Abstract: - Soft-products are intangible products that can be consumed without shipment, such as software, music and calling cards (calling time). The demand for soft-products on the Internet has been increasing for the past few years. At the same time, fraudulent credit card transactions have also increased. Compared to tangible products, fraudulent credit card transactions on soft-products are easier to conduct whilst difficult to recover. Fraudulent transactions are a major problem for e-commerce merchants, customers, and credit card issuers. The Trusted Email mechanism is new way to prevent fraudulent transactions on soft-products. Trusted Email is a custom email solution that can uniquely identify and authenticate the online customer, prevent unauthorized credit card transactions, and effectively resolve e-commerce disputes. In this paper we will study where the Trusted Email server should reside, who should handle it and why. In accordance with the best location of the Trusted Email server, Anonymous credit card transactions will be also studied in this paper and the new term “Selective Anonymity” will be introduced.

Key-Words: – E-Commerce, soft-products, credit card fraud, Internet security, trusted computing, privacy, anonymous transactions, Selective Anonymity

1. Introduction
The requirement to prevent fraudulent credit card transactions on soft-products e-commerce is increasing as never before. By soft-products, we mean products that can be delivered via the Internet without physical shipment, such as downloadable movies, music, software, and prepaid phone cards. Credit card fraud is costing merchants, and sometimes customers, hundreds of millions of dollars each year[1]. Fraud occurs 25% of the time due to stolen cards; 24% due to counterfeit cards, where the criminal acquires the technology that allows him to “skim” the data contained in the magnetic strip of an authentic card and then manufactures a fake card; 21% due to non-physical presence transactions in Mail, Telephone and Internet Orders (MTIO), the fastest increasing fraud; 15% due to lost cards; and the remaining 15% is distributed among the rest of credit card fraud [1].

Merchandise products are classified in two main categories: hard and soft. This paper will concentrate on the credit card frauds that can occur with soft-products. The information needed to charge a credit card is only the credit card number and the expiry date, but merchants usually request more information to prevent fraud. For example, the information required for some online systems to approve an order is the following: name, address, phone number, email, credit card number, expiry date, the customer service number of the credit card issuer, and special codes on the physical card. Some merchants ask for all of the above and some require only couple of them. The merchant then verifies with the credit card issuer the accuracy of the supplied information.
So far, the industry state-of-the-practice verification system is the online address verification service (AVS), which can only check whether the supplied address and the zip code match or mismatch with the stored information in the credit card issuer system [3] [4]. AVS is practical for hard-products since the billing address can be the same as the shipment address, or at least can be traced to a physical address. However, AVS is almost useless for soft-products. Any individual that obtains credit card information and the billing address of that card can easily place a fraudulent order for a soft-product. Neither AVS nor the conventional tips for fraud prevention [5] [6], are designed for soft-product e-commerce. Trusted Email mechanism [2] solves most of the existing problems with soft-products.

The location of the trusted email server is what makes the difference in the implementation and the policies required. With a Trusted Email server an anonymous transaction might be possible if it is located at the right place. The remainder of this paper is structured as follows: section 2 will give a brief description about Trusted Email. In section 3 we will state the way trusted email works. The location of the server in the Trusted Email mechanism will be studied in section 4. In section 5 the reason for choosing one location as the best location will be justified. The possibility of having an anonymous transaction with a Trusted Email server placed at the right place will be illustrated in section 6. We conclude this paper in section 7. Finally, Future Work will be suggested.

2. Trusted Email Technology
All MTIO merchants of soft-products that require an email delivery are taking a risk by emailing the customer the purchased products. This risk is even worse than delivering to a non-billing address for a hard-product, since email tracking is much more difficult compared to physical address tracking.

A trusted email (TE) solution [2] uses a customized email server that can prevent online frauds for soft-products and investigate disputes efficiently, see Fig.1. The concept of this solution is to treat the email address as the shipment/billing address, just as the physical address is used in the case of hard-products. The trusted email solution enables a more comprehensive address verification system, called full address verification system (FAVS), which (Fig.1) first, allows the customer to order from a merchant, then the merchant verifies the email address of the customer on top of traditional AVS. After that, if all the verifications are correct, the merchant will email it to the customer’s email and finally the customer reads his email to receive what he has ordered. The email address needs to be stored in the credit card issuer system in addition to the other information. 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 the order. Email accounts are unique which makes it easy to be verified.

