

**Date**

September 20, 1995

**To****File****From**

Edward J. Hogan

**Memorandum****Subject****Visa/MasterCard Cooperation on an Internet Security Standard****Copies To**

In late 1994, Visa and Microsoft announced an agreement to create, publish and implement a security standard called Secured Transaction Technology (STT), for securing bankcard transactions over the Internet and other public networks. At that time Visa stated in the press that they would essentially allow MasterCard to have STT after an appropriate interval of Visa use. In early 1995, MasterCard announced that it was working with Netscape to develop an open standard for security on the Internet. The difference between the two announcements were that the Visa announcement clearly indicated a proprietary interest and contractual agreement between Visa and Microsoft to effect security on the Internet, while the MasterCard announcement said that it was using the talents of Netscape to create an open standard for the industry.

Shortly thereafter, I contacted Pete Hill of Visa and suggested that we would be interested in a combined effort to reach a single bankcard security standard that was open and had no implicit vendor proprietary interest. He showed interest but did not commit.

In May, Visa and MasterCard started talking seriously about combining our efforts to reach a joint standard. The Visa executive that represented that company was Dick Lonnergan, an EVP. I represented MasterCard. In June of 1995, we announced our joint intention to conclude a bankcard standard for global bankcard interchange over the Internet and other public networks. I have attached that announcement as Exhibit 1, and any fair reading of it will clearly reflect the intentions of the two associations. MasterCard's first inkling that Visa's intentions were insincere was the fact that there was a subrosa theme in the press stating that the agreement was really nothing more than a propagation of Microsoft's STT. Microsoft was so quoted in the press, but Visa remained anonymous, although a number of press personnel stated that that was what Visa said in private. When confronted with this MasterCard accepted Visa's denial of the accusation.

There were two incidents that could be directly related to specific Visa employees:

- Enar Asbo attended a W3C meeting and declared that the MasterCard/Visa cooperation was really MasterCard accepting the Visa/Microsoft STT specification.

P-0405

GOVERNMENT  
 DEPOSITION  
 EXHIBIT  
 1168

He said that there would be very few changes made to STT as a result of any MasterCard accommodation and that when it was all over said and done, STT would be the order of the day. Dick Lonnergan disclaimed that performance, stating that he was just wrong and Visa offered to remove Enar from the joint effort.

- Pete Hill previously had been quoted in a press release that the joint effort would actually be STT with Microsoft and that it would be afforded to MasterCard. Again, Visa stated that the announcement was a carryover from their previous position prior to cooperating with us and making the joint announcement.

In the intervening months between January and June, MasterCard had determined that the Netscape solution for security was very communication oriented and not specific enough to protect payment instructions in a full interchange environment between multi-vendor platforms. Fortunately, IBM had promulgated its iKP payment security for open networks, and IBM was willing to cooperate with MasterCard. Additionally, MasterCard had engaged the services of GTE Corporation to assist us in forming a certificate authority management system. GTE also proved to be very knowledgeable about the workings of security and the Internet. Finally, MasterCard also used the services of CyberCash, a willing participant in development of an open standard and a knowledgeable player. The consequences of a MasterCard, IBM, Netscape, GTE and CyberCash consortium were such, that MasterCard formed a substantial detailed understanding of how it would effect security on the Internet.

After the joint announcement in June, the two associations immediately met and continued to meet thereafter regularly. Fortunately, our two approaches to security were quite similar and all things being equal a common standard would likely have been arrived at. MasterCard suggested that we actually start from scratch and proceed through an expedited process of establishing:

- Business requirements
- Functional requirements
- Detailed system design
- Program specifications

Visa agreed and the two associations very rapidly reached agreement on the first part - business requirements. However, a certain reluctance on the part of Visa became apparent as we proceeded on to functional requirements. Specifically:

- Visa was unwilling to have vendors attend the meetings to assist the effort. They said that Microsoft was vehemently opposed to any such arrangement.
- Visa was unwilling to exchange documentation about how the two associations intended to individually accomplish security. They implied, if not stated, that their agreement with Microsoft precluded such action.
- There were certain matters regarding security or the processing of transactions that they were unwilling to discuss as they stated that they were proprietary between Visa and Microsoft.
- They were reluctant to actually define functional requirements with MasterCard, outside of STT.

Despite the above, the two associations managed to agree on functional specifications, much of which was in direct conflict with suggested STT principals and procedures.

While this was going on I had met with Microsoft's Tom Johnston and Warren Dent at O'Hare Airport on June 16. Both companies expressed a willingness to work with each other, but I cautioned them that MasterCard was only interested in an open standard that was not vendor specific. They claimed STT would be open, but that they and Visa would both own it and would share that ownership with MasterCard. I rejected the notion and again emphasized that "open" means that no one with a vested commercial interest in the standard could own it or influence the nature and extent of how it was used by competitors of a vendor so favored. They also attempted to convince me that a deal could be worked out between MasterCard and Microsoft where MasterCard could institutionalize STT at acquirer and merchant sites at rebate prices, that MasterCard would collect from its acquirers on behalf of Microsoft. I rejected the offer and advised them that no such accommodation could ever be made between MasterCard and a vendor affecting MasterCard acquirers and merchants, and that Microsoft would have to compete in the open market with other vendors to influence merchant decisions, and that any price that they could agree upon with a merchant or acquirer under those circumstances was appropriate. However, it was completely inappropriate for Microsoft to have such an edge by being the owner or partial owner of the security standard that made it all work. We parted friends, but essentially agreed to disagree. I subsequently learned that accounts of that discussion were transmitted to Visa. That was to prove true of all meetings we also had with Visa, independent of Microsoft and vice-versa. Both Microsoft and Visa conversed openly about all meetings they had with MasterCard.

The meetings between the staffs of the two associations continued and Visa conceded to allow GTE to attend representing MasterCard. Visa was to be represented by Bellcorp, but they never appeared at the meetings. Visa's reluctance to really work at obtaining a standard became more apparent. John Gould and John Wankmueller complained to me that their efforts were being stymied by the hesitancy of Visa to cooperate. It also became apparent that the lead Visa employees on the cooperative effort, Linda Gage a SVP and Bill Morris a VP were really not part of the mainstay of the Visa/Microsoft STT effort, which was led by Enar Asbo and Tony Lewis. In fact, Tony Lewis had openly suggested to our staff that they, the Visa employees, were merely red herrings to keep MasterCard at bay while the real work got done.

What all of this meant to MasterCard staff was an uneasy and ever growing feeling that the joint effort to reach a common conclusion was in fact nothing more than Visa attempting to seduce and convince MasterCard to join them in their Visa/Microsoft STT effort. However, whenever we confronted the issue there was always enough assurance given from Visa that convinced us to go forward. However, we took our assurance in the mainstay from a letter written by Gene Lockhart to Ed Jensen in which Mr. Lockhart requested assurance from Mr. Jensen that it was Visa's intention to reach a common security standard with MasterCard, that was open to the industry and owned by the two bankcard associations, and was not specific to any vendor, including STT. Mr. Jensen replied in the affirmative that that was Visa's intention. Those two letters are attached as Exhibit 2.

There were two specific meetings held during this time which were particularly noteworthy:

1. On August 10, Ed Hogan, Phil Verdi and Robin Townend met with Bill Chenivich, Dick Lonnergan, Francois Dutrez and Pete Hill of Visa, in Chicago. During that meeting, Bill Chenivich said Visa was tired of dealing with vendors and that what both associations really needed to do was to agree to do that which is right for the banks and force the vendors to follow. We agreed. They then asked us to accept STT as the starting place and red line it to affect the joint standard. We declined and offered to have our document and STT placed on the table so that they could be combined into a single document. Visa agreed and we established a schedule to exchange documents and meet to merge them.

Bill Chenivich advised us that Visa had until October 25 to publish a standard other than STT or they had to join Microsoft in STT, as per their agreement with Microsoft. So, they requested that we agree by October 15 to a standard, and that STT, as is, need not be the standard. We agreed, but felt confused by the disparity between Bill Chenivich's expressed attitude of independence and the requests of Pete Hill, Francois Dutrez and Dick Lonnergan to "red-line STT."

So be it! We decided to press forward and force Visa to choose.

2. Paul Garcia of Nabanco, the acquirer for Microsoft, called Gene Lockhart and asked him to review the matter on behalf of Microsoft. A four way conversation between Misters Garcia, Lockhart, Dent of Microsoft and myself ensued in which it was agreed that MasterCard staff would meet with Microsoft staff in Redmond, Washington to review STT, and determine its appropriateness for MasterCard interchange.

