The following paper was originally published in the
Proceedings of the Second USENIX Workshop on Electronic Commerce
Oakland, California, November 1996

Financial EDI Over the Internet: Case Study II

Arie Segev, Janna Porra, Malu Roldan
University of California, Berkeley

For more information about USENIX Association contact:

1. Phone: 510 528-8649
2. FAX: 510 548-5738
3. Email: office@usenix.org
4. WWW URL: http://www.usenix.org

Financial EDI Over the Internet, Case Study II: The Bank of America and Lawrence Livermore National Laboratory Pilot

Arie Segev, Jaana Porra, and Malu Roldan
segev@haas.berkeley.edu, porra@haas.berkeley.edu, roldan@haas.berkeley.edu
The Fisher Center for Information Technology & Management
Haas School of Business
University of California, Berkeley

Abstract

Bank of America Corporation (BofA) has used Electronic Data Interchange (EDI) to transmit financial transactions between itself and its customers for years. Until recently, however, BofA has used direct private lines or third party value added networks (VANs) as the carrier of the EDI data. In 1994, BofA initiated a pilot project with its customer Lawrence Livermore National Laboratory (LLNL) to investigate whether the Internet could be used for secure, reliable, and fast financial EDI (FEDI) transactions. This follow up study is the second case study on BofA's EDI strategy conducted by the Fisher Center for Information Technology and Management at the University of California, Berkeley. The first case study was completed in August 1995 (Segev, et.al., 1995). In the first case study, the current practices in EDI, FEDI, and related technologies were reviewed and documented. In this second case study, the results of the pilot project, which ended June 30th, 1996, are presented and possible implications are discussed. According to the results, the Internet is a viable alternative carrier for critical or sensitive business transactions. It is suggested that the transition from the traditional EDI to EDI over the Internet has strategic implications.

1. Introduction

Electronic Data Interchange or EDI is a synonym for standardized inter-organizational data exchange (Kalakota, et.al., 1996). It has been used for more than 20 years in automating the interchange of business transactions between trading partners, suppliers, and customers in order to create a paperless flow of administrative, prepurchasing, purchasing, shipping, receiving, warehouse, customs, billing and payment information (Sokol, 1995). Forrester Research has estimated that today 120,000 of 2 million companies are EDI capable (Smith Bers, 1996). This means that only 5 percent of the companies that could be using EDI are actually doing so. For large corporations, who provide EDI based services, this means that 95 percent of the market is still to be harnessed.

Bank of America Corporation (BofA) has used Electronic Data Interchange (EDI) to transmit financial transactions between itself and its customers for years. Until recently, however, BofA has used direct private lines or third party value added networks (VANs) as the carrier of the EDI data. In 1994, BofA initiated a pilot project with its customer Lawrence Livermore National Laboratory (LLNL) to investigate whether the Internet could be used for secure, reliable, and fast financial EDI (FEDI) transactions. This follow up study is the second case study on BofA's EDI strategy conducted by the Fisher Center for Information Technology and Management at the University of California, Berkeley. The first case study was completed in August 1995 (Segev, et.al., 1995). In the first case study, the current practices in EDI, FEDI, and related technologies were reviewed and documented. In this second case study, the results of the pilot project, which ended June 30th, 1996, are presented and possible implications are discussed. According to the results, the Internet is a viable alternative carrier for critical or sensitive business transactions. It is suggested that the transition from the traditional EDI to EDI over the Internet has strategic implications.

2. EDI

Electronic Data Interchange (EDI) refers to business-to-business exchange of data (Sokol, 1995). It requires evaluating strategic and operational issues such as EDI related organizational change, service and development responsibilities, development of EDI based services, and their marketing. In the widest sense, EDI refers to all policies, procedures, and technologies related to the exchange of EDI information between two corporations. Defined this way, EDI includes the processes of procurement (handling of requests for quotes, price quotes, purchase orders, acknowledgments and invoices). This means that implementing EDI requires not only developing or purchasing the EDI software and hardware,

but also organizational change through Business Process Reengineering (BPR).

An EDI relationship starts with an agreement between a company and its trading partner (Segev, et.al., 1995). The agreement consists of technical decisions concerning the EDI standard, types of information exchanged (e.g., purchase orders, payments, etc.), and the exact format of each message exchanged. Other important decisions concern both technical and business aspects of the EDI relationship. These include agreements about the interbusiness procedures related to EDI such as why and when messages are sent; how are messages responded to; and what are the procedures for handling exceptions.

In addition to the format and procedural EDI decisions, an EDI relationship requires agreements on the degree of automation at both ends of the relationship. One of the main purposes for using EDI is the reduction in manual processing of paper based transactions. Reducing manual, paper based processing, in turn, leads to cost reduction and faster service to the customers. This means that the benefits of EDI are directly related to the degree of automation.

The higher the number of the human interventions, the more time and paper the process requires. Processing paper by humans is more costly and time consuming than using automated processes. Reduced processing speed, in turn, translates to lower quality customer service. Interorganizational EDI thus may be thought of as an interorganizational, fully automated assembly line (Figure 1).

Since EDI refers to a standard not to a business process, it is often presented not as an interorganizational information system, but in a purely technical way. In essence, EDI defines the *standard* format for exchanged *messages*. In this context, a *message* refers to a document such as a purchase order, an invoice, a payment, or any other formatted business-to-business, administrative, purchase, or sales transaction. *Standard* refers to one of the several international (e.g., EDIFACT), national (e.g., ASC X12 in the United States), or industry wide (e.g., National Wholesale Druggists Association (NWDA); and Uniform Communications Council (UCC)) agreements which define the data items on the EDI message (the number, type, order, and precise format for the fields of the document). Today, EDI standards initiatives take place at several fronts (Sokol, 1995).

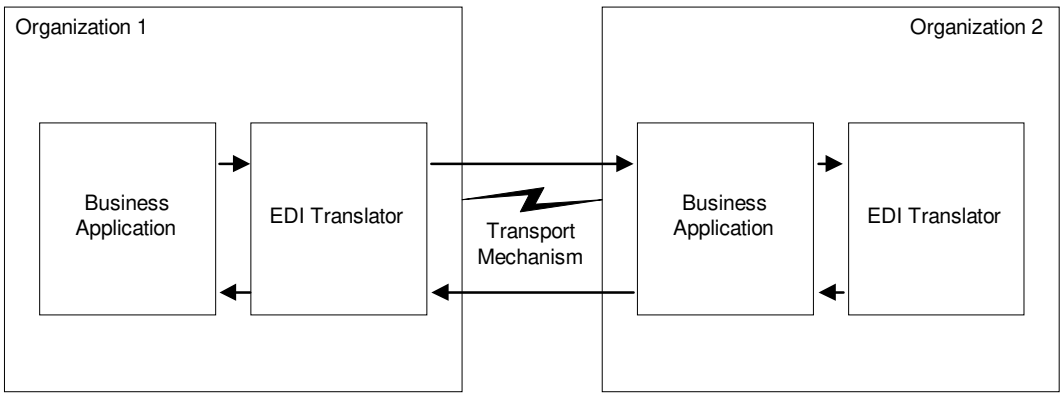


Figure 1. Automated Interorganizational Data Flow with EDI.

Today, it is possible to choose from a variety of EDI standards such as the ones mentioned above. Moreover, inside each standard, it is often possible to choose between several profiles (characteristics added by selected optional features of the standard). The purpose of standardization is to reach a general agreement on which current and future EDI users will commit to. A single standard, with no optional aspects, would guarantee that any two corporations were able to exchange EDI messages without negotiation. Many EDI standards, each with several options, create an array of possible formats for an EDI transaction. The advantage of using a standard, is in the predefined public agreement concerning the transaction format. The downside of the current EDI standardization situation is the number of possible standards and options which may make using an EDI standard unattractive. Luckily, the situation is not as serious as it may seem. Of the EDI standards, the two most likely candidates for a wide acceptance, are the ASC X12 in the United States, and EDIFACT internationally. Thus, using either of the two will increase the likelihood for successful EDI relationships at home and abroad.