This solution, to register the email in the credit card issuer system, will work perfectly if an outsider commits the fraud. However, if the credit card owner is the one who commits fraud by for example disputing a purchase he made, it will be difficult to convince the credit card issuer that the dispute is invalid, because the credit card company will not investigate with the free mail provider (e.g. Hotmail or Yahoo) to verify whether or not the merchant did send an email to the customer containing the ordered soft-product. Even if the email provider agrees
to investigate, there is no automatic investigation technology, and there may be many privacy and legal issues involved. The situation can be more challenging if the customer who denied his own transaction owns the email server.

Therefore, a trusted email server (TES) has been proposed to be used with e-commerce soft-products. The shopping-customers are requested to have an account on TES and to use it for their transactions. By that, when a fraud occurs, the credit card issuer can query the trusted email server whether the merchant M emailed customer C to his email E on a certain date and whether the email content included the ordered soft-product or not. After verifying that the transaction has occurred and the product has indeed been delivered, the credit card issuer can then reverse the charges to the merchant and reject customer’s dispute, as in Fig.2. This process can save the time of all the stakeholders and can protect the merchants from fraudulent transactions or unjust disputes.

![Fig.2: Disputes cycle in the new FAVS](image)

### 3. How Trusted Email Works

Trusted email (TE) is the name of the technology itself, and it consists of the following elements: credit card issuers, merchants, customers, and the trusted email server (TES). A brief explanation of each element role is listed below.

**Credit Card Issuer:** Each issuer will be granted access to the TES that enables him to use these services to check a customer credit history before approving the credit application, inform the customer of credit card approval and manage card activations through TES, dispute management for online purchases and set the dispute period duration after the charge is billed in the statement.

**Merchants:** Each merchant will have to register for a merchant TE account to deliver any soft-product item to their customers. The merchant account has the capability to send to an unlimited number of customers. TES allows merchants to send emails to TE normal accounts only. Through the TES, merchants will be receiving dispute emails from customers or credit card issuers. The TES dispute management system will integrate the necessary information for the dispute for all parties in order to resolve it efficiently. The TES will handle any mail delivery failure and notify senders of any problems. Merchants can have multiple TE email accounts if they have multiple sales departments. It is to the benefit of the merchants to request their customers to register for a TE account before purchasing using credit cards, hence preventing any possible credit card fraudulent transactions. The registration steps of TE accounts can be easily integrated with the merchant website and the process is similar to setting up any free email account (but with less marketing options not like most of the free emails). If a merchant allows a non-TE customer to purchase, he will deliver the soft-products under his own risk.

**Customers:** The customers will have to register with the TE and provide correct information, such as name, address, and telephone. If any of the information provided is incorrect or outdated, the customer will lose the right to dispute any fraudulent transactions through the TES. After obtaining an account on TES, the customer then has to register this TE account with all his credit cards issuers, in order to use the FAVS while shopping online. Each customer can have an unlimited number of accounts (since he might share them with
family members), but the customer is informed that sharing access to the TE account is similar to sharing a credit card. Customers’ TE accounts can only receive or reply to emails. They cannot send new emails, which prevents them from becoming a burden on the TES.

**Trusted Email Server (TES):** The server will be handling all the logistics to help optimize the efficiency of this solution. The TES is a mail server with added capabilities. The new capabilities are listed below with the benefit of each one:

1- Tracking and record keeping of all purchase transactions: The emails in the TES will remain in the system until the period of the dispute ends. The emails are then archived to offline storage. The dispute period is usually from the time of the purchase (in this case the time when the email is received) to the maximum time set by the credit cards issuers. The dispute period is typically from 30 days up to a maximum of 180 days from the date of receiving the statement (as in the case of American Express).

2- Allowing only TE user mail to be processed: TES will allow only the emails that are originated from a subscribed merchant or credit card issuer system (to prevent spam-mails and to save bandwidth and storage) and will block emails from non-TE users. Merchants are not allowed to send any marketing emails, such as new offers or deals; for this purpose they need to ask their customer for another email to which they can send such marketing emails. If a merchant violates these regulations, a fine will be charged. Repeated violations will result in disabling the account, which means that the merchant cannot send new emails, but it can still view old emails and investigate disputes. There are three types of emails that the merchant can send: order confirmations, ordered materials, and dispute follow-ups and chargebacks. For every email, the customers are facilitated with the functionality to report any merchant violations to the regulations.

---

**Visit any E-Site**

**Have a TE**

- **Make Order**
- **FAVS**
- **Approved**
- **Send Order**

**YES**

- **If not the first time**
  - (To avoid infinite loop)
  - (Deny Order)
- **Else**
  - Notify customer to add or update his credit card with his TE

**NO**

1- GO to TES.com
2- Apply for TE
3- Call all your credit card issuers and register your TE with them
4- When you apply for a new credit card use the TE in the application form

**Fig.3: How Trusted Email Works**
3- Encrypting the connection with a special email client: Trusted email clients will connect to the TES using encrypted communication. The client software differs on the bases of the types of users, normal-shoppers, merchants, and credit card issuers.