We went to that meeting on August 16 and were essentially asked to endorse and accept STT. We refused for all the same reasons noted above and Microsoft opted not to review the actual STT document with us. However, MasterCard and Microsoft discovered that we could work together and had very good and clear dialogue about the industry and security on the Internet. Microsoft advised us on a number of matters:

- i) That they were concerned about Visa's inability to bring MasterCard to their joint venture. Visa had assured them that MasterCard would follow Visa's lead. Microsoft now understood the folly of that assumption. They confirmed that their agreement with Visa had allowances for that occurrence.
- ii) That they now understood that, Microsoft would not get transaction fees from MasterCard directly. That they had to deal directly with acquirers and their merchants. That, that was all right with them, although not preferred.
- iii) That they were willing to change STT, but not so "drastically" as might be required by an "open" standard, conforming to industry specifications.

For our part, MasterCard assured Microsoft that we took no delight, nor would we allow "Microsoft bashing." We would like to work with them, but the standard could not be STT, and it had to be open and owned by the associations. They acknowledged our position but did not agree. They asked us to endorse STT; I refused. They asked if the standard could be called STT; I refused. They asked if MasterCard would join Microsoft in a press announcement where Microsoft would publicly agree to endorsing the about to be released MasterCard/Visa joint specification; I agreed - they declined.

We parted friendly and agreed to actively pursue a number of commercial opportunities of mutual interest. It was apparent that the two companies viewed the development of the Internet quite similarly - and that Visa did not! It was agreed that Microsoft could have agreed to accept MasterCard cards for payment on the Microsoft Network, using STT, if they wanted us. Engaged to so authorize it. They refused, holding out for such an occurrence to be linked, to a MasterCard endorsement of STT. In the final analysis, they refused to allow MasterCard to be so used, and they decided not to allow us to review STT, as promised.

Thus, MasterCard staff continued to work with the Visa staff towards reaching a position where the two documents could be combined into a single standard. It was agreed that we would start that exercise in San Mateo on September 27. In the interim, Microsoft sent MasterCard a draft of how STT might function. It was labeled as an early version and to be used only for general insight. It was high level, but did provide some insight as to how it worked. We had conversations with Microsoft and with Visa and we advised them that we saw a number of difficulties with the Microsoft provided STT document and its approach to security. We always advised Visa that we wished to have their version of STT, the one that would be finalized for a bankcard standard. We had not received any such documentation at this time. The high level difficulties with the Microsoft draft version of STT were relayed to Warren Dent as:

- Non-observance of X5.09 certificate standard
- Non-observance of the ANS.1 message standards
- That the methodology used by Microsoft for encryption seemed to be less efficient than the MasterCard approach
- That the MasterCard and Visa must own any standard outright, including STT, before it could become standard

Warren Dent wrote back that:

- Microsoft is adamant in not changing to the certificate standard. That that would be a deal breaker for them.
- That they were willing to negotiate on the use of the ANS.1 standards for messages
- That they were willing to engage in discussions with us about how encryption could be best done, and
- That they understood our concerns about ownership

It became readily apparent to both John Gould and John Wankmueller, and the St. Louis staff working with Visa personnel, that Visa personnel were not truly involved and dedicated to this outcome. Eventually, Visa staff openly admitted that any opportunity for an open bankcard standard, designed by the two associations was limited by the Microsoft/Visa agreement, and that

Microsoft was really in charge. Visa staff suggested that they wished their hands were not tied and they could truly join us and work this matter. These comments were made openly, unsolicited, both in private and during general sessions.

The planned exchange of security standards documents between MasterCard and Visa never occurred as deadlines passed. In the case of MasterCard, we had advised Visa that we would be later than them in getting a document because we were still compiling it. In Visa's case they missed two deadlines, but eventually had an STT document that they would provide to us. (In fairness, both associations missed deadlines.) However, Visa now required a non-disclosure agreement between MasterCard, GTE and Visa in order for us to review STT. The first version of the non-disclosure agreement contained the following types of provisions:

- That we could only receive a single copy for everyone to review and everyone would have to review it in the New York office, irrespective of whether they resided in St. Louis or Boston or wherever.
- That we would be personally liable for any press leakage of the document, and that the assumption could be made that if it were leaked, we did it. (Liability of \$10MM)
- That if MasterCard's document, subsequently provided to them, contained any like provisions from their STT document, they had the right to assume that we plagiarized it.

What followed was a series of revisions to the document over the next week and a half and finally, Visa agreed that a very basic, non-aggressive, non-disclosure agreement would now be acceptable. The reason it was now acceptable was simply that a few days earlier Visa had advised us that they intended to publish STT along with Microsoft. Copies of the non-disclosure agreements are attached as Exhibit 3. It was also apparent that Visa could not care less if it ever received the MasterCard document.

I advised Visa that if they published we would publish, and the industry would understand that the security standard effort had failed. I further told them that this was an incoherent act that could only be viewed as "commercial competition" by MasterCard and our vendor partners. Dick Lonnergan essentially acknowledged what I said and asked once again that we just accept STT, and I again refused. I advised them that until they actually published we would continue to cooperate, but I could offer no guarantee that cooperation would follow any such publication of STT. He fully understood the implications of Visa publishing and our actions that would surely follow.

A day or two later I got a call from Bill Chenivich who said that he was disappointed to find out that MasterCard was breaking the agreement made in Chicago with Visa, by publishing its own standard. He was totally nonplus when I told him the reason we were publishing was that Visa was going to publish STT first. He said, "nobody told me that part." He promised to get back to me, but never did. Instead, Dick Lonnergan and I continued to attempt to exchange a non-disclosure agreement that would be appropriate for both companies to sign, but that no company could possibly sign. It was very obvious to me at this point that Visa was not trying to cooperate and get such an agreement, they were bidding for time until they could get close enough to that

publication date when the STT document would be made public. However, giving them the benefit of the doubt we continued to attempt to work it out.

At about this time there were also two other important public announcements from Visa:

- Rosyln Fisher, a Visa EVP, publicly stated in a magazine article that Visa was working with Microsoft to publish the STT standard for security on the Internet, and that when they were ready they would "give it to MasterCard" for their use.
- Carl Pascarella announced at the ABA Bankcard Convention that Visa was working with Microsoft to create a U.S. standard for security on the Internet. This, after Alan Heuer announced that MasterCard was working with Visa to do the same.

On September 12, I notified Gene Lockhart about my concerns for completing the announced joint standard effort with Visa. That memo and his covering memo to the MasterCard International Executive Committee are attached as Exhibit 4.

On September 22, Gene Lockhart and Ed Hogan had a telephone conversation with Craig Mundie and Warren Dent of Microsoft about MasterCard allowing Microsoft to process MasterCard transactions, and MasterCard accepting STT as an acceptable security system. This was requested in light of the fact that Microsoft and Visa were about to announce STT publicly, and Microsoft truly wanted MasterCard to be a part of it.

We agreed provided that:

- The STT specification was truly implementable by all members.
- That MasterCard did not have to grant an exclusive approval of STT and could embrace other vendors.
- That the STT specification would be put into the public domain and not controlled by Microsoft.

Warren Dent and we understood Craig Mundie agreed.

Later that night, I received a phone call from Bennett Katz, Francois Dutrez and Dick Lonnergan of Visa who advised that they had been made aware of the MasterCard/Microsoft conversation that occurred earlier. They went on to suggest that MasterCard could become a full owner of STT along with Microsoft and Visa, and that the specification would be open, and that they wished us to join them as full partners in their press announcement. I said we would consider it, but that first we would have to actually see what STT was all about, that is, how open it was and what exactly were the consequences of such an approval. Visa now expedited the process by which a non-disclosure could occur and the documents were signed and exchanged. That is, MasterCard provided Visa its standard Secured Electronic Payment Protocol (SEPP), and Visa provided MasterCard, STT.

On Monday, September 25, MasterCard advised Visa that the STT specification had many substantial elements missing and was essentially unprogrammable for interoperability. They responded that it could essentially be enhanced later. We advised them that was totally unacceptable. Those documents are attached as Exhibit 5.