In the past, the initial cost of integrating EDI into the corporate information system has been one of the main issues preventing EDI's success. Traditionally, these EDI implementation costs have included the cost of purchasing or developing the EDI translator, the cost of integrating the EDI translator with the corporate information system, and the cost of establishing a transport mechanism (often provided by a telecommunications carrier). The first two cost categories consist of purchasing the hardware, software, and programming skills. Choosing the transport mechanism includes choosing between private networks, Value Added Network providers (VANs), and more recently, the Internet. Supporting the production system has been another, sometimes initially overlooked, contributor to the high cost of EDI. Once the software is designed and implemented, the cost of handling paper based transactions is reduced. What sometimes escapes the corporate cost benefit analysts, is the fact that the paper processing cost is partially replaced by the increased need for maintaining and operating the computer based EDI service.

3. FEDI and FEDI over the Internet

Bank of America Corporation (BofA) is one of the largest banking companies in the United States with assets of more than $227 billion (Segev, et.al., 1995). As a diversified global financial services institution, BofA provides banking products and services to individuals, businesses, government agencies, and other financial institutions in the United States, and in 36 other countries. Today, BofA supports all major electronic payment options, including FedWire funds transfer service; automated clearinghouse transfers or ACH; Clearinghouse Interbank Payments System or CHIPS service; and Society for Worldwide Interbank Financial Telecommunications or SWIFT funds transfer service. These transactions do not use EDI or FEDI. Rather, FEDI comprises the electronic transmission of payment and remittance instructions and acknowledgements between a payer, payee, and their respective banks (Figure 2). The BofA pilot project concentrates on FEDI between BofA and its customer, LLNL. Like most all other corporations engaged in EDI (Messmer, 1996), BofA has been using either direct private lines or third party vendors called value added network service providers (VANs) as the EDI network carrier. The objective of the BofA pilot was to evaluate the Internet as an alternative.

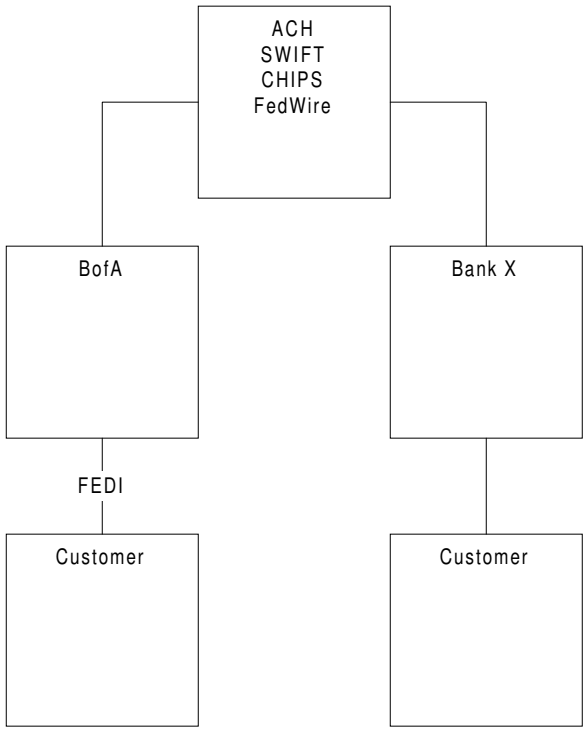


Figure 2. Financial transactions and FEDI.

In the case of BofA, the purpose of FEDI based customer service is to offer a set of the most widely used EDI standards to customers, rather than to advocate a single EDI standard. Another goal for the FEDI based customer service, is to integrate the EDI based solution with BofA's information systems without requiring comprehensive automation on the customer's part. The same desire to meet the customer's needs is apparent in BofA's response to the transport mechanism options. BofA will offer multiple transport mechanisms to serve a variety of customer needs. The case at BofA shows that EDI is rapidly overcoming several of its limitations. Today's flexible and cost effective EDI solutions can be used between large corporations, and increasingly in business transactions with small enterprises. Large corporations, such as BofA, are thinking ahead for their customers when selecting EDI solutions that alleviate the problems of incompatibility by offering multiple access methods.

The two main reasons for considering the Internet for FEDI transactions at BofA, are cost savings and new market potential. Both private lines and VANs charge based on the transaction volume while the Internet providers charge a flat fee (Jetter, in Smith Bers, 1996). Particularly, with high transaction volumes, the start up costs, fixed costs, and usage costs of the Internet are significantly lower than those of private networks or

VANs (Segev, et.al., 1995). The other main reason for considering the Internet as the FEDI transaction carrier is derived from two market segments: (1) the 95% potential, consisting of large EDI capable corporations which are not currently using EDI; and (2) the fast growing number of Internet users, who are mainly small businesses and individuals. Today, it is estimated that the Internet consists of more than 30 million computers world wide. The latest easy to use multimedia interface to the services of the Internet functionality, the World Wide Web (WWW), is said to be doubling in the number of users every 53 days (Pant, et.al., 1996). Even when measured merely by its size, the Internet and the WWW provide a compelling case for new business strategies. The modern Internet, and particularly the WWW, are the center of electronic commerce of which EDI is an integral part. A third, often overlooked reason to consider the Internet for EDI and FEDI transactions is that the Internet is already used in most organizations. Using Internet based electronic mail as the messaging system draws from familiar and available resources.

4. Internet Related Concerns – Security, Reliability and Speed

The Internet security concern has been supported by widely publicized compromises of Internet security (Bhimani, 1996). Over the decades, reports of actual Internet security problems have been confused with reports of security problems which were not caused by the Internet, but the computer systems attached to it (Hutt, et.al., 1995). The lack of real world examples of consistently delivering critical transactions over the Internet, keeps many corporations as spectators in the Internet explosion. However, the situation is rapidly changing as better technologies are being developed, and web-based transaction systems are becoming a high priority initiative for corporations in shipping, banking, airline, and retail industries.

Two other central concerns, (1) reliability, and (2) speed of transactions over the Internet, are founded on the original design principles of the Internet network. There is no centralized management and no centralized routing of the transactions. Instead, the management of the Internet, and the routing of the messages, are distributed. This means that no one organization or instance is responsible for carrying the transaction from the sending computer to the receiving computer. Moreover, the routing of a message is dynamic. There is no way of predicting or controlling the route the data will take from the transmitting computer to the destination. Corporate network service users are accustomed to a third party, who guarantees a level of service, and reliable, fast delivery. A common perception is that the Internet architecture has proven to be adequate in advertising and communications which are the two main business uses of the Internet today (Stipe, 1996). However, the concerns about lost data and prolonged transmission times will require addressing in the corporate transaction setting. Today's commercial Internet, and particularly the WWW, have corporations as users. In a corporate environment, the fastest transaction processing systems are based on executing real time transactions (the message is sent from the sending application to the receiving application at the moment of initiation of the transaction). Security, reliability, and speed are now being measured according to the corporate standards comparable to those used in private networks and by third party VANs.

5. The FEDI Pilot

The previous sections provided a general overview of EDI and FEDI, the Internet, their organizational impacts, and BofA's use of EDI. This section describes the parameters and operational results of the FEDI pilot project between BofA and LLNL. Section five presents conclusions and an examination of the above issues in the context of the pilot.

