TRUSTED EMAIL

A Proposed Approach to Prevent Credit Card Fraud in Soft-Products E-Commerce

Nien T. Sui, Saleh I. Alfuraih, Dennis McLeod
Department of Computer Science, Integrated Media Systems Center, University of Southern California, Los Angeles, CA 90089-2561, USA

Keywords: E-Commerce, credit card fraud, Internet security, trusted computing

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 while difficult to recover. The fraudulent transaction is a major problem for e-commerce merchants, customers, and credit card issuers. In this paper, we classify the type of products sold on the Internet, and the common fraud that occurs for each type. We review some of the best existing credit card fraud prevention methods and introduce the Trusted email mechanism as a new way to prevent fraudulent transactions on soft-product. 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.

1 INTRODUCTION

The demands to prevent fraudulent credit card transactions on soft-products e-commerce are 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. Fraud occurs 25% of the times 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), which is the fastest increasing fraud; 15% due to lost cards; and the remaining 15% is distributed among the rest of credit card fraud (Vantage Card Services, n.d).

We classify the merchandise products into two main categories: hard-products and soft-products. Then we further classify them based on the traceability of the fraud (Alfuraih, Sui, McLeod 2002):

Hard-Products: This includes all tangible products that require delivery to a physical address if purchased, such as laptops or clothes.

Soft-Products: This includes all intangible products that can be shipped electronically.

Has-Cost-Traceable: The loss in this one is not very high. Often times the cost of tracing can be higher than the cost of the product itself, due to the high cost of tracing (time of the agents at the financial institutes, merchants, and FBI).

Has-Cost-Non-Traceable: The loss is high, and traceability is almost impossible. For example a Calling card pin number is sent to a free email and accessed from an Internet café, or from an international location. In such case there is absolutely no way to trace it, yet the loss can be high.

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.

Has-No-Cost-Non-Traceable: The loss in this one is almost the same as the previous one, but it is practically impossible to trace the thief. An example

T. Sui N., I. Alfuraih S. and McLeod D. (2004).
TRUSTED EMAIL - A Proposed Approach to Prevent Credit Card Fraud in Soft-Products E-Commerce.
In *Proceedings of the Sixth International Conference on Enterprise Information Systems*, pages 106-113
DOI: 10.5220/0002612101060113

of this is delivering an ordered picture to email, not by download (no exact IP). In this case, with so many free email services and the ease of getting one, it is almost non-traceable and therefore impractical to spend time and investigate with the email provider.

This paper will concentrate on the credit card frauds 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 the credit card number and the expiration 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, expiration date, the customer service number of the credit card issuer, and special codes on the physical card. The merchant then verifies with the credit card issuer for the correctness 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 (CPPS, n.d.) (VeriSign, n.d). 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, (PayPal, n.d.), (AntiFraud.com, n.d.), is designed for soft-product e-commerce.

2 PREVIOUS SOLUTIONS

Credit card fraud has been a problem since the beginning, and solutions for fraud detection have been continuously proposed:

The most widely used billing address verification system (AVS). (CCPS, n.d.), (VeriSign, n.d.)

A distributed data mining approach for credit card fraud detection (Chan, Fan, Prodromidis, et. al. Stolfo 1999)

Various types of neural network solutions were proposed for credit card fraud detection (Aleskerov, Freisleben, 1997), (Brause, Langsdorf, Hepp, 1999) (Ghosh, and Reilly, 1994), (Syeda, Zhang, Pan 2002)

A density-based clustering and radial basis function modeling to generate credit card fraud scores (Hanagandi, Dhar, Buescher 1996)

However, the credit card fraud in soft-products is an emerging problem. The old solutions that were used for hard-products may not be sufficient for the problem at hand. Various new ways of detecting and preventing credit card frauds have been proposed as well. Most of these solutions are vendor specific solutions and/or require major modifications on existing e-commerce sites.

As an example of solutions from IT vendors, Microsoft and other vendors, Orbiscom Inc. and Cyota, have come up with a credit card surrogate number that can be used for only one online transaction (Bruno n.d). American Express has a similar “proxy/filter” service that shields users’ credit card information from being exposed on the net. Visa has introduced “Verified by Visa” solution, and similarly, Master Cards and Discover have their own fraud prevention methods (Heun 2002).