At about the same time we received a phone call from Microsoft wherein they upped the "ante" by offering MasterCard essentially the same deal that they had provided Visa. They were aware of our conversations with Visa. They pointed out to us that it was important that MasterCard realize that Microsoft's implementation of the STT specifications did not come totally free. They expected a license fee at the server level, per credential and/or per transaction. They stated that that was exactly what they had in their contract with Visa and it primarily involved a license fee on a transaction basis in the 5-15bp range depending on volume. They expected us to acknowledge that there would be some license fee of this type or form paid to Microsoft. We did not. That documentation is attached as Exhibit 6.

Subsequently, MasterCard and Visa engaged in a number of conversations among their staffs. Participating from Visa were Bennett Katz, Francois Dutrez and Dick Lonnergan, and from MasterCard myself, Bob Norton and John Gould. In order to move the matter forward MasterCard requested that Visa agree to five matters:

1. Have Microsoft place in the public domain all patents assigned to STT, Visa and we would do likewise.
2. Publish the current version of STT as "preliminary for review purposes only," and subject to a 30 day industry review.
3. That MasterCard and Visa complete the specification so that in the opinion of diverse industry experts, it was implementable.
4. That MasterCard and Visa develop detailed testing procedures to ensure conformance with the completed specification.
5. That the two associations own a reference software specification that vendors could use.

The document is attached as Exhibit 7.

Visa responded somewhat positively by accepting the first, third and fifth requirements. However, with respect to the second specification they were not willing to publish it as preliminary, but were willing to state that they would work with Microsoft and MasterCard to ensure that it was robust enough for interchange interoperability over the next 30 days. With respect to the fourth requirement of testing procedure, again they agree to work with us to accomplish it within the next 30 days. However, Microsoft testing would need commence prior to that time and they could actually implement, and further they expected that the testing procedures would use the Microsoft software as the testing foundation. The fax supporting those two positions is attached as Exhibit 8.

MasterCard had a final telephone call with Visa, and Microsoft executives joined in the conference at Visa's request. Representing Visa were Bennett Katz and Francois Dutrez, representing Microsoft were Laura Jennings and Warren Dent, and representing MasterCard were Ed Hogan and Bob Norton. MasterCard advised Visa that we would not accept their offer to participate as an owner in STT. That, essentially STT was not sufficiently detailed to provide members and vendors the ability to program it from the specification and that they would have to purchase it from Microsoft. Further, that Microsoft was too intimately involved in the



transaction for our endorsement. Finally, we could not proceed with the transaction on the basis of trust, assuming that it would be worked out later. I said that it was not that we did not trust the Visa and Microsoft companies, but rather that were it not to be actually worked out later, MasterCard would have no likely alternative at that time and, that to place the MasterCard association in such a position would be very inappropriate.

Visa responded, mainly in the person of Bennett Katz, very angrily. They challenged MasterCard by stating that they would make it known to the industry that they, Visa, were not the culprits in not having a single standard for the industry. That, they Visa would not accept the blame from the banks for causing this apparent breach. Further, that were MasterCard to approach Microsoft and Visa to participate in STT at a later date, the terms could be different and we would then be viewed as a "Johnny come lately" or an "afterthought." The conversation became argumentative on both sides and MasterCard ended it by repeating that it would not be involved in the Visa/Microsoft press announcement, but that we would not openly challenge them, provided they did not cause us to need to defend ourselves by their actions or words. When asked what they should say about MasterCard when the reporters inquired, we provided a short response that was essentially neutral and advised Visa to refer the inquiring party to us.

The next day, Visa announced STT. All the particulars of that announcement are attached as Exhibit 9<sup>\*</sup>. MasterCard sent a letter, personal and confidential, to its Board of Directors about these events. That letter is attached as Exhibit 10. Subsequently, we sent a letter to our members, attached as Exhibit 11.

This is the chronology of the events, as best as I can recall and document them. While there might be some specific details that were overlooked or omitted, those details could only be incidental and not operative to the truth. In conclusion, it is quite apparent that Visa's current position is that the cooperation between MasterCard and Visa was always meant to be MasterCard adopting STT. This is how they will characterize it, however, the facts clearly state that it was otherwise. Most notably; (i) the letter from Ed Jensen to Gene Lockhart agreeing that the standard would be open and not rely on any vendor specific technology; and (ii) the joint press announcement which essentially said the same.

---

\* A brief analysis of Exhibit 9 is attached as Exhibit 12 and was drafted on November 27<sup>th</sup>.

Attachments to memo "Visa/MasterCard Cooperation on an Internet Security Standard"

- Exhibit 1: June 1995 announcement of joint intention to conclude bankcard standard for global bankcard interchange over the Internet between MasterCard and Visa
- Exhibit 2: Letter from H.E. Lockhart to Ed Jensen (Visa) requesting assurances of Visa's commitment to joint effort and Mr. Jensen's reply
- Exhibit 3: Non-disclosure agreement between the two associations
- Exhibit 4: Memorandum from Ed Hogan to H.E. Lockhart addressing concerns about completing announced joint effort and H.E. Lockhart's related memorandum to MCI Executive Committee
- Exhibit 5: Documents stating MasterCard's concerns over missing elements and unprogrammability of STT, Visa/Microsoft reply stating it could be enhanced, and MC's response saying this is unacceptable
- Exhibit 6: Document outlining Microsoft's "licensing agreement" for use of STT and MC response to this information
- Exhibit 7: MasterCard requirements for Visa and STT if joint association is to continue
- Exhibit 8: Visa response to five requirements outlined in Exhibit 7
- Exhibit 9: Visa STT announcement
- Exhibit 10: MasterCard confidential letter to Board of Directors about these events
- Exhibit 11: MasterCard letter to member banks regarding same topic
- Exhibit 12: Brief analysis, from Ed Hogan, of Exhibit 9.

**Exhibit 1**

Release Date



EXHIBIT 1

**FOR IMMEDIATE RELEASE**  
Contact

Dorea Smith  
MasterCard International  
212/649-1421  
mascard@aol.com  
<http://www.mastercard.com>

David Melancon  
Visa International  
415/432-2427  
melancon@visa.com

**Visa and MasterCard Working Together to Support Specifications for Secure Card Transactions on the Internet**

NEW YORK & SAN FRANCISCO, June 23, 1995 – MasterCard International and Visa International today announced that the two associations will integrate their current efforts to provide a method for secure bankcard purchases on open networks such as the Internet. Consumers around the world hold more than 690 million bankcards, and with this security it means using those cards to conduct transactions in cyberspace will soon be as secure as using a card at a physical point of sale today.

Visa and MasterCard will support specifications expected to be published by September, and anticipate that consumers will begin participating in secure card transactions on the Internet in early 1996. As a first step, the associations are agreeing upon a common set of requirements and sharing technical information.

The security specification supported by MasterCard and Visa will be open and available to all entities. This standard will provide payment security for all bankcard transactions; other security protocols can be used to protect personal data. The new standard also will facilitate deployment of personal-computer (PC) software to incorporate payment-security applications.

"The first requirement necessary to grow a new market is consumer and merchant confidence. A secure transaction within a secure payment system is the foundation of that confidence," said Edmund Jensen, president and CEO of Visa International. "Establishing that environment for our member financial institutions -- and their consumers and merchants -- is the purpose of our groundbreaking efforts to forge partnerships that bridge the worlds of high-tech and financial services. Working together to build a common security payment standard for bankcard acceptance and use is a crucial step in the development of electronic commerce -- and will be the significant enabler in the commercial growth of the Internet."

-more-

**News Release**

## MasterCard/Visa Support Specifications--Page 2

"Establishing one standard for card purchases on the Internet is absolutely the right thing to do for consumers, merchants and financial institutions worldwide," said H. Eugene Lockhart, CEO of MasterCard. "The industry has a rich history of setting standards --the global chip-card specifications are an excellent example -- that benefit consumers worldwide. And, it's exciting that we will do the same in the dynamic environment of the Internet. Our objective is to ensure that every transaction, no matter what type it is and no matter where it occurs, is processed quickly, securely and reliably."

The specifications supported by the associations will call for the use of extensive encryption capabilities based on RSA Data Security to protect card transactions on the Internet and other networks. And, MasterCard and Visa anticipate that purchases and payments performed on open networks such as the Internet will function similarly to other bankcard purchases.

Protecting card transactions over open networks is crucial for both card associations. Bankcards represent the best payment option for users of the Internet, and that use will expand exponentially as the market continues its explosive growth. Protecting and leveraging their powerful brands in a non-physical world will be key to Visa and MasterCard. With a combined global-transaction volume of more than \$1 trillion, the associations' joint work in establishing security standards on the Internet will be a forceful engine for its continued growth.