As discussed above, the Internet presents a seemingly attractive alternative to BofANet and VANS. It is widely available and reputably inexpensive when compared to VANs. Since the bank already has an Internet connection for other applications, e.g. electronic mail, the incremental cost required to carry EDI traffic over the Internet is mimimal. The bank views the flat-fee, volume-independent and time-of-day independent pricing structure of the Internet as one major benefit over other types of networks, like VANs. Because of the large volume of transactions, the bank expects to achieve tangible savings, over the long term, by either redirecting EDI traffic from other channels, generating new customers from current Internet users, or both.

Thus, in late 1994, individuals at BofA were searching for a client partner to start a FEDI pilot project. Because of general concerns over Internet security, particularly for transmissions involving financial transactions, BofA expected that it would have a difficult time finding a willing partner. At about the same time, individuals at LLNL became interested in building the capability for FEDI over the Internet, as part of a planned overhaul of its accounts payable system. At LLNL, this was seen as a next step in its continuing leadership with innovation in the practice of EDI. Quite fortuitously, representatives

from both organizations made contact at several CommerceNet and Special Interest Group meetings in the Bay area, and decided to pursue a possible pilot for conducting FEDI over the Internet.

After high level talks, both organizations decided on a limited pilot, requiring minimal investment from the parties involved. The pilot involved participation from several departments at both organizations – most strongly from BofA's Global Payments Services and Interactive Banking groups, and LLNL's Accounts Payable and Electronic Commerce departments. The key objective of the pilot was to demonstrate that it was possible to achieve secure and reliable transmission of sensitive data like payment instructions over the Internet. The pilot was meant to dispel negative perceptions of the Internet held by the general public and the business community. The pilot would be especially valuable in addressing the concerns in the Banking Industry over sending critical financial data over the distributed public networks of the Internet. As discussed above, these perceptions centered primarily on two concerns: security -- that transactions over the Internet were easily intercepted and tampered with, and reliability and speed -- that transactions tended to get lost and/or delayed as they were passed from node to node over the Internet.

5.1. Chronology of the Pilot

The FEDI pilot included two phases. The first phase limited the exposure of both LLNL and BofA to the risk of financial loses due to compromised payment instructions. Success with this limited test led to the relaxation of the limits during the second phase of the pilot. The second phase also included volume testing to simulate any problems that might result from a full-scale implementation. All throughout the seven months of the pilot, BofA project participants were also involved in designing a full-production platform to support FEDI and similar applications.

FEDI pilot participants from LLNL and BofA spent most of the first half of 1995 designing, coding and testing the FEDI system. At BofA, the pilot required development of a gateway system for encrypting and decrypting EDI documents that it would transmit to its existing EDI and ACH systems (running on its ECS server). This gateway was located inside the bank's firewall. Part of an existing Unix machine on that platform was allocated to the project. The main software development work involved installing PEM/MIME on this Unix machine and automating the file handoffs between various BofA systems. At LLNL, the pilot was part of an effort to improve the accounts payable system. Since the Lab already had an existing PEM/MIME server and EDI translators, the main development work involved automating the handoffs between various LLNL systems and creating reports used to monitor the progress of transactions throughout the system. Additionally, during the testing phase, LLNL's implementation of a new version of their A/P database necessitated further development work to make the translators and handoffs work with the new database.

In August 1995, the first payments instructions were successfully sent from LLNL to BofA, resulting in payments to selected vendors. This started the first phase of the pilot project. To minimize risks, the pilot was limited to five vendors and a cap of $10,000 was established for payments to a single vendor per day. The process included vigilant monitoring by key pilot representatives of both organizations. E-mail messages were used to track the progress of FEDI documents through the system. Any anomalies were quickly identified and resolved. The key pilot representatives were in touch with each other via phone and beeper systems. Weekly meetings were used to track progress with resolving recurring problems. Because of this vigilance, all payments were made within the contract time frame – that is, all payments were received by each vendor's bank within two days of the generation of payment instructions from LLNL.

The first seven months of the pilot convinced both organizations of the viability of sending payment instructions over the Internet using a PEM/MIME-based security system. Measures of security, reliability, and speed -- described in section 4.4 -- provided a measure of confidence that the instructions were not lost in the Internet or tampered with. Both organizations were, at that point, ready to step up their levels of exposure. LLNL added new vendors to the system and increased the cap on payments to $100,000 for each vendor per day. Additionally, LLNL started a program to use the same process to provide Travel and Entertainment reimbursements to their employees. As of July 1996, LLNL had approximately 12 vendors on the system and about 100 employees signed up to receive Travel and Entertainment reimbursements using the FEDI system. Lastly, to test the robustness of the system to full implementation, the two organizations conducted volume testing. This involved tracking the time it took to process transmissions that contained up to 1000 payment instructions. The results of these tests are reported in section 4.5.

Even as they were going through the pilot, the BofA project group knew that they needed to design a production system to eventually replace the pilot system. They anticipated that the current system would be impractical for meeting the demand for supporting secure transactions over the Internet -- particularly if the pilot proved successful and the numerous parties interested in the pilot signed up for the service. Through discussions among representatives of the bank's security, marketing and information systems areas, as well as with key hardware vendors, the project group designed both an interim system and a full production system. At the same time, as interest in the FEDI project and the Internet grew outside and within the bank, senior management started to become amenable to possibly investing in better FEDI platforms. The project group obtained funding for an interim production system and as of July 1996, were waiting to hear if the full production system would be funded.

BofA has obtained the hardware and software to move their FEDI operations to an interim platform. This was the first step in moving the FEDI platform from a research to a production environment. The interim system involves software and hardware improvements. The new platform uses Trusted Information Systems' (TIS) MOSS software instead of PEM/MIME. MOSS – MIME Object Security Services is a proposed standard that extends PEM capabilities by supporting e-mail messages with arbitrary contents (including video, voice, images), improving functionality and expanding trust and naming rules. The hardware configuration of BofA's interim system involves three Unix workstations. Two of the workstations will be running MOSS in parallel and will be located in the bank's production environment in San Francisco. The third workstation will be used for development purposes and will stay in the Concord facility. BofA plans to add other EDI packages (e.g. Premenos' Templar) as new customers request them. The proposed production system currently under review at BofA, brings security to a higher level by not only using software but also hardware to achieve it. Aside from being more secure, a hardware-based system also speeds up encryption and decryption processes. The key to the final system is a hardware level security server. This server will make sure that no sensitive data -- e.g. payment instructions -- is ever visible as clear text during transport over the Internet or participating organizations' internal networks.

5.2. The Pilot System

The following description is organized around three aspects of the pilot system – the exchange of documents, the achievement of security, and the monitoring of system performance. All three are key to making the case for the viability of FEDI over the Internet. In general, the system involved the exchange of EDI documents containing payment instructions and acknowledgements. To achieve security, the documents were processed through servers running PEM/MIME at entry into and exit from each organization's existing network of EDI systems. A system of e-mail and human monitoring tracked messages through the system – insuring that payments were completed accurately, and collecting data to assess system performance.

FEDI Document Exchange. The process starts when LLNL extracts a batch of payment instructions (EDI document 820) from its Accounts Payable database. After extraction, LLNL's PEM server processes the batch of 820s according to the security measures described below. LLNL then transmits the secured batch of 820s to BofA via the Internet. Upon receipt of the LLNL message, BofA's PEM server processes the batch to confirm its authenticity and decrypt its message. The clear text message, containing a batch of 820s, is then transmitted through a dedicated line to BofA's EDI server (ECS). BofA's ECS server then confirms that the data was received, that it is in the right format, and contains the correct information. The ECS server then sends back a functional acknowledgment (EDI document 997) to the BofA PEM server for security processing. The PEM server, in turn, transmits the secured 997 over the Internet. Upon receiving the message, LLNL's PEM server authenticates and decrypts this 997. It then matches up the information in this 997 with its record of the information contained in the original 820 document that it sent to BofA.