4- Internationalization and localization: The TES will allow business rule settings and dispute policy depending on the country of the credit card issuer. The language of the user interface is customizable as well to meet the local needs.

Fig.3 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 account, the customer needs to register one and inform his credit card issuer of this email. If he has a Trusted Email account (TE) he can proceed and place the order, which will be subject to full address verification (FAVS) including Trusted Email verification. If the verification is unsuccessful 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.

TE solution covers the following key requirements:

**Authentication:** TES provides user login validation.

**Privacy:** The credit card issuer and merchants can only view the transactions that are under dispute. As for credit history, the credit card issuer can only know the credit rating of the customer not the type of merchants that were involved in the purchases.

**Integrity:** TES maintains integrity by ensuring the recording of the transactions and handling email failures.

**Non-repudiation:** All transactions are recorded and logged. If the merchant has delivered the product to the customer, yet the customer denied payment, all these details can be viewed in the system.

**Low Cost:** The cost of such system can be economic compared to monopoly solutions from single vendors, such as Visa or American Express alone.

**Ease of Use:** The concept of Email is known to all the stakeholders of e-commerce. Even with the TES special secure client software, it can be easily integrated into the existing email client software (a plug in).

There are other quality issues (level of service) related to the design of the TE solution. The main ones will be pointed out here:

**Scalability:** The system shall be able to scale as the number of users grow. This requirement is achievable as we see in current email systems. However, there are many trade-off issues in how to scale and whether or not we should divide users according to their countries.

**Security:** Encrypted email is not a new technology. However, the use of it in a large scale by the public, and integrating it with other non-secure existing software requires a more careful study.

**Availability:** TES should be used by users 24*7 as in current verification and financial systems. Therefore, single failure may affect a large
number of e-commerce stakeholders.

**Compatibility:** The interface to TES should be simple and should adhere to current existing e-commerce technologies. Since compatibility is a major factor affecting the acceptance and adoption of the users, it is necessary for the merchant systems to use the new FAVS codes, and to redirect shopping-customers to register for TE accounts. The credit card issuers systems need to store the new TE information of their card holders, and to generate the proper FAVS codes.

For a technology to succeed, the acceptance and adoption of the critical stakeholders is vital [20]. In TE solution, the winners are the technology key stakeholders [21] [22]. For TE solution, the needs and the win-conditions of all key stakeholders should be analyzed, namely credit card issuers, merchants, and shopping customers. In [2] the analysis of one type of soft-product e-commerce sites, namely calling card sites is stated.

**4. Where To Place TES**

TE is a great way to fight fraud in soft products, choosing the right location for TES may increase the functionality of the system. As any other SW system it could have two main locations, centralized or distributed.

**Centralized TES:** the server will be placed at one trusted location e.g. government agency or a University. Every TES user has to visit TES and open an account and all the transactions and disputes have to go through this TES. It is clear that this centralization will benefit all parties since they deal with one trusted party and they will not have many places to visit every time they want to buy something. Implementing, monitoring and maintaining the TES is not a cheap thing to do, so making it operate as one centralized system will lower the expenses and the ROI is greater. Spending more in securing the system will be justifiable since the number of users will be huge and a lot of sensitive information could be stored in it. Having a centralized system suffers the usual problem facing any centralized one. Single point of failure, delay because of geographical location or massive number of concurrent transactions, and customizing the system to fit all the possible users’ needs is a difficult job since some of them may conflict and the system will be asking for many inputs to satisfy all the users. For example, some merchant may need your home address and some may not, but since the system does not know what information it needs- and what is necessary- it will ask for every thing.

If we choose the Centralized system, then it has to be hosted and maintained by a global trusted party, either related to one major country like the DNS root server which is hosted in the USA and maintained by them and all the Internet users rely on it, or it could be a separate global organization some how connected to the WTO or the United Nations.

**Distributed TES:** the TES will be located at many TES providers, each provider serves many users and every user may subscribe to more than one provider. Every provider has to be trusted by his users and that is what differentiates one TES from an other.

If we choose the distributed system, then any company can buy the license to use the TES and attract customers by providing many additional features and increase their trust. Some good candidates are current Email providers, since they already have most of the needed hardware and software infrastructure, Telecommunication companies, and credit card issuers.