The notion of trust in e-commerce is not new. Tradecraft, (Duvall 2001), has obtained a patent for its Internet Payments solution. Their 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 online third parties. This consortium of ISPs and/or vendors will act as the intermediary to facilitate Internet payment, somewhat similar to Visa International. Hsiung et al pointed out the importance of trust in e-Business growth (Hsiung, Sheurich, Ferrante 2001). Manchala (2000) developed trust models and metrics for e-commerce. Arif (2002) proposed establishing a trust service provider (TSP) that is somehow similar to the role of conventional banks that manage overseas trading via letter of credits. The TSP will act as an Internet-based intermediary and is responsible for verifying the commodity of the online merchant and the payment of the online customer.

Often, these solutions are not universal, meaning they are specific to certain credit cards (Visa, or American Express, but not both) or specific to certain vendors (e.g. Tradecraft). These solutions require customers to download some software (as in Master Card and Discover solutions) or require the bank and merchants to modify their system or checkout procedure (as in Verified by Visa). All these solutions cost money for merchants or banks to be compliant with, and require mass acceptance before they can be declared successful.

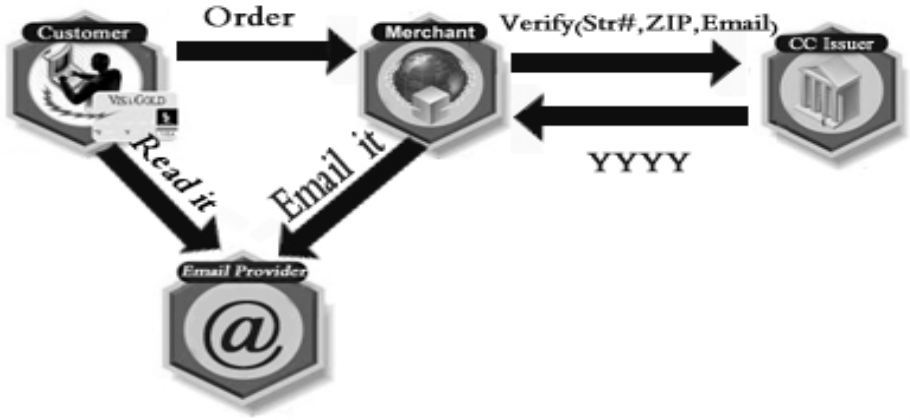

Figure 1: Proposed New AVS

3 TRUSTED EMAIL SOLUTION

All MTIO merchants of soft-products that require an email delivery are taking a risk by emailing the customer the purchased products (if the transaction is fraudulent). 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 compared to physical address tracking.

We propose a trusted email (TE) solution, which is a custom email server that can prevent online frauds for soft-products and investigate disputes efficiently, see Figure 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 will enable a more comprehensive address verification system, called full address verification system (FAVS), which will verify the email address of the customer on top of traditional AVS. The email address needs to be stored in the credit card issuer system in addition to the other information. 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 the order.

The solution of simply registering 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, it is 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 if 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, we propose to have a trusted email server (TES) to be used with soft-products e-commerce. The parities involved in the transaction (the stakeholders: shopping-customers, merchants, and credit card issuers) 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 that trusted email server if 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 Figure 2. This process can save the time of all the stakeholders and can protect the merchants from fraudulent transactions or unjust disputes.