Meanwhile, BofA's ECS server completes processing of the batch of 820 documents, sending payment instructions to a payments server – e.g. ACH for electronic funds transfer, or a check processing system. After handing off the instructions to a payments server, the ECS system sends an Application Advice (EDI document 824), back to BofA's PEM server. The 824, containing information on payment acceptances and rejections, is secured and transmitted to LLNL over the Internet. LLNL authenticates and decrypts the message then matches it up with the information set out in the original payment instructions (820) and with BofA's acknowledgment (997). If all the information matches up, LLNL sends a

secured 997 functional acknowledgment to BofA through the Internet. On average, if problem-free, this whole process takes 11 minutes (Average of logged time for problem-free transmissions computed from BofA's Daily Tracking Log, July 12, 1996).

The agreement between LLNL and BofA requires that a vendor bank receive payment within 2 days of LLNL sending an 820 to BofA. Since the entire FEDI transaction takes only an average of 11 minutes, both organizations have ample time to research and resolve any problems related to the transmission of a given payment between BofA and LLNL. Problems could also occur if the vendor's bank rejects a payment request for a variety of reasons – e.g. insufficient funds, vendor has changed banks. Should a vendor's bank eventually reject a payment instruction, BofA receives a financial return notice from the vendor bank (EDI document 827). As with the other documents, this 827 is secured by BofA's PEM server and sent to LLNL over the Internet. Personnel at LLNL's Accounts Payable department then conduct the research to determine why the payment instruction was rejected then take the necessary steps to resolve the problem.

Security Measures. A system of multiple acknowledgements, information matching at LLNL's EDI server, and encryption and signing of all e-mail transmissions containing EDI documents formed the basis for addressing the minimum security requirements discussed in section 3.2 – confidentiality, authentication, data integrity, nonrepudiation, and selective application of services (Bhimani, 1996; IETF-EDI Working Group, 1993). Confidentiality was achieved using encryption, while a system of digital signatures, encryption and one-way hash functions helped achieve authentication, data integrity and nonrepudiation. Lastly, selective application of services was achieved by transmitting any clear text only through dedicated network lines. Any text that went through shared networks like the Internet was encrypted and digitally signed as PEM/MIME documents.

At the start of the pilot, the two organizations had to exchange public keys to be used in RSA encryption and decryption procedures. Ideally, a third party, called a Certifying Authority, would vouch for the authenticity of these public keys. Since the two parties had an ongoing relationship based on trust, and due to the lack of Certifying Authorities, the two organizations essentially certified themselves as bound by their respective public keys. Both LLNL and BofA also had to agree upon the algorithms to be used for security procedures. For the purpose of the pilot, the algorithms were part of the PEM/MIME software acquired from TIS – RSA's PK1 for asymmetric public key encryption, DES for symmetric encryption, and RSA's MD5 for the calculation of one-way hash values. Additionally, the pilot participants had to agree on appropriate lengths for the encryption keys. As with any other encryption process, an important determinant of the strength of the security associated with this standard depends on the length of these keys.

In essence, the security procedures consisted of three major steps. The first step was used to insure the confidentiality of the EDI document through encryption. Encryption makes it difficult for unauthorized individuals to read the document while it is in transit to the receiver's system. The second step, use of a one-way hash procedure, insures the integrity of the document contents. Using an agreed upon algorithm, the sender calculates a hash value for the EDI document and sends it to the receiver in encrypted form. Using the same algorithm, the receiver can calculate a hash value for the EDI document it receives. If the hash values match, the receiver can have some level of assurance that the document was not tampered with. In the last step, the sending organization guarantees its identity by sending a digital signature. The digital signature consists of the one-way hash value encrypted by the sender's private key. The receiver can then use the sender's public key to decrypt this hash value and match it to the hash value it calculates.

The security procedures apply every time an EDI document comes to a PEM server– e.g. when an 820 is sent by LLNL Accounts Payable system to LLNL's PEM server or when BofA's ECS server sends an 824 to BofA's PEM server. The sender's PEM server first calculates a one-way hash value for the document using the MD5 algorithm. It then generates a symmetric key and uses the DES algorithm to encrypt the EDI document. Next, it encrypts the symmetric key with the receiver's public key, and encrypts the one-way hash value with the sender's private key. The EDI document, symmetric key, and one-way hash value – all in encrypted form -- are then bundled in a MIME envelope and sent over the Internet to the receiver's PEM server. Upon receipt of the message, the receiving organization's PEM server first authenticates the sender's identity by decrypting the one-way hash value using the sender's public key. It then decrypts the symmetric key using the receiver's private key. Next, the decrypted symmetric key is used to decrypt the EDI document. This document is then sent on to the receiver's EDI server for processing.

The PEM/MIME security procedures were set up to meet minimum security requirements, at high speed, and with simple key management. They involve a combination of

symmetric key encryption (DES) and asymmetric public-key encryption (RSA). This system speeds up the encryption/decryption process as well as simplifies key management. Under this system, the faster DES algorithm is used to encrypt relatively large documents like the FEDI documents. The key used for the DES encryption, a relatively smaller document, is then encrypted using the sending organization's private key. Key management is simplified so that the two parties need to exchange only their public keys. There is no need to exchange symmetric DES keys since a new, random DES symmetric key is generated for each transmission. This symmetric key is encrypted with the receiver's public key and sent along with the PEM/MIME message. An additional benefit of this system is that the DES keys are linked to only one EDI transmission at a time. An individual who could figure out a given DES key could only pose a threat to that one transmission. In contrast, if the two organizations used the convention of agreeing on a single DES key to be used for a range of transmissions, any individual who could figure out this agreed upon DES key could potentially decrypt a large number of transmissions (IETF-EDI Working Group, 1993.).

Monitoring the System. The pilot system required multiple confirmations of the information transmitted at key steps in the process (using 997 EDI documents). This system of acknowledgements provided one method of establishing the reliability and security of the process. Additionally, key contacts at each organization monitored each phase of the process and would telephone his/her counterpart if an error or omission occurred in the process. BofA summarized the movement of each and every transmission between BofA and LLNL through this process for the seven month duration of the pilot in a Daily Tracking Log (July 12, 1996). At each point where a time reading is taken, an email message is generated by the LLNL EDI server and sent to key personnel at BofA and LLNL. In this way, several individuals kept vigilant watch over every transaction and were able to quickly determine and react to any errors or delays.

Security of the network was monitored using standard procedures at both organizations. The groups managing the firewalls of each organization conducted their own tests and monitoring procedures to keep track of both legal and illegal access attempts to each organization's network. These procedures were part of the general network security protocols at each organization and were not done especially for the FEDI project. None of the informants reported on the use of procedures to trace the transit of message packets through the Internet.

Based on the data from BofA's daily tracking log, we generated a summary of the problems encountered throughout the pilot (Table A). As the table shows, almost 50% of the problems stemmed from systems going down or off-line. This figure reflects the difficulty of coordinating the separately managed systems that were all part of the FEDI pilot process. This condition was magnified because BofA's PEM server was part of the firewall operation that resides in an R&D location – as opposed to a financial production environment. Thus, BofA's PEM server was at times accessible to individuals who were unaware of the impact on the FEDI pilot of any processes they might run on the PEM server. Furthermore, both BofA and LLNL went through several software problems and upgrades over the course of the pilot – resulting in further problems with compatibilities between the systems in the network. Much of the early work done by the project team involved solving these incompatibilities and instituting procedures to coordinate all the different systems involved in the pilot process. Table A shows how most of these problems were resolved by January 1996. It should be noted though that despite these problems, all payments were completed within agreed upon timeframes – 2 days from the time that LLNL sent a payment instruction to BofA.