MasterCard International Incorporated, a global payments franchise company with offices in 20 countries and headquarters in New York City, is comprised of more than 22,000 member financial institutions worldwide. Through its family of brands, MasterCard, Maestro and Cirrus, MasterCard offers a full range of credit and debit products and services supported by a global transaction processing network. MasterCard has more than 270 million cards issued which are accepted at more than 12 million locations worldwide. Consumers worldwide can access MasterCard "Pointers," the MasterCard World Wide Web site on the Internet, by dialing <http://www.mastercard.com>.

Visa, a worldwide consumer payment system, is playing a pivotal role in developing and implementing new technologies that benefit its members and their cardholders, business, government and the global economy. Headquartered in San Francisco, Calif., Visa and its 20,000 member financial institutions serve more than 12 million merchants and 402 million cards worldwide. It also operates Visa/Plus, the largest global ATM network. In 1994, Visa consumer card transactions (credit and debit) totaled more than \$630 billion worldwide. Visa maintains a home page on the Internet's World Wide Web at <http://www.visa.com>.

###

Exhibit 2

MasterCard International  
888 Seventh Avenue  
New York, NY 10106  
212 649-5100  
Fax: 212 649-5510



EXHIBIT 2 (c)

August 1, 1995

H. Eugene Lockhart  
President and  
Chief Executive Officer

Mr. Edward P. Jensen  
President and Chief Executive Officer  
Visa International  
P.O. Box 8999  
San Francisco, CA 94128

Dear Ed:

I enjoyed the many matters we discussed last week and I continue to share your enthusiasm for the development of electronic commerce on the Internet. We will continue to have our Ed Hogan cooperate fully with your Dick Lonergan to reach a usable security standard.

However, there is one significant point that I believe needs to be clearly understood between ourselves. Ed Hogan assures me that the end product of the security effort will be a single document from the two associations that defines interoperability for interchange. That document will be vendor neutral to protocols such as Netscape's SSL or Microsoft's STT, and rather define what those protocols need do in order to comply with the bankcard standard.

Ed, could you please confirm that this is also your understanding of the goal of the effort. Again, I enjoyed our conversation and look forward to continuing it.

Sincerely,

A handwritten signature in cursive script, appearing to read "Gene".

HEL/le



*Edmund P. Jensen*  
President and  
Chief Executive Officer

August 15, 1995

Mr. H. Eugene Lockhart  
President and CEO  
MasterCard International  
888 Seventh Avenue  
New York, N.Y. 10108

Dear Gene:

Thank you for your August 1, 1995 letter.

As you requested, I can confirm that our understandings are mutual. A single document defining interoperability for interchange will be vendor neutral to protocols and define what those protocols need to do in order to comply with bankcard standards.

I am pleased that we can aggressively compete for member business while providing real value for members through common standards.

Sincerely,

A handwritten signature in black ink, appearing to be "E. Jensen", written in a cursive style.

VISA INTERNATIONAL Post Office Box 8000, San Francisco, California 94128-8000 (415) 437-3200 Facsimile (415) 432-8085



**Exhibit 3**

*Chron*  
EXHIBIT 4



Date  
September 12, 1995

To  
MasterCard International Executive Committee

From  
H. Eugene Lockhart

**Memorandum**  
**STRICTLY PRIVATE AND CONFIDENTIAL;**  
**Privileged to Executive Committee Members**  
**Only**

Subject  
Internet, Visa, and Microsoft

Copies To

Attached you will see a note which on the surface may seem technical and very long-term, but is actually quite important. Basically the issue being addressed is the following:

1. With respect to the Visa/Microsoft relationship regarding the Internet announced several months ago, we strongly suspect that Visa also agreed with Microsoft that Microsoft's software should be used for secure transmission of credit/debit card transactions over the Internet. If implemented, this could effectively:
  - (a) provide Microsoft an insurmountable advantage vis-a-vis all other software suppliers.
  - (b) make all credit/debit card issuers operate only within Microsoft operating/technical standards at Microsoft's prices.
  - (c) result in the vast majority of credit/debit card transactions over the Internet being routed through Microsoft On-Line/Network.
2. We do not believe Visa fully informed their membership of the potential impact of this arrangement.
3. Visa apparently committed to Microsoft that they could "deliver" MasterCard; i.e., we would "fall into line" with their agreed approach.
4. On behalf of the industry, we have been resisting this because:
  - (a) we feel any such standard should be open.
  - (b) other suppliers (e.g., IBM, Netscape, etc.) should be encouraged to participate as well as Microsoft.
  - (c) the financial services industry should not confer upon Microsoft such a significant advantage with respect to routing of transactions.

Memorandum - MasterCard International Executive Committee  
Page 2  
September 12, 1995

5. We are beginning to see success in taking this approach. Other suppliers are actively engaged in working with us on an "open" standard which we hope enters the public domain sponsored both by Visa and MasterCard and gives everyone who desires to do so the opportunity to compete for this business.

We should discuss the implications of this briefly at the next Executive Committee. While the Internet is a lot of hype now, positions are being taken which could have significant, long-term consequences.

HEL/te

Attachment

Date

September 11, 1995



To

H. E. Lockhart

From

Edward Hogan *EH*

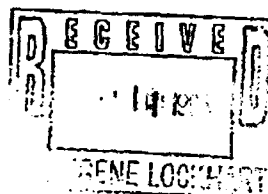
Memorandum

CONFIDENTIAL

Subject

The Internet, Visa and Microsoft

Copies To



BACKGROUND

In January, Visa and Microsoft announced that they had agreed to publish a joint specification to influence the processing and security of transactions over the Internet. They called it Secure Transmission Technology or STT. They believed that they had enough authority to influence the outcome and to force MasterCard and vendors to observe their conclusions. In fact, Visa stated in the press and in numerous speeches at various executive levels, that they intended to "give STT to MasterCard" when the time was right. Microsoft has since confirmed to us that their agreement with Visa was based upon their providing the functions and programming for STT and the belief that Visa could deliver MasterCard to the joint agreement.

In response to that effort MasterCard enlisted the aid of Netscape and IBM to counter the Visa/Microsoft effort and afford MasterCard's members a different opportunity. Our effort is aimed at promulgating an open industry standard that any vendor could comply, with license free. MasterCard definitively advised both Microsoft and Visa of our intentions and resolve not to have STT, by itself, be the basis of the standard, always asserting our willingness to compromise in favor of an open industry-wide standard. As you might expect the MasterCard position has been applauded by both the membership and vendors, while that same group was quite critical of Visa's position.

CURRENT SITUATION

While Visa has given up on MasterCard capitulating in favor of STT it continues trying to maneuver MasterCard to favoring STT. We believe they need to do this in order to resolve the dilemma they find themselves in. Specifically, they have agreed to announce STT as the

\*\*\*\*\*

only security specification for Visa interchange, and subsequently have also agreed to announce a joint bankcard specification with MasterCard. Those two notions are in competition with one another.

MasterCard has honored its commitment to develop an open non-proprietary standard. However, while Visa has repeatedly told MasterCard they are working on a joint MasterCard/Visa standard, they have been sending a clear and consistent message to the press, vendors and members that is at odds with a joint standard. Furthermore, many of their statements and actions towards MasterCard are consistent with this other posture. The

- Visa has refused to share with MasterCard any information about STT because of their non-disclosure agreement with Microsoft, which has similarly refused (until August 24th) to share any documentation on STT with MasterCard.
- Visa senior staff has told vendors, members forums and reporters (a) Visa will publish, with Microsoft STT, as their implementation of the standard, (b) Visa will share STT with MasterCard and MasterCard has agreed to adopt STT, (c) merchants who use electronic commerce software other than STT will not qualify for discounted fees.

Recently, Visa asked MasterCard to expedite the process of reaching a standard by effectively taking STT and changing it as necessary so it could become the joint standard. As has been our continuous position, we disagreed. Rather, we suggested that we combine the Visa STT document with the MasterCard-like document and create a single bankcard "open standard," even though combining the two documents is infinitely more arduous than creating a single original document

Visa agreed. We further questioned their intention to publish a joint Visa/Microsoft standard in September, prior to the publication of the joint MasterCard/Visa standard. We advised them that such a publication would confuse the industry and would cause MasterCard to also publish effectively undermining the joint effort. They advised us that they would reconsider.

Since then, Visa continues to internally characterize this MasterCard/Visa agreement as "MasterCard adopting STT." Recently, Roz Fisher, a Visa EVP, gave an interview in which she stated that Visa and Microsoft were going to promulgate a security standard and "give it to MasterCard." We believe Visa staff is not facing reality with regard to the "choice" that need be made between Microsoft and MasterCard.

