who is making this purchase is really having the card physically. CVV2 can lose its purpose if it is used everywhere, since in almost all the cases where a fraud can happen,

Figure 3. Current AVS.

the fraudulent customer can have such info. For example, if the thief stole the cards then he has the CVV, also if he hacked into an on-line system or sniffed a connection then he will also obtain the number.

3.2. Address Verification Service (AVS)

In this service (see figure 3), a real-time checking of the cardholder first 5 digits of the street address number and zip code is performed to verify that the billing address of the customer matches with what is stored with the credit card issuer. This is to ensure that the merchants will not risk the possibility of the customer end up disputing the transaction. Because it is the responsibility of the customer in case the merchandise is delivered to his billing address, even if he did not sign for it. This is the reason why many merchants require their customers to register their shipping address as an alternative shipping address if it is different than their billing address.

4. Proposed solution – Temail

Nowadays, for all soft products MTIO, which require an email delivery, the merchant is taking the risk by emailing the customer the products. As explained before, this risk is even worse than delivering to a non-billing address for a hard-product, since email tracking is much more difficult comparing to tracking who lives at that address at the time of delivery. Figure 4 shows the current situation.

In this paper, we propose a Trusted Email solution that can track and minimize on-line frauds, see figure 5. Before we state the solution, let us examine some cases where an email is used as a verification method (instead of billing address). In this case, the email address of the customer is stored at his credit card issuer database. When the customer makes an on-line order for something to be delivered via email, the system contacts the bank automatically and compares the two emails, the stored and the supplied emails. This can be performed easily since an email address is not like a name or a street address, which can be written in different way. It is more effective than matching the billing address. Since there are no two different emails, one for shipping and one for billing, and even if other people know your email address, they cannot access your account (unless by hacking). Email accounts are unique which makes it easy to be verified. In case the email does not match, the only thing the merchant has to do is to email the customer to send his "trusted" email address or cancel his order.

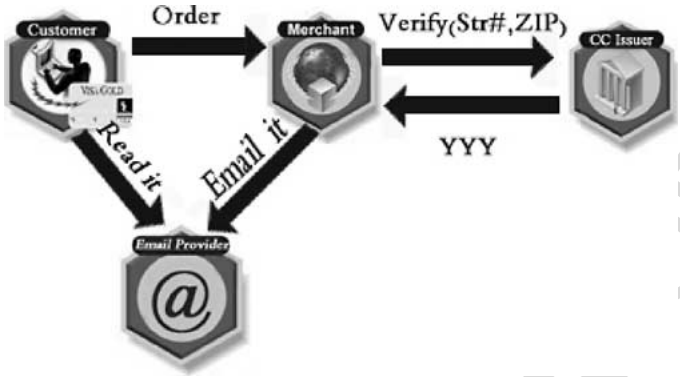

Figure 4. Current AVS with soft-products.

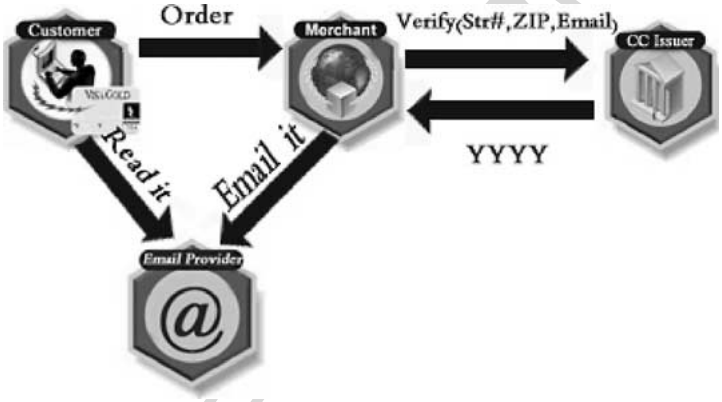

Figure 5. Proposed new AVS.

This solution will work perfectly if the fraud comes from an outsider. However, if the credit card owner is the one who commits fraud, it is difficult to convince the credit card issuer that the dispute is invalid. Because the credit card company will not investigate and ask Hotmail or Yahoo if merchant M did sent an email to customer C with email E at that date and the content of the email. Even if there are automatic investigation technology between the credit card issuer and the email provider, there may be many privacy and legal issues involved. Moreover, what if the customer who denied his own transaction has his own email server.