Aside from tracking problems, both BofA and LLNL monitored the performance of the FEDI process with the use of a variety of measures. These measures may be grouped according to the top concerns related to FEDI over the Internet– security, reliability and speed.

Security. Security measures were used to determine that there were no attempts to access the network or tamper with messages sent between the two organizations. These measures included attempts to break into the system as well as a system of cross-checks and acknowledgements to insure that the data received at one end of a transaction, matched the data sent from the other end. Security measures included the following:

- LLNL had their internal security group run a "white hat" test of the LLNL FEDI network. The network did well and got even better with the implementation of recommendations of the "white hat" team. Additionally, LLNL staff checked the pattern of log-ins to their FEDI system periodically to check for patterns that would suggest security breaches – none were observed.

Table A. Problem Summary BofA/LLNL FEDI Pilot (Based on BofA's daily tracking log)

Type of Error	Aug. 1995	Sept. 1995	Oct. 1995	Nov. 1995	Dec. 1995	Jan. 1996	Feb. 1996	Mar. 1996	% of total problems
Applications, Operating System incompatibilities	2	1			4				17%
Systems going down or off-line	7		6	1	2	1	2	1	49%
Document delivery problems (duplicate, delayed, or lost documents)		1	3	3	2		1		24%
Message problems (truncation)			2						5%
Decryption problems						1	1		5%
A. Total # of Problems for the month	9	2	11	4	8	2	4	1	
B. Total # of EDI transmissions for the month	19	21	22	22	21	23	21	21	
Error Rate for the month = A/B	47%	10%	50%	18%	38%	9%	19%	5%	

- Dollar amounts, payee information, transaction numbers and EDI formats were checked and matched using the series of EDI documents (820-997-824-997-827) described in section 4.0. All of the mismatches generated by this system were explained with reasons other than security breaches. Additionally, as noted above none of these problems resulted in payments sent beyond agreed upon timeframes.

- The group in charge of BofA's firewall tracked all access attempts to the firewall. Additionally, a member of the project team tried, unsuccessfully, to break into the system by sending an unauthorized file to the ECS system. BofA also contracted with an outside vendor to conduct a test of the firewall's penetrability.

Reliability. Reliability measures were used to insure that the data sent by one organization matched the data received by the other. Again these measures were taken as part of the series of cross-checks and acknowledgements sent between BofA and LLNL.

- The LLNL EDI server matched up information on the 820, 997, and 824 and generated error messages whenever it detected a mismatch.

- LLNL personnel checked a daily EDI Batch Control report to insure that the batch total sent was equal to the total acknowledged by the bank.

- A monthly bank reconciliation report used to make sure all payments matched payment instructions sent.

Speed. Speed measures tracked how long it took to transmit and process the series of EDI documents between the two organizations. The speed of transmission and processing measures were key to addressing the concern that because of the Internet's decentralized and dynamic routing, messages tend to get lost and delayed. The reliability measures included the following:

- The pilot project team tracked how much time it took a transmission to complete the entire FEDI document exchange process described in section 4.3. This time was tracked by noting the amount of time it took for a transmission to reach seven points in the process. At each of these seven points, e-mail messages were sent to key BofA and LLNL personnel to indicate when EDI documents reached key parts of the process. This data were used to track where a problem occurred when a transaction did not go through properly. This data were also used to calculate the time it took for transactions to complete the loop (from the time LLNL sends the 820 to the time it sends the 997 -- after it first receives a 997 and an 824 from BofA. This data was tracked throughout the pilot and during volume testing.

5.3. Operational Results of the pilot

Security. In the assessment of participants from both BofA and LLNL, the results of the pilot provided support for the viability of the secure and timely transmission of sensitive information over the Internet. Most of this support comes from the finding that none of the problems with payment transmissions were due to any breach of the network or tampering with the messages being transmitted. As shown in Table A, most of the problems encountered during the pilot were due to non-recurring software and procedural issues that were resolved. Problems stemming from the situation where BofA's PEM server was a shared, non-production machine are expected to be alleviated when the process moves to the dedicated interim system in the next few months.

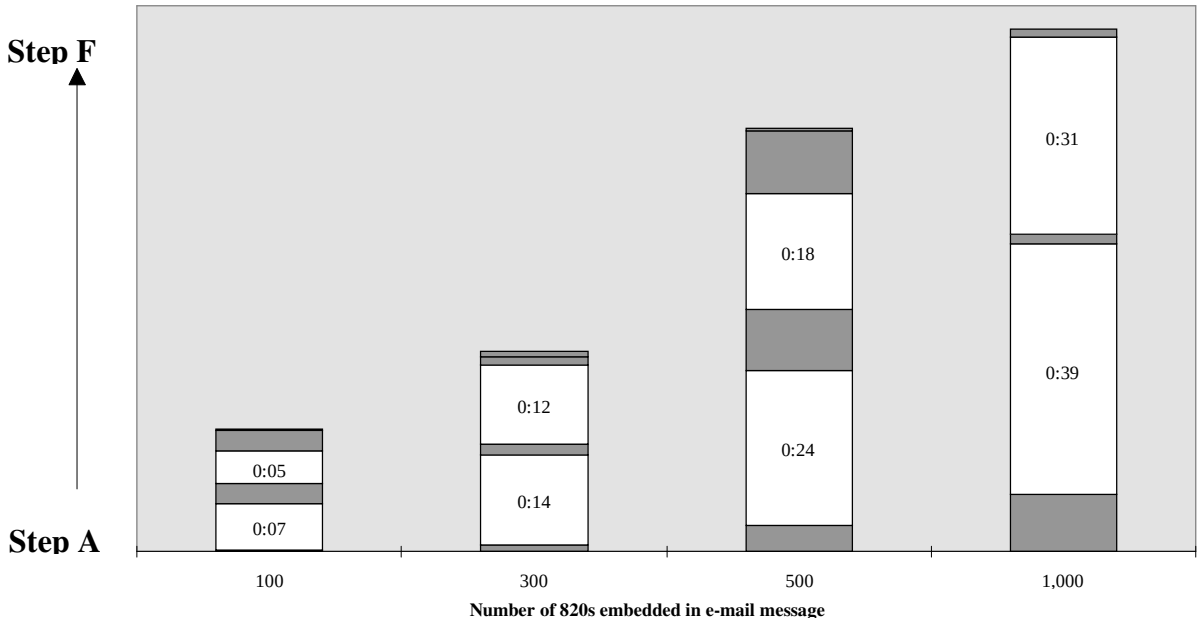
Reliability. The most striking finding regarding the reliability of the Internet for FEDI transmission is that none of the messages were lost in transit between BofA and LLNL. The reliability measures also showed that, despite delays and problems, information on payment instructions, acknowledgements, and payments remained consistent. As shown in Table A, there were only two occasions out of 170 transmissions (October 1995) when the EDI document received by the bank did not match that sent by LLNL (duplicate header on 10/2 and message truncated on 10/30). In all the rest of the transmissions, no mismatches were reported by the LLNL server among the FEDI documents sent between BofA and LLNL. This suggests to the participants that, given the security measures used and despite its decentralized nature, the Internet has the capability to accurately transmit critical data like payment instructions.