More recently, Microsoft has taken to dealing directly with MasterCard and is requesting that we accept STT and forget the standard. Failing that, they wish to have assurances that the standard we adopt will not adversely affect the software code they have already written for STT. They have enlisted the aid of Nabanco, their acquirer, to influence that outcome.

\*\*\*\*\*

MasterCard's Course of Action

MasterCard has proceeded on a consistent course to: (1) have Visa adopt an open bankcard standard; or (2) have MasterCard promulgate an alternative. Having said that, we believe their are major parts of STT that are proprietary to Microsoft and that Microsoft's long term plan is to own the operating system for Internet servers and browsers. Microsoft has told us that they envision STT as a foundation, not unlike a new type of operating system, on which applications would be built. We believe that Visa did not really appreciate the nature of the deal it entered into with Microsoft, and that at this time Visa is dependent upon Microsoft STT for their Internet processing. They have not yet given us a STT document and are currently writing it. However, they can only start when Microsoft provides documentation that they can in turn edit.

It is our intention to stay this course, and encourage Visa to join MasterCard in an independent, open bankcard security standard. We believe we will succeed. We know we will likely not change Microsoft as they are truly single-minded, but we believe we can change Visa because, in the final analysis, Visa needs politically to endorse an open standard. We must continue with our resolve, we must force Visa to choose.

Assuming that all goes well, by October 15th, three documents will be created:

- A business requirement for the processing and security of transactions on public networks - agreed to and completed.
- A functional specification for processing on the Internet - virtually completed, but not completely agree upon. There are three or four significant items of disagreement.
- Software specifications as to how vendors are to implement the standard. This will be a source of contention and will be the point at which Visa need make a choice. Currently we anticipate harmonizing the Visa STT document with the MasterCard-like document. The MasterCard software specification is being written by MasterCard and GTE, assisted by IBM and Netscape. It will be ready in mid September and when combined with the above functional specification will serve as a complete standard for interchange. Without this specification MasterCard would have been forced to accept STT software specifications as provided by the Microsoft Corporation.

We are in the home stretch and we should know the truth of the matter in the next two or three weeks. It is our intention to have Microsoft adhere to a bankcard standard and not have a bankcard standard adhere to STT. There is always the risk of Visa and Microsoft breaking away and having an exclusive arrangement which omits MasterCard as a payment card. I don't believe that will occur and before such an outcome does occur I will convene a meeting.

01/18/98 doc

Exhibit 5



EXHIBIT 5

Date: September 25, 1995

To:                   DICK LONERGAN  
       Company        VISA  
       Phone #  
       Fax #           415-432-8132

From:                ED HOGAN  
       Company        MasterCard  
       Phone #        212-649-5456  
       Fax #           212-649-4742

RE:

1001

09-25-95 06:07 PM FROM MasterCard



**Elements Missing from Visa STT Specifications****Version 1.5**

We have broken down the deficiencies in the provided documentation into two broad categories: (a) missing or incomplete component definition, and (b) missing sections.

**A Missing/Incomplete Component Definitions**

The following components, which are necessary to provisioning a complete definition of all the functions and processes necessary to support secure electronic commerce, are absent.

- certificate request management
- management and ownership of root keys
- user interface functions
- certificate renewal
- certification revocation and management of CRLs for merchants
- securing cardholder/merchant secret keys and other data on computers connected to networks
- portability of cardholder keys/certificates
- complete and detailed function definitions for each entity (e.g. cardholder, merchant, acquirer, and issuer software)

**B Missing or Incomplete Sections**

The following sections, which are essential to a detailed programming specification, are completely absent from the document.

- Entity relationship diagrams
- Process specifications per entity to initiate, act upon, and respond to input
- Edits
- Error Handling
- Exception Processing
- Data Dictionary

9/25/95

1

2004

09-25-95 06:07 PM FROM MasterCard

- The only detailed specification provided is for the message formats, which are incomplete, proprietary (e.g. compression), specific to MSN, and many fields are not defined (e.g. Keyblob)
- Cryptographic techniques are incomplete and ambiguous (e.g. data to be hashed is not clearly defined)

In addition to the above deficiencies, there are several other areas of concern, including:

- Use of proprietary cryptography syntax
- No optional fields written to allow for expansion
- Use of Little Endian is platform specific favoring Intel

---

9/23/95

1

0001

09-25-95 06:07 PM FROM MASTERCARD

FROM: DICK LONERGAN  
VISA

FAX: 415-432-8132  
VOICE: 415-432-3549

TO: ED HOGAN  
MASTERCARD

FAX: 212-649-4742

Ed: Thank you for your quick response. The following addresses the points you made in your fax. We feel that many of them are quite important to work on together, but they by and large describe issues that are outside the intended scope of the STT specification.

Can we discuss this before your noon (9 a.m. our time) call with François Dutray and Bennett Katz to ensure that all your concerns can be answered. I will call you at 11 (8 a.m. in San Mateo) unless you leave a message on my voice mail that a different time is better.

Dick

Response to MasterCard fax on Elements Missing from STT Specifications

1. The STT Specifications were written to describe, at the protocol level, the dialogue, messages and cryptography necessary to meet business requirements for secure bankcard transactions. As a result, issues relating to policy of the bankcard brands (such as root key management) or specific application development options (such as user interface functions) were consciously not included in the STT document. Certainly, policy issues must be addressed before STT compliant software can be tested in the market place; this is an area where the bankcard associations should work together in the future.

Policy-related:	management and ownership of root keys certificate request management securing cardholder/merchant secret keys (policy) exception handling (at policy level)
-----------------	--

2. Visa believes that the application specific areas identified as missing are better left to the software developers, thus ensuring that STT implementations are open and not proprietary. In addition, the need to fully define the application program logic (entity relationship diagrams, process specifications, edits, and data dictionary) appears to us not to be necessary for the software development audience. These developers will choose to differentiate their products using their own proprietary development methodologies.

Application	user interface functions entity relationship diagrams securing cardholder/merchant secret keys process specifications per entity edits exception processing data dictionary
-------------	---

3. Certain functions identified as missing from the protocol were not intended to be part of the initial STT implementation, but would be included in a future enhancement (such as credential renewal and credential revocation dialogues or portability of cardholder keys and credentials). There was a conscious decision to limit the scope of STT at this time to those elements necessary to provide the basic protocol necessary for pilots in early 1996 and initial service introduction later in 1996. We agree that the document would be improved by adding a section describing the protocol for each software entity and also by more fully describing error handling.

Protocol	certificate renewal certificate revocation and CRL portability of cardholder keys
----------	---

complete and detailed function definitions by software entity  
error handling

4. While the detailed STT Specifications are terse, they are complete and are not proprietary. The cryptographic techniques are complete, but require a thorough knowledge of cryptographic annotations. The references to proprietary aspects are not in the current version (Pre-publication 1.8) that MasterCard received on Saturday, September 23, 1995.

5. The listed areas of concern are not deficiencies, but rather benefits of approaches taken by STT.

The cryptography syntax is not ASN.1, but it is not proprietary. It is open to all software vendors, and it is easier and quicker to program than ASN.1.

STT does not specify precise optional fields because the TLV format provides more flexibility and efficiency than does the use of optional fields. TLV enables optimal field expansion, plus forward and backward compatibility.

Little endian was consciously chosen to favor Intel, the predominant processor in the marketplace. The alternative favors Motorola and DEC at the expense of disadvantaging the majority of the market. Microsoft informed us that they expect an imminent commitment from a vendor to create a UNIX version of STT-compliant software.

7  
Exhibit 6

EXHIBIT 6

# FAX

Date: 09/25/95  
Number of pages including cover sheet: 1


TO: Doree Smith  
MasterCard  
  
Phone: 212-649-1421  
Fax Phone: 212-649-1473

FROM: Warren Dent  
Microsoft  
One Microsoft Way  
Redmond, WA 98052  
  
Phone: 206-936-1100  
Fax Phone: 206-936-7717

CC:

REMARKS:  Urgent  For your review  Reply ASAP  Please Comment

Date: Second fax today. We would like to request one adjustment in the second para of your quote. Where you say "placing their protocols into the public domain", could we either change the word "protocols" to "specifications" or double it to say "protocol specifications". The reason for this is that some people regard "protocol" as the actual implementation of a specification. We and others won't put our implementation into the public domain - but will put the specs.