Therefore, we propose to have a *Trusted Email Server* that anyone who wants to buy products that can be delivered via email should subscribe to it and register it with his credit card company. Therefore, when a fraud occurs, the credit card company will ask that Trusted Email company if the merchant M emailed customer C to his email E at that date and what was in that email. After verifying that the transaction has occurred and the product has indeed been delivered, the credit card company can then reverse the charges to the merchant and reject customer's dispute, as in figure 6.

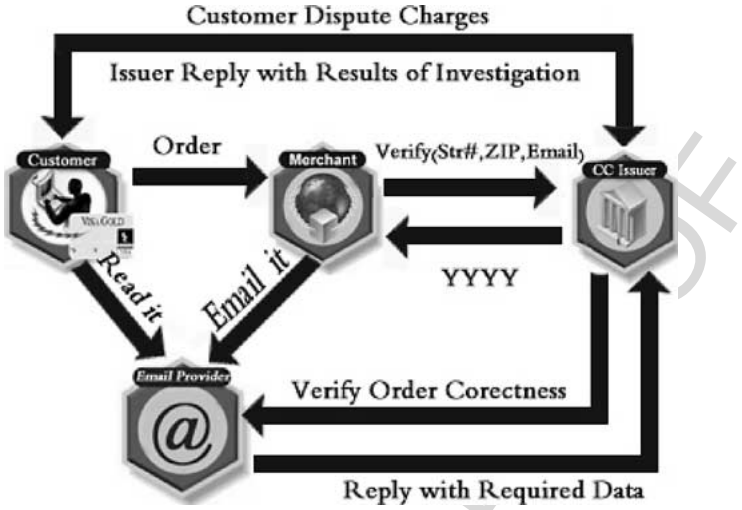

Figure 6. Disputes cycle in the new AVS.

4.1. How Trusted Email works

The Trusted Email (TE) will have the first 6 digits to identify the card issuer. The customer will register his email with his credit card issuer. Each bank fraud department will have an account to login to the Trusted Email Server (TES) and view the history of the customer and verify the transactions. The bank will only view the customer who has cc with them. The emails in the TES will not be deleted until the dispute time is over. All e-sites have to register an email where we only accept email from it. The TES will block any incoming emails that are not originated from a subscribed merchant system. The user will not be able to access this email account, but merchants can connect to the TES with a special client.

Figure 7 shows the steps for approval or denial when an order is placed. The customer will visit the e-commerce site (e-site). If he does not have a Trusted Email, the customer needs to register one and inform his credit card issuer of this email. If he has a Trusted Email (TE), he can proceed and place the order, which will be subject to full address verification (FAVS) which includes Trusted Email verification, in addition to the traditional AVS. If the verification failed, the customer will be notified and his order will be verified one more time only. Repeated denied transactions will be black listed, to avoid infinite looping for FAVS step.

5. Discussion

Some will argue that fraud committer can obtain the email password, or can sniff unsecured email contents, which results in the customer paying the price for the fraud, instead of the merchants or the credit card issuers. This argument can be true with any solution, say the fraud committer got access to your physical mailbox, or he obtained your Verified by Visa