Speed. The results of volume testing showed that as the number of payment instructions contained in a message increased, processing time increased (Table B). The total processing time ranged from 11 minutes for messages containing zero to five instructions, to 58 minutes for those containing 1000 instructions. However, this increase can be attributed to the increased time required to processes the instructions and not to increases in the time required for transmission of the email message over the Internet. BofA's daily tracking log (July 12, 1996) and Volume Testing log (July 10, 1996) provided the raw data for the findings summarized in Table B. These data were also summarized to delineate time spent on transmission versus time allocated to processing by BofA servers. The analysis, summarized in Figure 3, shows that most of the time increase resulted from the greater time required to process the transactions at the BofA ECS server (white areas of the figure). There were no systematic or large increases in the message transmission times (gray areas of the figure).

Table B. Results of Volume Testing – Average Total Processing Time (transmission, decryption/encryption, translation, acknowledgment) for increasing numbers of embedded 820 payment instructions.

Number of 820 payment instructions in the e-mail message	Average Total Processing Time (from the time LLNL sends 820 to the time LLNL sends the final 997)	Notes
null to 5	11 minutes	N=129 (Average over 7 months of the pilot – includes only problem-free transmissions.)
100	12 minutes	N=8
300	19 minutes	N=6
500	43 minutes	N=7
1000	58 minutes	N=4

Figure 3. Volume Testing -- Summary of Bank of America/LLNL FEDI Pilot Results



Note: White areas show time required by BofA servers to process EDI documents (Steps B and D).
Gray areas show time spent transmitting messages over the Internet (Steps A, C, E and F).

# of 820 (payment instructions) in the mail message	message containing 820s transmitted from LLNL to BofA over internet	decryption and format checking of 820, generation and encryption of 997	997 transmitted from BofA to LLNL over Internet	BofA's ECS processes payment instructions, generation and encryption of the 824	824 transmitted from BofA to LLNL over the Internet	LLNL system matches information on 820, 997 and 824 and sends a 997 acknowledgement back to BofA over the Internet
Step	A	B	C	D	E	F
100	0:00	0:07	0:03	0:05	0:03	0:00
300	0:01	0:14	0:01	0:12	0:01	0:00
500	0:04	0:24	0:09	0:18	0:09	0:00
1,000	0:09	0:39	0:01	0:31	0:01	0:00

For the pilot participants, the results of the pilot testing showed that many of the problems of security, reliability and timeliness stemmed from problems with their own FEDI systems and not from the use of the Internet as a transmission channel. The pilot participants were satisfied that the system of acknowledgements, cross-checks, and encryption/decryption processes provided a level of performance that is acceptable for sending sensitive information like payment instructions over the Internet.

6. Summary

BofA's decision to offer Internet based FEDI services is customer driven. The central question is "when" to begin Internet based services rather than "whether" to offer them. Consequently, the purpose of *the Financial-EDI-over-the-Internet* pilot was to gain confidence concerning the viability of offering Internet based EDI services rather than to sort out the currently available technical solutions for secure Internet transactions. The technical success of the FEDI project was critical. Since BofA is a pioneer in the area, failure to deliver a thorough examination of Internet EDI security, reliability and speed would be costly.

6.1 Objectives for the Pilot Project

The challenge for BofA in the *Financial-EDI-over-the-Internet* was twofold. First it was the challenge of publicly promising to exchange actual, secure, financial transactions over the Internet under actual circumstances and with a real customer, Lawrence Livermore National Laboratory, over an extended time period. The second part was to deliver a working implementation. To sort out and choose a viable technical solution amidst the prevailing Internet security debate, is a difficult task. Today, it is effortless to find material and WWW sites discussing and advertising Internet security options. To find out which solutions actually work in the large corporate environment when exchanging critical financial data, was an open challenge. No objective data was readily available.

6.2 The Pilot Project as a Learning Experience

Under the exploratory circumstances, BofA formed an entrepreneurial group, which took up the challenge while not relinquishing the performance of the members' day-to-day responsibilities. Like so many information system driven ideas, the *Financial-EDI-over-the-Internet* project had to sell itself to senior management. The project group, consisting of two organizations, and more than six business units developed ways of collaborating through large group meetings, use of the Internet, the organizations' respective Intranets, voice mail, and electronic mail. The team used meetings with experts to learn about the issues relating to EDI. Such meetings sometimes consisted of more than 25 people and resulted in interorganizational and interfunctional solutions. The team proved that critical, FEDI transactions over the Internet works. Moreover, the team showed that projects formed around technological novelties are an effective way of testing and incorporating new technologies into business solutions.

6.3 Security

Of the areas of information systems security, the *Financial-EDI-over-the-Internet* pilot concentrated on the technical protection of the special security problem, the Internet. The management of information systems security, physical protection, and security concerns related to the corporate network are addressed elsewhere. Of the special Internet security issues, the project directly addressed data modification, repudiation, confidentiality, and data integrity. Internet security issues related to eavesdropping, password sniffing, spoofing, and selective application of services were out of the pilot's scope.

Pilot projects, such as BofA's and LLNL's, are suitable for focused security risk evaluations. Although it is impossible to claim that successful security attacks did not occur, none were encountered during the months of the pilot project. The careful monitoring of the system at both BofA's and LLNL leads to a confidence level of adequate security in the addressed categories. Increased assurance comes from both parties' security departments which evaluated the system and suggested improvements during the project. When evaluating the success of the *Financial-EDI-over-the-Internet* project, it is important to remember that the system and its security testing will only serve as a proof of concept. On this proof, the final production system incorporating these security lessons and others will be designed. Although done under actual circumstances and with actual transactions, the pilot project provided

a relatively controlled environment and intentionally limited risk.

6.4 Reliability and Speed

The other two concerns, reliability and speed, were also adequately addressed at relatively small transaction volumes. Sending EDI transactions over the Internet turned out to be reliable (no messages were lost), and adequately fast. Again, it is important to remember that the *Financial-EDI-over-the-Internet* pilot was not meant to provide absolute proof of reliability and speed at levels of volumes much higher than a 1000 transactions per day. Rather, the purpose of the pilot was to gain confidence in a relatively small scale. After the level of confidence is achieved, the system can be scaled up.

Since the pilot project ended, BofA has been comfortable with the level of security achieved in the *Financial-EDI-over-the-Internet* pilot project. According to George Cheng, the Senior Vice President of Interactive Banking (a newly formed business unit for electronic commerce applications at BofA) it would be foolish to assume that the Internet is absolutely secure. No absolutely secure business solution exists, paper based or computerized. The *Financial-EDI-over-the-Internet* pilot project provided BofA with a learning experience about the issues and risks involved in Internet based business transactions. The pilot served as a proof of concept. Based on the proof BofA is implementing an improved production system.

7. Lessons

The purpose of the *Financial-EDI-over-the-Internet* pilot project at BofA is to test the security, reliability, and speed of the Internet in critical business transactions. Despite the technical orientation of the project, it can be viewed as a strategic project for BofA. It has been said that the risks of banking over the Internet are not technical or security related (Ogilve, 1996). Rather, the risks are strategic and competitive. The threat is that banks will be facing competition from unexpected directions. Some predict that in the electronic era, financial transactions over the Internet service can be offered by a software company as well as by a bank (Ogilve, 1996). Others say that banking can be done by personal computers on the Internet as well as by people in the bank branch offices (Williamson, 1996). According to these scenarios, banks will be reducing the number of branch offices and employees while increasing their services over the Internet. The fear is that unless banks are among the pioneers of secure transaction processing over the Internet, other industries will claim the market. In this light, it can be claimed that the technical components of the *Financial-EDI-over-the-Internet* project have strategic consequences. The lessons of the project can be viewed from the perspective of EDI, cost, the Internet, and the organization.