A midway possibility could be between centralized and distributed, which is distributed
in general which means many systems exist but centralized to some factor like geographical location, one example of this is the architecture of the PKI Technology which distributed from the sense that it allow many (Root Authorities) RAs to exist but it is centralized since each country has it is own Root Authority and all the citizens of this country have to use it if they want to use their country PKI.

5. Best TES Provider

It is clear that there is no easy choice to be made, but if mixing the centralized and distributed systems to get the best of both, it will lead us to use one location as the best location, which will satisfy most of the features in both systems and will avoid most of the obstacles. Credit card issuers are our choice.

Credit cards issuers are our choice for the best location for many reasons. They are distributed from the sense that every issuer (Visa, MC, AMX, etc) will have their own copy of the TES and are centralized from the sense that all the card holders are using the system of their card issuers and they have no other choice. We will analyze this location and study the advantages and disadvantages and what other improvements can be made to solve the disadvantages or improve the system.

The Choice of credit card issuers as the best location can have many advantages, first, they are the most qualified in terms of having direct involvement in the transaction – the people who have direct involvement in the transaction are customers, merchants and credit cards issuers. Second, they are also the most capable to invest in this financially. Third, they usually have the latest technology in terms of software and hardware and most of the issuers already have email servers. Fourth, one of the most important features of TES is to assist in any dispute case, and credit card issuers are the ones who will take the decision in such cases. Having the TES at the credit card issuers control will ease the case for dispute resolution since there is no access control problem, no delay for negotiation, and all the information pulled is 100% correct. Imagine what will happen in case where the TES was located somewhere else, first they would need a good security check to make sure that the people who are asking for the information are really the credit card issuers, and also this is not enough, they would need to make sure that this issuer was the one who issued the credit card which was used in this transaction. The negotiations to verify the identity of the issuers and to get the information required would consume a lot of time and resources. Last but not least, the information received from the TES if it is not controlled by the credit card issuer is not authentic, so the credit card issuer would have to make a decision on non-authentic information. The fifth advantage is that there would not be any need for the customer to call to register his email, since all this information would be taken from the credit card application and they would be the ones to ask him for his email since they would issue him the email themselves. For example saleh_alfuraih@visa.com. Sixth, in case of any problem in the order then the customer could make one call to enquire why he was not getting the product yet and was his credit card being charged or not, in the second scenario he has to call the TES and check why no delivery yet, and then he would have to make another call to check whether or not his credit card was being charged or not and by how much.

At the moment the only conceivable disadvantages are first, the limited choice for the customer as to which TES he/she should use. For example if the customer wishes to use a Visa card but does not like the way Visa delivers the product or the Visa interface. Secondly, lack of competition, which implies lack of improvement in the system since there will not be so many competitors, compared to an open market situation.
6. Selective Anonymity

After justifying why we chose the credit card issuer as the best location for TES, we are proposing here an improvement to the system if this choice is selected. The improvement proposed is having the credit card number to be your email address instead of using your real name or a nick name, so instead of issuing Saleh I alfuraih, the email saleh_I_alfuraih@visa.com when he apply for a visa, we issue him the email 4226350100001111@visa.com. We are claiming that doing so, will provide a desirable level of anonymity to many people. The following example explains our claim, suppose that Saleh wants to buy a piece of video that is banned, illegal or he does not want any body to know about him for any reason, then he goes to this website which sells this piece of video and purchases it, at the check out stage he enters the following information, name 4226350100001111 and email 4226350100001111@visa.com and credit card is 4226350100001111 expire 11/05. This information is enough for the merchant to send the piece of video to the email and charge the credit card since there is no risk of some one using another persons credit card because he will not benefit from the video in 4226350100001111@visa.com mail box.

This example illustrates that the merchant has no way to know who the card holder of this credit card is, so the identity of the card holder is anonymous to the riskiest part of the transaction which is the merchant since most of the time they sell the information they have about their customers. Only in the case of a dispute will the credit card issuer know what the customer purchased, since it appears as a soft-product from XYZ merchant and no more. If the customer disputes a charge on his credit card then it is either he says that he never ordered, which is ok since that’s not a problem for him, or he claims that he never received what they have charged him for and also this is ok since there is nothing for the issuer to check. Only if the customer claims that what he ordered is not what he received then the credit card issuer will check with the merchant and know what has been ordered. It is clear here that this gives the customer a high level of anonymity which is not available now in the credit card system. Most of the people have no problem that credit card issuers know what they ordered since they will bill them at the end of the month anyway, but what is important is that the merchant knows nothing about their identity and this improvement in the TES will provide this level of anonymity and we call it “Selective Anonymity”. Selective anonymity means that the person can be selectively anonymous. If the credit card holder could apply for a credit card anonymously, then we reach a full instead of selective anonymity.