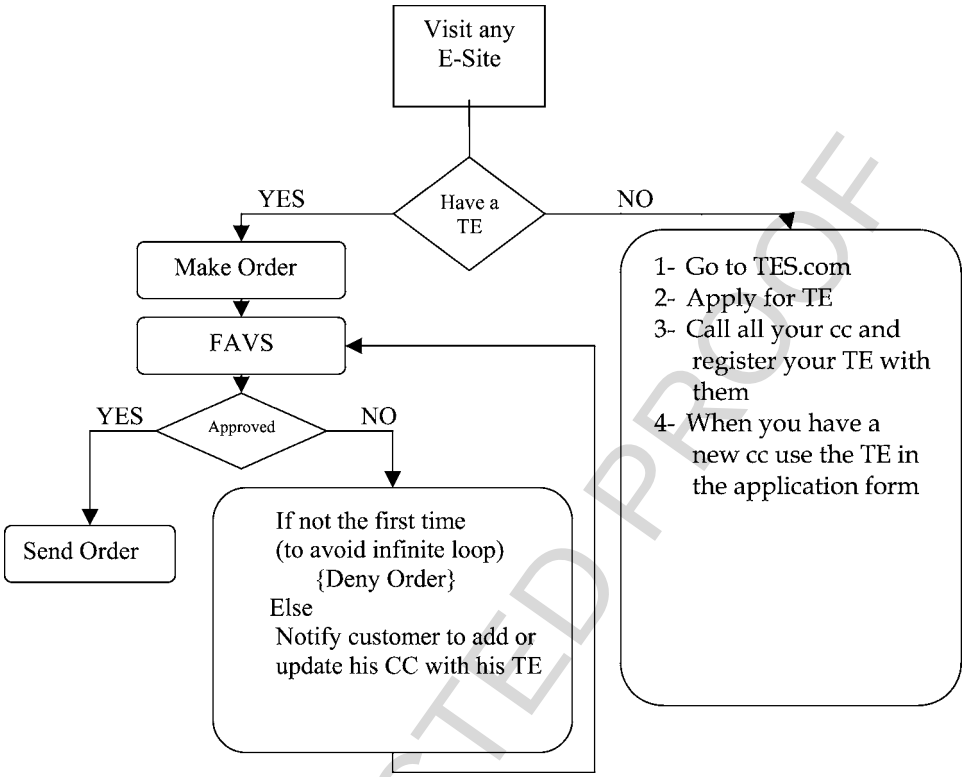

Figure 7. How Trusted Email works.

password! There are no silver bullet solutions. Our proposed solution is much superior than any current system that uses billing address or other codes for verification. This solution is easier to implement than credit card secret codes or having a surrogate credit card number. The solution has none of the common drawbacks of other proposed solutions [8], such as altering current e-commerce sites checkout procedures (as in Verified by Visa), requiring customers to download (as in MasterCard or Discover), or changing the systems of existing credit card numbers (as in surrogate numbers).

The best solution to prevent credit card fraud transactions is the one that can be implemented with minimum cost, requires minimum changes for all parties (customers, merchants, and credit card companies/banks), and has incentive for all parties to participate.

We will discuss our solution's implementation details and comparison with other solutions in future papers.

6. Conclusion

In this paper we reviewed the fraud types that occur in e-commerce transactions using credit card as payment method. We classified the merchant products into soft and hard

products, in terms of their delivery method; and has-cost and no-cost, in terms of product values; and traceable and non-traceable, in terms of fraud traceability.

Our proposed Trusted Email Server solution is a noble solution that uses familiar concepts as Email to satisfy the fraud prevention requirement and minimize disturbance in the current credit card and e-commerce systems.

References

[1] E. Aleskerov, B. Freisleben, and B. Rao, "CARDWATCH: A neural network based database mining system for credit card fraud detection," in *Computational Intelligence for Financial Engineering (CIFEr), Proceedings of the IEEE/IAFE 1997*, 1997, pp. 220–226.

[2] R. Brause, T. Langsdorf, and M. Hepp, "Neural data mining for credit card fraud detection," in *Proceedings of 11th IEEE International Conference on Tools with Artificial Intelligence*, 1999, pp. 103–106.

[3] M. Bruno, "Microsoft gives boost to surrogate card numbers," Bank Technology News, `http://www.breakbanktechnews.com/btn/articles/btnoct01-1.shtml`

[4] P. K. Chan, W. Fan, A. L. Prodromidis, and S. J. Stolfo, "Distributed data mining in credit card fraud detection," *IEEE Intelligent Systems* 14(6), November–December 1999, pp. 67–74.

[5] M. Duvall, "Consortium to facilitate Internet payments," *Interactive Week*, September 24, 2001, 26.

[6] S. Ghosh and D. L. Reilly, "Credit card fraud detection with a neural-network," in *Proceedings of the Twenty-Seventh Hawaii International Conference on Information Systems: Decision Support and Knowledge-Based Systems*, System Sciences, Vol. 8, 1994, pp. 621–630.

[7] V. Hanagandi, A. Dhar, and K. Buescher, "Density-based clustering and radial basis function modeling to generate credit card fraud scores," in *Proceedings of the IEEE/IAFE 1996 Conference on Computational Intelligence for Financial Engineering*, 1996, pp. 247–251.

[8] Ch. T. Heun, "Fear of fraud," Information Week.com, March 4, 2002, `http://www.informationweek.com/story/IWK20020301S0002`

[9] Vantage Card Services Inc., Prevent chargebacks, `http://www.vantagecard.com/html/preventchargebacks.html`

[10] Yahoo, Merchant operating procedures guide, `http://sg.store.yahoo.com/mopg.html`