7.1 EDI Related Lessons

Today, the project group is confident about the future of EDI. As a large corporation, BofA has the opportunity to influence the shape and form EDI will take. As a member of CommerceNet, BofA is participating in the ongoing development of interorganizational standards of which EDI is one. As a large organization, BofA is also an attractive partner in development of more open EDI solutions by software and hardware vendors interested in the area. It is likely, that EDI will evolve toward easier to use solutions as interorganizational standards are implemented in environments such as the WWW and the Internet influenced by corporations such as BofA and its customers. The pilot study has shown that today's EDI solutions already adequately accomplish the task. Moreover, it confirmed that EDI will be a part of the future services provided by BofA on the Internet.

7.2 Cost Issues

While costs savings are one of the most obvious benefits of using the Internet instead of VANs to transmit FEDI documents, experts take a more cautionary approach. One estimate places transport costs as taking only 5% to 15% of the total cost of a VAN services (Adhikari, 1996). Whether this represents a significant cost saving for a company depends on several factors. These include differences in one-time set-up costs, monthly charges, any usage charges, whether or not messages will be transmitted during the VAN's peak or off-peak hours, and how much the company needs the non-transmission services of the VANs. Table C provides a worksheet for thinking about these issues.

Table C. Worksheet for comparing costs between VANS and the Internet.

Types of Charges	Value Added Network	Internet Service Provider
Set-up Costs		
Monthly Rate		
Character Rates Off Peak vs. Peak		
Other Services used by your company		

How to use the worksheet:

1. Determine how much it will cost to initiate and set-up the system using either a VAN or ISP. These costs include start-up fees as well as any hardware or software purchases, programming and customization (e.g. building EDI translators). At BofA, setting up the PEM server, translators and links to the ECS server cost $75,000.00

2. Determine basic monthly charges you have to pay even if you do not send any data over the network

3. Decide whether you will send the EDI documents during peak or off-peak hours of the VAN. Approximate how many characters you will send over the network monthly and multiply this by the rate that is in effect when you send the documents

4. List the VAN services that you use (e.g. mailboxes, message tracing). Decide whether those services are worth the price differential between the two channels.

7.3 Internet Related Organizational Impacts

Although cost was one of the central issues in the initiation of the *Financial-EDI-Over-The-Internet* pilot project, the Internet related lessons from the *Financial-EDI-over-the-Internet* pilot project do not revolve around the cost and service level concerns of using the Internet versus other transport mechanisms. Rather, it is clear that special attention had to be paid on the organization of Internet based services. Like most large corporations, BofA is organized into functions such as marketing, product development, customer service, information systems support, and information systems security. When designing and implementing Internet based electronic commerce services, it is no longer clear which function should be responsible for the project. For example, is the firewall a part of information systems support, the business unit providing the EDI based service, or should it be a responsibility of telecommunications? Moreover, is a corporate WWW site a part of marketing, each business unit, or does it belong to the network support? In the *Financial-EDI-over-the-Internet* project, the organizational issues were solved by forming a project organization which included marketing, the responsible business unit called Global Payment Services, information systems support, information systems security, telecommunications, and the customer partner, Lawrence Livermore National Laboratory (LLNL).

Also during the pilot project, a new unit called Interactive Banking was formed to answer to the customers' increasing requests for Internet based services. The Interactive Banking unit, a company within a company, was founded to overcome some limitations of the functional organization. Instead of attempting to coordinate the corporate functions for electronic commerce, the Interactive Banking unit consists of its own technology, marketing, product development and customer service. Such serviced based concerns are indicative of the infrastructure changes the Internet is bringing to those engaged in the electronic market place.

7.4 Open Issues

After the questions concerning security, reliability and speed have been adequately addressed by the *Financial-EDI-over-the-Internet* pilot project, several issues remain open. The open management questions include: what are the arrangements with the EDI business partners concerning electronic signatures, certification, or encryption key management?; what is the policy for offering public WWW services of which EDI service may be a part of?; and can all functions decide about their own Internet policy and implement their own WWW sites? EDI and Internet based services require a new kind of planning to address these

questions. This planning is essential, because of immediate and global visibility called "web presence." BofA has solved the problem by centralizing the Internet management. All units may develop WWW sites for internal use, but only one unit is responsible for the external BofA WWW image and standards.

Other open issues are directly related to the pilot project. First, the data we have is somewhat biased since the organizations only tracked the messages within their systems and not through their transit over the Internet. We do not have much information about the intermediate nodes through which the message packets traveled. Some of this information could be used to explain some of the unresolved problems. These involved message truncation and problems with LLNL's difficulty with decrypting two 824 documents.

Second, as BofA ramps up to handle a greater number of clients, two issues become important beyond building a full-scale hardware-based system:

- The pilot system relied on e-mail messages and intense human attention to track the transit of the messages through the system. This worked during the pilot since transmission occurred only once, maybe twice a day. This system will probably not be feasible once BofA has numerous clients and has to manage many FEDI transmissions a day. The standards for monitoring message sequencing and transmission problems for Internet FEDI are not very well developed (IETF-EDI Working Group, 1993). There is a need and opportunity for an organization to make these procedures explicit and independent of human monitoring as much as possible.

- There is also a need to develop a system for managing the public keys of BofA's clients – to certify them, store them, and apply them to incoming encrypted messages. One option would be to use a package like Premenos' Templar, although this would work only for clients that use Premenos Templar as well. For non-Templar clients, BofA has to develop the procedures and storage facilities for managing these keys, including determining who would serve as a Certifying Authority.

Some critics of EDI over the Net also claim that the projected savings are more apparent than real. Transport costs, a big savings from using the Net, constitute only 5% to 15% of the total cost of a VAN operation, says Brian Dearing, president and CEO of ARI Network Services Inc., a provider of vertical turnkey services in Milwaukee and a 10-year veteran of the EDI industry. The rest, he says, goes to support and maintenance. That cost will shift to users that start using the Net for EDI. "The deeper we go into the Internet, the more demand there's going to be for in-house management," says Roger Cadaret, chairman of the board of directors at the Data Interchange Standards Association, a not-for-profit corporation in Alexandria, Va., that is the

secretariat for the Accredited Standards Committee X.12 and the administrator for the Pan-American EDIFACT Board. For example, a corporation handling 125,000 messages a month pays $50,000 to $100,000, depending on the VAN and how much of the traffic is transmitted during prime time, according to David Raye, VP of operations at the PC division of TSI International in Bannockburn, Ill., which sells PC-based EDI software.

8. Conclusion

Because of the pilot project, BofA has gained significant experience in the immediate organizational issues involved in electronic commerce initiatives. For BofA, from a technical standpoint, the *Financial-EDI-over-the-Internet* pilot is a systems integration project. Systems integration today seldom involves novel or unsolvable problems. Thus, the *Financial-EDI-over-the-Internet* project may have significant technical obstacles, yet it is mainly about management and policies.

Retrospectively, the pilot project had a characteristic, which can be called real time research (Porra, 1996). Real time research means that instead of conducting an isolated and insulated laboratory pilot study, the *Financial-EDI-over-the-Internet* pilot project included *real* organizational units which worked together under *real* circumstances using *real* business transactions. Moreover, up to certain dollar amounts, the pilot system was the only system used for FEDI transactions between BofA and LLNL. BofA sees such real time research as a basic part of their experimental method to employ new technologies. Real time research uses the existing organizational resources, people, software, and hardware to manufacture a technological and organizational solution. Compared with more

traditional research and development projects, real time research is effective. It solves *real* problems in actual circumstances by the people who will be responsible for the electronic commerce service in the future. In real time research, the functional organizational unit creates an environment for entrepreneurial teams. They behave like start up businesses within businesses. Reality based experiments like BofA and LLNL demonstrate the feasibility to utilize the Internet as an entrepreneurial rather than laboratory environment.