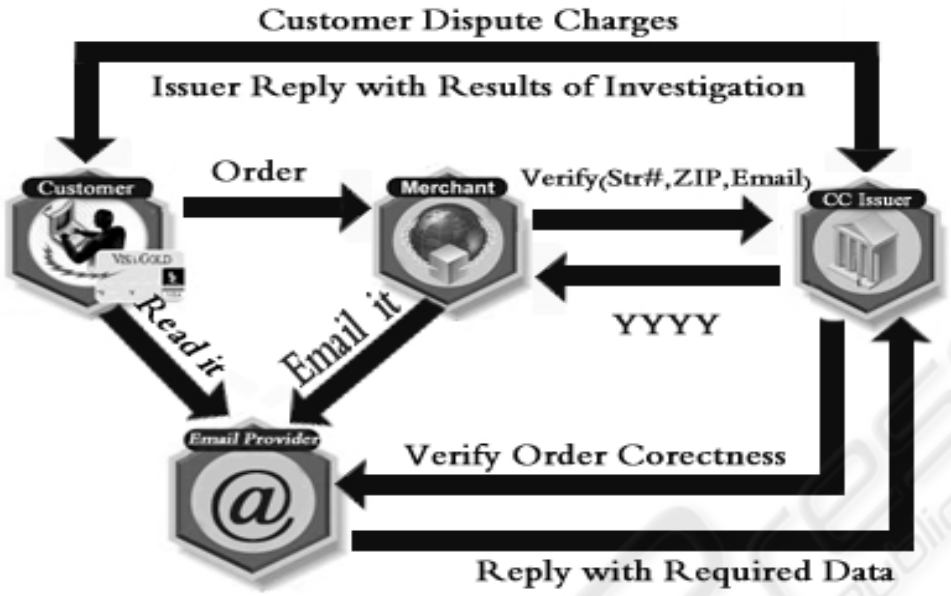

Figure 2: Disputes cycle in the new AVS

4 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). The details are explained below.

Credit Card Issuer: Each issuer will be granted access to the TES that enables them to use these services:

Checking a customer credit history before approving the credit application (since eventually, TES will contain payment and dispute history of its users).

Informing the customer of credit card approval and managing card activations through TES.

On going dispute management for online purchases. When there is a dispute regarding any card the issuer will access TES to investigate the dispute. Every issuer can only view the details of its customer accounts.

Setting the dispute period duration after the charge is billed in the statement, which is usually 3 months but some increase or decrease it.

Merchants: Each merchant will have to register for a merchant TE account to deliver any soft-product items to their customers. The TES has mainly two types of accounts: normal accounts for shopping customers, and special accounts for merchants and credit card issuers. One of the differences between the merchant account and normal accounts is that the merchant account has the capability to send to an unlimited number of customers, while the normal account can only receive emails and reply to the sender. 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 the FAVS will return N in the 4th field of the verification result.

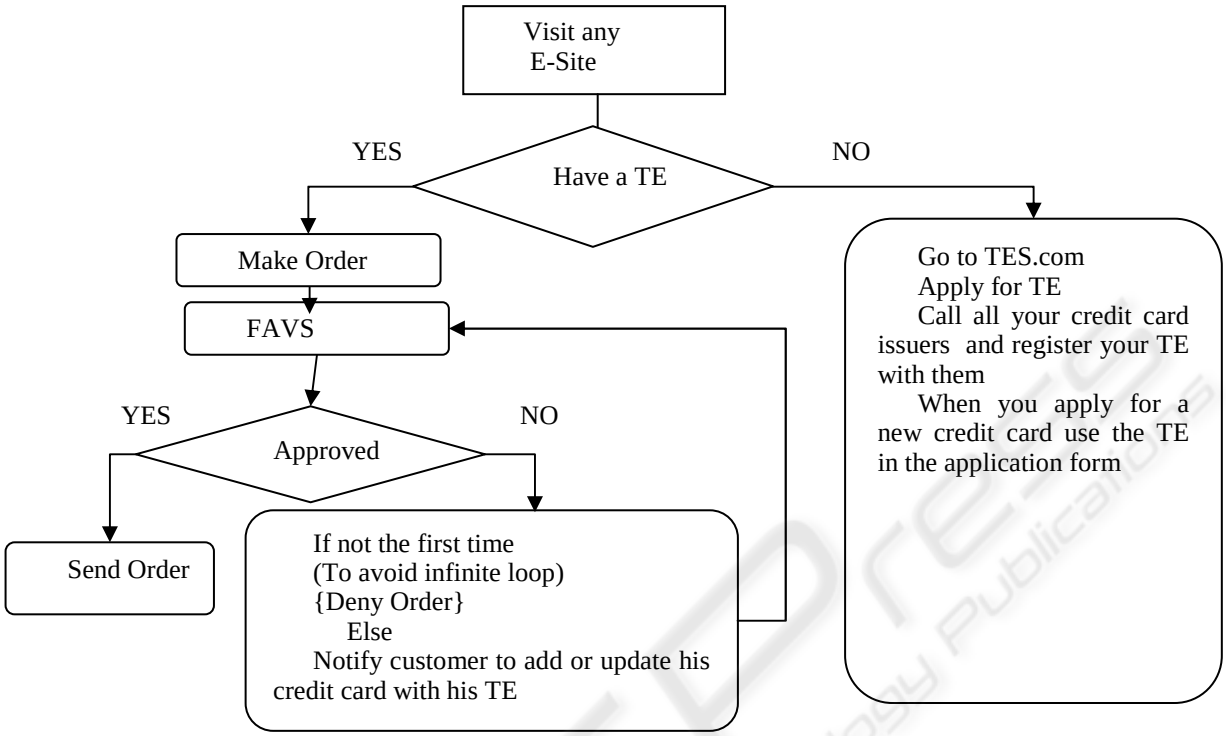

Figure 3: How Trusted Email Works

Customers: The customers will have to register with the TE and provide correct information, such as name, address, and telephone. If any of 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 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 the 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.