Sincerely,  
  
Warren Dent

FAX to Ed Hogan  
FYI - I don't know whether his change is significant...  
Doree  
9/25/95

Highly Confidential Subject to Protective Order

**FAX**

Date 09/25/95

Number of pages including cover sheet 1

TO: Ed Hogan  
MasterCardPhone 212-649-5456  
Fax Phone 212-649-5555FROM: Warren Dent  
Microsoft  
One Microsoft Way  
Redmond, WA 98052Phone 206-936-1109  
Fax Phone 206-936-7717

CC:

REMARKS:  Urgent  For your review  Reply ASAP  Please Comment

EA:

I know you are working with legal etc on press release. Since we have not yet received the follow-up letter Gene indicated he'd send I thought I'd jot down a couple of important points for discussion. Craig indicated to Gene in their call that our arrangement with VISA does include a licence fee but that this is very small at the transaction level since our main revenue expectation is through the licensing of merchant servers. There are several different ways we could arrange a business relationship with MasterCard and as you indicated on Friday night we need to move this forward immediately. I think especially since your quote endorses placing specs in the public domain, it's important that MasterCard realize that Microsoft's implementation of these specs does not come totally free. We could ask license fees at the server level, per credential and /or per transaction.

To get to a bottom line understanding quickly Ed, we are prepared to offer MasterCard exactly what we have in our contract with VISA. This primarily involves a licence fee on a transaction basis in the 5-15bp range depending on volume. There are other arrangements possible. We could receive this fee directly from an acquiring bank, we could receive fees per credential issued etc. But in any event we'd like acknowledgement that there will be some licence fee of this type of form paid to Microsoft.

I'm looking forward to chatting with you. Tied up over next hour, will call when I get back. Cheers

Warren



Exhibit 7

September 26, 1995

Dick Lonergan

Edward Hogan

**STT Acceptance**

It would seem to me that MasterCard could accept STT as a joint MasterCard/Visa specification if Visa/Microsoft would agree to the following (in addition to what has already been offered to MasterCard):

1. MasterCard, Visa and Microsoft publicly state that they will place in the public domain all patents assigned to any of them that would be infringed by a normal, straightforward implementation of the specification.
2. The current version of the specification is published as a "preliminary, for review purposes only" and subject to a 30-day industry review. [It is inappropriate for MasterCard/Visa to promulgate a specification that is the sole work of a single industry entity.]
3. MasterCard/Visa complete the specification so that, in the opinion of diverse industry experts (obtained during the review process), it is implementable. Such additions are published as soon as available and subject to a minimum two-week industry review.
4. MasterCard/Visa develop detailed testing procedures to ensure conformance with the completed specifications. These testing procedures are made available to the industry.
5. By the two associations owning a reference software specification, Microsoft does not become the exclusive software supplier for the security protocol.

4. 10/14.doc

Exhibit 8

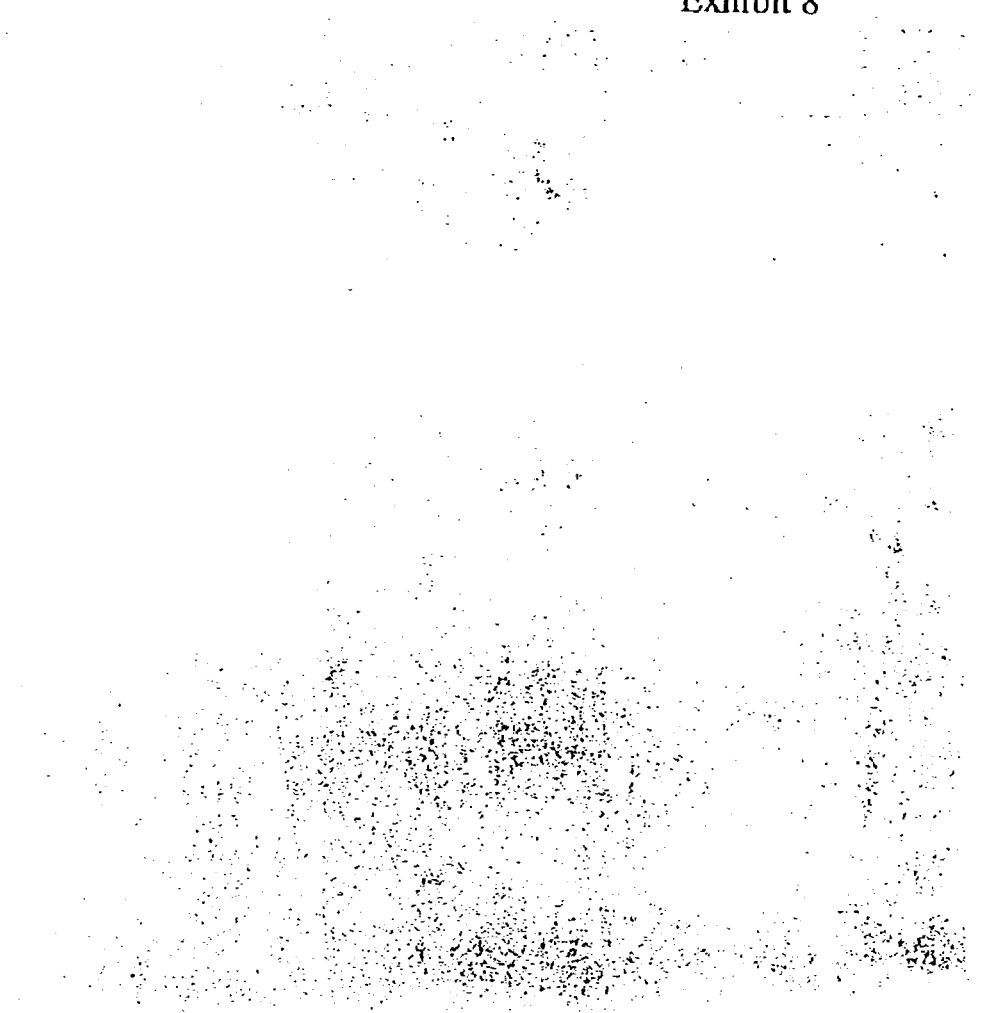


EXHIBIT 8

---

4. [POSITIONING WITH MASTERCARD – NOT FOR PUBLIC RELEASE]  
MasterCard and Visa will develop testing criteria/procedures to certify non-Microsoft software as STT compliant. These testing procedures must be ~~completed~~<sup>agreed to</sup> within 30 days. Microsoft testing will commence prior to establishment of any joint testing procedures, it will thereby form a testing foundation. Testing procedures for application functions beyond the STT specified protocols, such as payment system specific operations, will not be part of this joint effort.

P. 2

EXEC VISA LAB:28 55, 92 P35  
SEP 26 1992

STT specifications are being jointly released by Visa and Microsoft and will be supported by MasterCard. Comments from software developers and others will be received over the next 30 days and Microsoft, MasterCard and Visa will work to ensure that these open specifications are robust enough to satisfy the needs of the software industry.

669 5555

649

Exhibit 9

EXHIBIT 9



RECEIVED

SEP 28 1995

William J. Moore

September 27, 1995

Dear Member:

There is no question that the Internet is having a profound impact on the financial services industry. Today, more and more financial institutions are developing Web sites to increase their presence on the Internet. Merchants are also looking to take advantage of the electronic commerce opportunities provided by on-line shopping systems. These trends indicate that the marketplace is "in-tune" with today's savvy consumers who demand convenience and who look to technology to improve their lives. And while the potential for electronic commerce is staggering, the key issue is confidence. Consumers must believe the service will work and that they will be protected from the threat of fraud.

Recognizing that security poses the greatest obstacle to the emergence of electronic commerce, last November, Visa and Microsoft announced their intentions to jointly develop a standard, convenient and secure method for executing electronic bankcard transactions across global public and private networks. Since that time, we've been working diligently to develop a secure technology solution that will expand the market for electronic commerce by providing new opportunities for Visa Members and their cardholders and merchants.

I want you to be among the first to know that we have achieved our goal! Today, Visa is pleased to announce that our secure transaction technology is ready and available as a specification for the financial services and software industries. This technology protects account numbers on open networks and it authenticates buyers and sellers — assuring consumers that merchants are legitimate and validating the identity of consumers to merchants. To encourage the widespread adoption and usage of our published specification, it will be available on the Visa and Microsoft home pages on the Internet. (Visa is located on the worldwide web at: <http://www.visa.com>).