By choosing to be proactive by stepping into the real-time world of the Internet, BofA has demonstrated a strategic shift in its marketing, services, and information systems development methods. As the Financial-EDI-over-the-Internet pilot demonstrates, the openness of the electronic markets will fundamentally change the way companies organize and interact. Preparing for the Internet explosion, both organizationally and technically, BofA is not overly concerned with competition. Banking is a complex business which has both regulated and unregulated areas. Some of the unregulated areas are attractive for companies, such as financial software manufacturers who know the technology and aspects of electronic banking. BofA, however, knows both the regulated and unregulated banking and is able to provide integrated customer services. As such, BofA can guarantee its continued presence in the financial market place by the implementation of the Internet project.

With the validation provided by this *Financial-EDI-over-the-Internet* project, BofA is in position to make strategic changes to its marketing and operational components by incorporating the new Internet solutions in its product/service mix. The strategic lessons are not technical -- the are organizational. Any large firm wishing to examine the Internet for possibilities can be assured that the technical solutions exist. However, without the willingness to make significant organizational, strategic marketing and technical infrastructure changes, the technology of the Internet will have little utility.

References:

Adhikari, R. (1996). Electronic Commerce – EDI Heads For the Net – Companies Get Faster Messages, Reach New Markets, And Cut Costs. *Information Week*, (May 6).

Bhimani, A. (1996). Securing the Commercial Internet. *Communications of the ACM*, 39, 6 (Jun 1996), 29-31+.

Cohen, F. (1996). Your firewall won't save you. *Forbes*, ASAP Supplement, (Jun 3), 84.

Davis, J., & Parsons, M. (1995). EDI vendors adjust strategies in face of growing Internet. *InfoWorld*, 17/18, 52/1 (Dec 25, 1995/Jan 1, 1996), 39.

Fleishman, G. (1996). *Transactions over the Net*. Http://maigret.popco.com/hyper/inet-marketing/archives/9501/0120.html. Internet Marketing Mailing List.

Gaffin, A. (1994). *NCD will provide secure banking over the Internet*. Http://haas.berkeley.edu/~helmer/e…t/artikel/epayment/palyers/fv.html, Network World, Inc.

Green, C. (1993). EDI: *Adoption Rationale and its Relationship to Implementation*. A White Paper. Information Systems Research Center, College of Business Administration, University of Houston.

Hutt, A.E., Bosworth, S., & Hoyt, D. B. (1995). *Computer Security Handbook*. (Third, ed.). New York, NY: John Wiley & Sons, Inc.

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic data interchange and small organizations: Adoption and impact of technology. *MIS Quarterly*, 19, 4 (Dec 1995), 465-485.

IETF-EDI Working Group. (1993). *Requirements for Interoperable Internet EDI*. Internet Engineering Task Force for EDI (ftp.sterling.com/edi/lists/ietf-ediint/IETF03.txt).

Lawrence Livermore National Laboratory. (1996). *Financial Electronic Data Interchange Pilot Project*. Lawrence Livermore National Laboratory, Finance Department, UCRL-AR-124103, (May 1, 1996).

Mann, S. (1996). Good-bye EDI, hello Internet. *Manufacturing Systems*, Supply-Chain Strategies: Forecasting and Demand Management Supplement, (Jun 1996), 16A-17A.

Messmer, E. (1995). EDI heavies push data over the "Net". *Network World*, 12 48 (Nov 27, 1995), 1,8.

Messmer, E. (1996). The Internet rocks EDI boat. *Network World*, 13, 18 (Apr 29, 1996), 57.

Ogilve, C. W III (1996). Cyberbanking. *Bank Management*, 72, 3 (May/Jun, 1996), 14-18.

Pant, S., & Hsu C. (1996). Business on the Web: Strategies and Economics. *Computer Networks & ISDN Systems,* 28, 7-11 (May 1996), 1481-1492.

Premenos (1996). *Templar Software and Services – Secure, Reliable, Standards-Based EDI Over The Internet*. Http://www.templar.net/, Premenos.

Porra, J. (1996) *Colonial Systems, Information Colonies and Punctuated Prototyping*. Jyvaskyla Studies in Computer Science, Economics and Statistics, 33. Jyvaskyla University Press, Jyvaskyla, Finland.

Segev, A., Wan, D., Beam, C., Toma, B., & Weinrot, D. (1995). *Internet-Based Financial EDI: A Case Study*. The Fisher Center for Information Technology and Management, Institute of Management, Innovation and Organization, University of California, Berkeley, Working Paper CITM-95-WP-1006, (August 1995).

Smith Bers, J. (1996). Diving into Internet EDI. *Bank Systems & Technology*, 33, 3 (Mar 1996), 38-40.

Sokol, P. K. (1995). *From EDI to Electronic Commerce – A Business Initiative*. New York, NY: McGraw-Hill, Inc.

Sterne, J. (1995). *World Wide Web Marketing – Integrating the Internet into Your Marketing Strategy*. New York, NY: John Wiley & Sons, Inc.

Stipe, S. E. (1996). CEO's express skepticism about selling on the Internet. *Best's Review* (Life/Health), 96, 12 (Apr, 1996), 24-29.

Stuart, A., & Dahle, C. (1996). CIOs at the crossroads. *CIO*, 9, 16 (Jun 1, 1996), 28-30.

Vacca, J. (1996). Internet Security Secrets. Foster City, CA: IDG Books Worldwide, Inc.

Wan, D., Beam, C., & Weinrot, D. (1995*). Interview with Bill Jetter and Diana Bowler*, Apr.5, 1995. Haas School of Business, University of California, Berkeley.

Wheatman, V. (1995). *Financial EDI: Getting from Here to There*. Northern California EDI User's Group.

Williamson, M. (1996). Banks on balance. *CIO*, 9, 17 (Jun 15, 1996), 70-80.

Glossary

820 -- Payment Order/Remittance Advice Transaction Set (820). The 820 transaction set can be used to make a payment send a remittance advice or make a payment and send a remittance advice. This transaction set can be an order to a financial institution to make a payment to a payee. It can also be a remittance advice identifying the detail needed to perform cash application to the payee's accounts receivable system. The remittance advice can go directly from payer to payee through a financial institution or through a third party agent.

824 -- Application Advice Transaction Set (824). The 824 transaction set can be used to provide the ability to report the results of an application system's data content edits of transaction sets. It is designed to accommodate the business need of reporting the acceptance rejection or acceptance with change of any transaction set.

827 -- Financial Return Notice Transaction Set (827). The 827 transaction set can be used to report to the originator the inability of the originating financial institution to have the Payment Order/Remittance Advice Transaction Set (820) processed.

997 -- Functional Acknowledgment Transaction Set (997). The 997 transaction set can be used to define the control structures for a set of acknowledgments to indicate the results of the syntactical analysis of the electronically encoded documents. This standard does not cover the semantic meaning of the information encoded in the transaction sets.

MIME -- Multi-purpose Internet Mail Extensions. MIME is an Internet Standard that defines the format of email message bodies to allow multi-part textual and non-textual message bodies to be represented and exchanged without loss of information, including video, audio, graphics, and other application specific data.

MOSS -- MOSS is a Privacy Enhanced Mail (PEM) derivative that is a Proposed Internet Standard for

adding security services to (MIME). It uses the cryptographic techniques of digital signature and encryption to provide origin authentication, integrity, and confidentiality to MIME objects. Users of MOSS can know who originated a message, that the message has not been changed enroute, and that the message was kept secret from everyone except the intended recipients.

PEM -- Previously, the Internet community endorsed a secure email technology standard called Privacy Enhanced Mail (PEM), which provides authentication, integrity, confidentiality, and non-repudiation of text-based email messages.