3- Encrypting the connection with a special email client: Trusted email clients will connect to the TES using encrypted communication. The client software differs based on the type of the 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.

Figure 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 (TE) he can proceed and place the order, which will be subject to full address verification (FAVS) including Trusted Email verification, in addition to the traditional AVS. 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.

5 DISCUSSION

We believe that our solution of using TE is a universal solution that precisely targeting the core problem of fraud purchases in soft-product e-commerce. Email has been already widespread and adopted by e-commerce stakeholders (customers, merchants, and credit card issuers). Therefore, using email as a starting point for our solution comes very natural. However, the success of this proposed solution depends on its technical soundness and its ability to meet the needs of the stakeholders that are affected by the new solution.

5.1 High-level Assessment

We will perform a high level assessment for the TE solution in light of the following aspects: technological, economic, social, and regulatory aspects (Lee; Yu; Ku 2001). Although the analysis performed by Lee et. al. 2001) was on payment systems and TE is not a payment system, nevertheless these aspects are applicable and are vital to the success of such solutions.

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 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. The TES special secure client-software 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. We will point out the main ones here:

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

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

Availability: TES shall 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 shall be simple and shall adhere to current existing e-

commerce technologies. As compatibility is a major factor that affects 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.

5.2 Making Winners of the Stakeholders

For a technology to succeed, the acceptance and adoption of the critical stakeholders are vital (Moore 1999). In TE solution, we want to make winners of the technology key stakeholders (Boehm and Ross 1989), (Boehm, Bose, Horowitz, Lee 1994). For TE solution, we analyze the needs and the win-conditions of all key stakeholders, namely credit card issuers, merchants, and shopping customers.

Each type of stakeholders has a different level of needs for using the TE solution. Some can realize more benefits than others. From analyzing one type of soft-product e-commerce sites, namely calling card sites, we reached to the following results:

Merchants: Calling card site merchants are the most eager to adopt TE solution, due to the hassle and inefficiency that they encounter using the current manual verification system, and due to the high loss if the transaction is fraudulent. With TE, calling card merchants can avoid the delay and effort of using manual verifications, and can eliminate the risk of approving fraudulent transactions that will later cause chargeback penalty.

Credit Issuers: It is to the advantage of the credit card issuers to use the TE system. They can eliminate the time spent to respond and investigate customer dispute claims. The dispute process often involves taking the claim from the customer, contacting the merchant's payment gateway provider for chargeback penalty, waiting for the gateway provider to get the merchant's explanation, replying back to the customer, and refunding the customer or declining the dispute.

The main advantage for credit card issuers in adopting TE solution is preventing credit card fraud in one of the most difficult to trace fraud types in e-commerce (soft-product, has-cost-non-traceable). This has a far impact, as it will boost the confidence of the online customers, and consequently promote the use of credit cards in e-commerce transactions.

Shopping Customers: It is of great convenience for the shopping customers to be able to purchase simple products such as calling cards online whenever they are needed without going to a local gas station or grocery store. However, currently one difficulty for the customers is that online calling card sites require manual approval that can take 24 hours or more to verify customer information (which the AVS cannot verify, such as phone number and email). Thus, it is to the advantage of the customers to use TE, which facilitates FAVS, in order to receive immediate approval for their purchase.

More important, with TE, unauthorized purchases of soft-products can be traced (if not prevented) which in turn relieves the customers from the problem of fraudulent transactions and dispute hassles.

6 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 proposed TE 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; in addition to several non-technical challenges as well, such as adoption and mass acceptance.

We believe that the proposed solution is far superior to any current system that uses billing address or other codes for verification. This solution is easier to implement than the credit card secret pin or surrogate credit card numbers. The solution has none of the common drawbacks of other proposed solutions, such as altering current e-commerce sites' checkout procedures (as in verified by Visa) or changing the systems of existing credit card numbers (as in surrogate numbers). The proposed solution also carries high incentives for current soft-product e-commerce stakeholders to adopt.