Through a unique registration process that incorporates authentication and encryption technology that protects the message flow, we can offer a fast, reliable and secure transaction method; a new channel for card usage; and another opportunity for revenues and profitability. We also protect your investment in the Visa franchise, protecting the brand and instilling confidence in your cardholders.

VISA U.S.A. INC. • Post Office Box 4000 • San Francisco • California 94128-5000 • (415) 432-1220

September 27, 1995  
Page Two

Other technologies in the marketplace to secure transactions have encountered problems. We are confident and excited about the progress we've made with Microsoft that offers safety for your cardholders while minimizing your risk.

To further explain our progress, I am enclosing materials for your review. These include an executive summary, a primer and the news release. In addition, your Visa account executive is prepared to answer questions and demonstrate how this new technology standard will be of value to your business.

Thank you for your confidence in our efforts.

Sincerely,



Carl F. Pascarella  
President and Chief Executive Officer





## NEWS RELEASE

---

Contact: Microsoft  
Mike Jackman  
Waggener Edstrom  
415/388-3216  
mikej@wagged.com

Visa  
David Melancon  
415/432-2427  
melancon@visa.com

### VISA AND MICROSOFT PUBLISH OPEN SPECIFICATION TO ENABLE SECURE TRANSACTIONS ON THE INTERNET

NEW YORK, September 27, 1995 – Microsoft Corporation and Visa International announced today publication of a specification to secure payments over public and private networks. The announcement, made simultaneously here and at NetWorld + InterOp in Atlanta, is the result of almost a year of joint effort between the two companies.

The open specification, known as Secure Transaction Technology (STT), is designed to provide a secure method for handling payment card transactions across electronic networks, such as the Internet. Built as an electronic version of the payment card system used today, STT extends the current transaction security and convenience advantages to the electronic commerce market. By providing a technology that is completely integrated with the current bankcard system, STT will serve as a reliable payment system for software providers to incorporate in their products.

To encourage widespread adoption of STT, Microsoft and Visa are making the specification available at no charge to all card brands, financial institutions, software developers and the Internet community to create STT-compliant applications.

-more-

VISA INTERNATIONAL Post Office Box 8000 San Francisco, California 94128-8000 (415) 570-3200 Telex 8771373



STT  
QUESTIONS & ANSWERS

FOR RESPONSE ONLY

**Q:** What exactly is STT -- is it only a specification or is it software being developed by Microsoft?

**A:** Secure Transaction Technology (STT) is a specification which provides the foundation for security and authentication for bankcard transactions over open networks such as the Internet. The specification is available to any software developer to use. Microsoft and other software developers will design and introduce proprietary software based on STT.

**Q:** Are Visa and Microsoft working jointly on software?

**A:** Visa and Microsoft have worked jointly on developing the STT standard, with each company bringing expertise in it's core competencies to the collaboration. In developing software applications that use this technology standard, Microsoft is building software for both consumers and merchants -- beyond working on the specification, Visa is not involved in this part of the development.

In developing software for the payment server and the credential authority server -- both key elements to enabling electronic commerce -- Visa and Microsoft are collaborating.

**Q:** This specification is an open one -- what exactly does that mean?

**A:** The specification is open to the public and available to any software developer -- free of charge -- who wishes to use it to develop their own security solutions. To further define what we mean by "open," we mean that any competent programmer should be able to program software compliant to the specification without requiring Microsoft or Visa proprietary technology.

**Q:** Why do an open specification -- why not make it proprietary?

**A:** The fastest, easiest and safest way to build an electronic commerce market is to have one secure payment standard for all to use. Visa and Microsoft have been working together for almost a year to build a foundation for that payment standard. In the spirit of openness that characterizes the Internet -- and for the good of the industry -- we want STT to be available to all to use for this purpose.

**Q:** Why are Microsoft and Visa interested in "the good of the industry"?

**A:** Protecting the good of the industry means protecting our brand. The possibility for excessive fraud means a denigration of the Visa brand. Consumers and merchants expect a high level of security and quality whenever they use or accept a Visa card and it's our responsibility to protect that trust. By protecting our brand in this manner, we are also

protecting the industry. Additionally, the "good of the industry" is served by providing a catalyst for the electronic commerce marketplace that will increase competition and ensure realization of the enormous potential of this market.

**Q:** If it's openly available, doesn't that mean that hackers will be able to break it? How do you protect against that?

**A:** The fact that the specification is openly available has no effect on whether or not hackers will be able to break it. The STT spec is merely the foundation on which security applications can be built -- the actual security features are in the form of public and private keys.

No security system can be absolutely foolproof against criminals determined to break in -- just as no lock or key in the physical world is absolutely foolproof. Anyone who claims that a specification or system is foolproof is speaking rashly. A security specification must be sound, reliable and as foolproof as possible -- which STT is. We will remain alert to the threat of criminals and hackers and continue to enhance the security of our specification as necessary -- as we do for all Visa systems today.

**Q:** How will STT be made available?

**A:** The specification will be available to download from either the Microsoft ([www:/microsoft.com](http://www:/microsoft.com)) or the Visa ([www:/visa.com](http://www:/visa.com)) website.

**Q:** What will it cost for software developers?

**A:** The specification will be provided free of charge to all. Software developers will then differentiate their offerings by wrapping value-added services around the basic security specification.

**Q:** What will it cost for merchants?

**A:** Merchants will be able to buy software based on this technology from any software developers who choose to use it. The price for this software will be set by the individual software vendor. The specification will be provided free of charge.

**Q:** What will it cost for consumers?

**A:** Consumers will be able to buy software based on this technology from any software developers who choose to use it. The price for this software will be set by the individual software vendor. The specification will be provided free of charge.

**Q:** If this standard is open and free to everyone, how are Visa and Microsoft making money on this?

**A:** Visa is paying Microsoft for the development of STT. We are doing this through a usage-based fee that Visa -- and not Visa members -- is paying.

This fee pays Microsoft for the cost of the development of payment server and credential server software -- it is not sharing transaction fees. Visa realizes revenue by increased card usage and reduced fraud. Additionally, Visa protects its current revenue by aggressively protecting its brand.

- Q: When will consumers and merchants be able to use this?
- A: The specification will be available on-line or through the mail beginning today (Wednesday, September 27). Microsoft plans to release products based on STT by early next year and other software developers will be following suit.
- Q: Does this specification give Microsoft or Visa a competitive advantage in the electronic commerce marketplace?
- A: This specification is available for any software developer, payment card company, financial institution or other qualified user -- free of charge. After today, the marketplace will decide who makes the best use of it. Any competitive advantage Microsoft and Visa may have is a result of the lead time garnered from our year of joint work on the specification.
- Q: What exactly is the relationship between Visa and Microsoft?
- A: Visa and Microsoft have been working together for almost a year to develop a specification for secure transactions over open networks. This specification is being published today.
- Q: Are you working together on other projects besides STT?
- A: While there are no additional joint efforts between Microsoft and Visa for public announcement, both companies are always exploring ways to extend and expand their individual brands in a quickly evolving marketplace and are building alliances and relationships with many industry players. With that in mind, future joint efforts can not be ruled out.
- Q: Do you expect companies such as Netscape to use this technology?
- A: The specification is available for any software developer free of charge. We expect and hope that developers such as Netscape will adopt this technology, thereby helping to ensure the electronic commerce marketplace has one secure transaction standard.
- Q: Will this technology correct software flaws such as the one in the Netscape browser disclosed earlier this week in *The New York Times*?
- A: Unfortunately, no security system can be absolutely foolproof against criminals determined to break in -- just as no lock or key in the physical world is absolutely foolproof. Anyone who claims that a specification or system is foolproof is speaking rashly. A security specification must be sound, reliable and as foolproof as possible -- which STT is. We will remain alert to the threat of criminals and hackers and continue to

enhance the security of our specification as necessary -- as we do for all Visa systems today. (IF PRESSED TO BE SPECIFIC ABOUT NETSCAPE FLAW: I really can't comment further on the Netscape issue -- you should probably address your questions to someone at Netscape.)

TO BE USED IF MASTERCARD IS NOT PARTICIPATING:

- Q: Where is MasterCard in this announcement? Doesn't Visa already have an agreement with them to develop secure transaction technology?
- A: We have been working with MasterCard since May to pursue their participation in the development and release of this specification. We have every hope that MasterCard and other payment card companies will use this specification, ensuring that the electronic commerce marketplace has one secure transaction standard.