Possible holes in this suggestion are the same holes exist in the TES which some one knowing your email is ordering something just for the fun of it not to benefit from it. Even though the inventors of TES suggested some solutions, in this paper we give one solution that could fit all the systems. The solution is classifying the products by the merchant. The following example will clearly show what we mean. The Merchant M has a soft-products store and he sells air-lines tickets, Music, and calling time. Since each of these products have different value to the merchant, air-lines tickets before traveling is just bits going through his web server and the actual cost is the charge from the hosting company, then it is almost worthless and he classify it as class C. music has some cost but the benefit is high and it worth the risk or the value is not very high, this is classified as B. Calling time is expensive since the merchant pay for the time on the card in advance, so he classify it as A. now the merchant will program his e-shop system to do the following: If the product is class C, check the validity of the card and send the products if valid. If the class is B, then the merchant will send the products after verify the card and ask the customer to check. Only if the customer claims that what he ordered is not what he received then the credit card issuer will check with the merchant and know what has been ordered. It is clear here that this gives the customer a high level of anonymity which is not available now in the credit card system. Most of the people have no problem that credit card issuers know what they ordered since they will bill them at the end of the month anyway, but what is important is that the merchant knows nothing about their identity and this improvement in the TES will provide this level of anonymity and we call it “Selective Anonymity”. Selective anonymity means that the person can be selectively anonymous. If the credit card holder could apply for a credit card anonymously, then we reach a full instead of selective anonymity.
to reply with an email if he acknowledge the order, then the merchant will email the product if he receive the confirmation email.

In case of a dispute then in class C always the customer wins but the merchant’s loss is minimal. In case it is B then the TES will allow the credit card issuers to verify if there is disclaimer saying don’t download it if it is not yours and if it there then the merchant win, if not, the customer win. In class C the credit card issuer will check if the customer reply with a purchase confirmation, if yes then merchant win if not the customer win.

One main point here, this classification is just for the example and it could be two instead of three or more than three if the merchant wants and depending on the sensitivity and the cost of the products.

People reading this paper may ask, what happens if the customer order class A product then deletes the confirmation email, in this case we encourage the reader to read the first 2 papers about TES.

7. Conclusion
The best solution to prevent credit card fraud transactions is the one that can be implemented with minimum cost, requires minimum changes for all stakeholders (customers, merchants, and credit card issuers), and has strong incentive for all stakeholders to adopt.

The TES solution is very promising and precisely serves the need of preventing credit card fraud in soft-product e-commerce. However, several technical challenges are there, such as scalability, security, and integration with existing systems; as well as several non-technical challenges, such as adoption and mass acceptance.

It is believed that the proposed solution is far superior to any current system that uses billing address or other codes for verification. This paper studies the possible location of TES and who should be responsible for it. Implementing maintaining, and monitoring the TES is not an easy thing to do, so many decisive factors have to be available in the chosen location and candidate. Credit card issuers were the best choice and we justify it clearly. An improvement to the system if the credit cards issuer is chosen to be the best TES host is proposed by using the credit card number as the email of the card holder. Selective Anonymity which is to be anonymous to a group of people who you choose is introduced. It was clearly shown that using the credit card number as the email of the card holder will satisfy the selective anonymity feature. Finally a possible hacking to the system is mentioned and the solution to each is proposed by classifying the soft products.

8. Future Work
This is on going research and the details of the TES architecture and implementation are still in the abstract stages. Other future plans include:

- Investigating the use of Web Services technology in the TES (particularly in implementing the FAVS)
- Developing the notion of “Trusted Receiver” in the email domain, as so far the industry is mainly focused on “Trusted Sender” [23] [24]
- Investigating other forms of trusted interaction between components in e-commerce

REFERENCES


Brause, R., Langsdorf, T., Hepp, M. Neural data mining for credit card fraud detection. Proceedings of 11th IEEE International Conference on Tools with Artificial Intelligence, 1999 Page(s): 103 –106


Duvall, Mel, Consortium to Facilitate Internet Payments. Interactive Week September 24, 2001 Issue page 26


Atif, Y., Building trust in e-commerce, Internet Computing, IEEE, Volume: 6 Issue: 1, Jan/Feb 2002 Page(s): 18 –24


Boehm, B., Bose, P., Horowitz, E., Ming-June Lee, Software requirements as negotiated win conditions, Proceedings of Requirements Engineering, 1994., 18-22 Apr 1994 Page(s): 74 –83


TRUSTe and ePrivacy Group, Trusted Sender program, http://www.truste.org/programs/pub_trustedsender.html