7 FUTURE WORK

This is an on going research and the details of the TES architecture and implementation are still in the design stage. Other future plans include:

Investigating the use of Web Services technology in the TE solution (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" (Postiva.com n.d.), (TRUSTe and ePrivacy Group, n.d.)

REFERENCES

Aleskerov, E., Freisleben, B., Rao, B. (1997) CARDWATCH: a neural network based database mining system for credit card fraud detection. Computational Intelligence for Financial Engineering (CIFEr), 1997., Proceedings of the IEEE/IAFE 1997 , 1997 Page(s): 220 –226

Alfuraih, Saleh, Sui, Nien T. Sui, McLeod, Dennis (2002). Using trusted Email to Prevent Credit Card Frauds in Multimedia Products, World Wide Web 5(2): 245-262

AntiFraud.com, Online Fraud Prevention Tips, (n.d.), Retrieved March 10, 2002, from http://www.antifraud.com/tips.htm

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

Boehm, B.W.; Ross, R. (1989), Theory-W software project management principles and examples, IEEE Transactions on Software Engineering, Volume: 15 Issue: 7, Jul 1989 Page(s): 902 –916

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

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

Bruno, Maria, (n.d) Microsoft Gives Boost to Surrogate Card Numbers. Bank Technology News, Retrieved March 10, 2002, from http://www.banktechnews.com/btn/articles/btnoct01-1.shtml

CCPS, Address Verification Service (n.d.), Retrieved March 10, 2002, from http://mcvisa.com/avs.html

Chan, P.K., Fan, W., Prodromidis, A.L., Stolfo, S.J (1999), Distributed data mining in credit card fraud detection. IEEE Intelligent Systems Volume: 14 Issue: 6 , Nov.-Dec. 1999 Page(s): 67 –74

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

Ghosh, S., Reilly, D.L.(1994) Credit card fraud detection with a neural-network. System Sciences, Proceedings of the Twenty-Seventh Hawaii International Conference on Information Systems: Decision Support and Knowledge-Based Systems, 1994 Vol.III Page(s): 621 –630

Hanagandi, V.; Dhar, A.; Buescher, K. (1996) Density-based clustering and radial basis function modeling to generate credit card fraud scores. Computational Intelligence for Financial Engineering, 1996., Proceedings of the IEEE/IAFE 1996 Conference on , 1996 Page(s): 247 -251

Heun, Christopher T. (2002), Fear of Fraud InformationWeek.com (March 4, 2002), Retrieved March 10, 2002, from http://www.informationweek.com/story/IWK20020301S0002

Hsiung, H. Sheurich, S. and Ferrante, F. (2001), Bridging E-Business and Added Trust: Keys to E-Business Growth, IT Professional, vol. 3, no. 2, Mar. 2001, pp. 41-45.

Lee, Zon-Yau, Yu, Hsiao-Cheng, Ku, Pei-Jen (2001), An analysis and comparison of different types of electronic payment systems, Management of Engineering and Technology, 2001. PICMET '01, Volume: Supplement, 2001, Page(s): 38 -45 vol.2

Manchala, D.W. (2000), E-Commerce Trust Metrics and Models, IEEE Internet Computing, vol. 4, no. 2, 2000, pp. 36-44.

Moore, Geoffrey A. (1999), Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers, HarperCollins Publishers, 1999

PayPal, Fraud Prevention Tips For Sellers, (n.d.), Retrieved March 10, 2002, from http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/fraud-tips-sellers-outside

Postiva.com Trusted Sender Program, (n.d.), Retrieved June 10, 2003, from http://www.postiva.com/article/articlestatic/17/1/5/

Syeda, M., Yan-Qing Zhang, Yi Pan, (2002) Parallel granular neural networks for fast credit card fraud detection, Fuzzy Systems, 2002. Proceedings of FUZZ-IEEE'02, Volume: 1, 2002 Page(s): 572 –577

TRUSTe and ePrivacy Group, Trusted Sender program, (n.d.), Retrieved June 10, 2003, from http://www.truste.org/programs/pub_trustedsender.html

Vantage Card Services, Inc, Prevent Chargebacks, (n.d) Retrieved Oct 1, 2003, from http://www.vantagecard.com/html/preventchargebacks.html

VeriSign, Address Verification Service (AVS) Security Feature, (n.d.), Retrieved March 10, 2002, from http://www.verisign.com/support/payflow/genResources/avs.html