## SECURE TRANSACTION TECHNOLOGY

### Executive Summary

#### Introduction

An explosion of commerce will take place over the Internet in the near future. It is coming through the home computer, as consumers and business people learn more and more about how to use the Internet. In this new "wired world" the possibilities for electronic commerce are clear and compelling.

Consumer research confirms that the number of consumers who plan to purchase goods and services on-line grows continually. And, as the availability of goods and services increases, bankcard payment will be the easiest choice for these consumers. They will be able to pay with the swift click of a computer key stroke, which is appealingly simple and convenient.

But, if the potential for electronic commerce is so obvious, why hasn't it really taken off yet? There are three major reasons. For one, it is only recently that the necessary personal computer and network technologies have been readily available and affordable to consumers. Secondly, the availability of desirable goods and services has been limited, but that is changing, too. And, third, there hasn't been a readily-available way for consumers to safely pay using their bankcards over open computer networks, including the Internet.

That's about to change because Visa and Microsoft have developed an open specification for protecting bankcards on any type of network. This specification is called Secure Transaction Technology, or STT for short. Visa and Microsoft have been working on the STT specification for nearly a year and have just released it as an open specification to member financial institutions, software developers, and other interested parties.

STT isn't a product Visa is trying to sell. Rather, it is an enabling technology that other companies can easily incorporate into their own software for buying or selling in cyberspace. This effort should provide a foundation for a new, widely-accepted standard to aid the growth of an emerging industry. By employing sophisticated cryptographic techniques, it will make cyberspace a safe place for doing business.

Visa plans to use STT as a foundation to develop services that will ensure Visa remains the payment brand of choice on the Internet, as it is today at most other points of sale. Through these efforts, the expectations by cardholders and merchants of a Visa-branded payment will be met.

### Secure Transaction Technology - What is it?

The Secure Transaction Technology focuses on three major goals: maintaining confidentiality of information, ensuring message integrity, and authenticating the parties involved in a transaction. Software developers will use these open specifications to develop products that meet its requirements, without having to use proprietary technology from Microsoft. It does, however, require the use of patented cryptography from RSA Data Security, Inc. This will ensure that cardholder software from one company will be able to talk safely to merchant software provided by another software company.

STT describes how payment and ordering messages are exchanged between buyer and seller, the content of those messages, and the cryptographic techniques used to protect them. It also describes the messages between the merchant and its Acquiring bank for each transaction and between the cardholder and his Issuing bank to establish a one-time "permission to shop."

It is important to understand that STT is not a product, but simply an enabling technology for assuring the safety of bankcard purchases over computer networks such as the Internet. However, it is convenient to refer to STT as providing benefits, which will actually be realized by the software products themselves. Please keep this in mind as you read more about STT.

### How does STT work?

Since the Visa card does not directly participate in electronic commerce transactions, STT enables the cardholder and merchants to take on new roles, which are necessary for Visa to be able to ensure secure processing of Visa card transactions. Following is a brief description of how a cardholder and a merchant will handle the ordering and payment processes using software following the STT specification.

#### 1. Cardholders and Merchants obtain credentials

In order to shop safely over open networks, cardholders must request that their issuer provide them with permission to use their card number. Issuers (or Visa, on behalf of the Issuer) will validate not only that a Visa account number is in good standing, but will also request corroborating information from a cardholder to ensure that the requester is who they say they are. This validation is completed with the issuance of a shopping credential to the cardholder. This one-time activity is much like the telephone call made by cardholders when they receive a new card in the mail. Issuers want to be certain that the card was received by the party it was sent to.



The credential is a set of electronic information, containing cryptographic keys and other data, that is saved by the cardholder's software for later use every time the cardholder shops using his computer. It also contains the electronic "signature" of both the Issuing bank and of Visa. This credential will allow a merchant to know that the cardholder's card number is able to participate in an STT transaction and will ensure that Visa is able to validate the safety of the card number. A cardholder will obtain a separate credential for each card he wishes to use for STT electronic commerce.

Merchants will also request a credential from their Acquiring bank (or Visa, on behalf of the Acquirer). After appropriate validation, the merchant receives an electronic credential, "signed" by both the Acquirer and Visa, that will be stored the merchant's computer. It allows the cardholder's STT-compliant software to know that the merchant is certified to accept STT transactions, and that the merchant is authorized by the Acquirer to accept Visa card numbers for payment.

## 2. Cardholders and merchants conduct a shopping dialog

Cardholders with credentials can now shop, using STT, at merchants with credentials. Once the decision to buy is made by the cardholder, the merchant sends an order form together with his merchant credential. The cardholder selects a bankcard and sends the related credential when he or she makes an order. That order is marked by the cardholder's software in such a way that the merchant can be certain it was not read or altered along the way.

When the cardholder decides to commit to a purchase, payment instructions are created by the cardholder software and sent to the merchant. They are fully encrypted using public key cryptography in such a way that the merchant cannot see the bankcard information until the acquirer decrypts it.

Although the cardholder and merchant computers play a major role in processing the cryptography, it is not noticeable to either party.

## 3. Authorization and settlement

Once the purchase and payment information has been safely received, the Acquirer requests an authorization from the Issuer, using VisaNet, just as with mail and phone order transactions. STT ensures that the card number arrives safely at the Acquirer, who is responsible for decrypting the payment instruction. Once authorized, the merchant confirms the sale to the cardholder. Clearing and settlement take place as they do for today's bankcard transactions.

### STT Software Components

The STT specifications require four separate software components:

Cardholder software includes public key technology necessary to secure a goods or services order and a related payment instruction across an open network. It also supports the cardholder's registration of his or her bankcards with Issuing banks, and stores the resulting credentials on the cardholder's personal computer. Cardholders will find that this software is included in a shopping application program, a network browser, or even an operating system.

Merchant software includes the public key technology required to communicate securely with both cardholder and acquirer software. It also supports the process of requesting and storing credentials. Merchants will find that STT-compliant merchant software will be included as part of offerings provided by firms or network providers who can aid in setting merchants up to sell over the Internet or on other networks.

Credential server software allows Visa to issue credentials to Issuers and to Acquirers who wish to offer STT-based electronic services to merchants. This server will also issue credentials to cardholders and merchants. Visa will operate credential issuing technology on behalf of its Members, although Members will also be able to operate their own credential servers.

Payment server software performs the decryption of payment instructions from cardholders. It also supports the process for a merchant's credential request. Visa will provide payment server technology to Members, much as it provides VisaNet Access Point technology today.

### Role of Microsoft in Developing STT-compliant Software

There has been confusion resulting from Microsoft's dual role as Visa's partner in creating the STT specifications and as a supplier to Visa of STT software.

Microsoft is developing cardholder and merchant software that are STT compliant, but the software purchase price will be established by Microsoft and paid for by the cardholders and the merchants. The openness of STT ensures that other software developers will also be able to build STT compliant software without the use of any Microsoft technology.

Microsoft is also developing server software for Visa. In order to have a credential issuing service available for the pilots, Visa has asked Microsoft to

build a credential server for that purpose. It is expected that, as the demand for such a service grows, Visa will either develop its own server or use one built to our specifications by a third party.

In addition, Microsoft is developing payment server software for Visa to supply to our Members to initiate STT. As with the credential server, it is anticipated that Visa will develop an enhanced version in the future.

For developing the two servers, Visa is paying Microsoft a software development fee. That fee, which continues only as long as Visa continues to use the software, will not begin to be paid to Microsoft until the payment server software is used for "live" bankcard payments. This arrangement strongly encourages Microsoft to ensure that both cardholder and merchant software are widely distributed. The fee, paid by Visa, is based on the transaction value as passed through the payment server. Visa expects that this cost, which will amount to less than \$2 million over the next two years, is entirely appropriate for the development work that Microsoft will deliver to Visa this year.

#### STT Member Pilots

A limited number of pilot tests will take place prior to the establishment of a STT-based electronic commerce payment service. As has been done in the past to accommodate Visa card payments from new points of transaction, interim payment service rules will be established to support these pilots. These rules will only apply to electronic commerce transactions that are secured through cardholder and merchant software that fully complies with the STT specifications.

The pilot period will extend until October 1, 1996. While current fees for card-not-present transactions apply, applicable interchange reimbursement fees will be reevaluated before then. It is expected that, when compared to today's best card-not-present transactions, both Issuers and Acquirers will see areas of significant cost savings, particularly in the areas of reduced fraud and fewer chargebacks. STT could significantly reduce merchant fraud costs. Once a substantial number of cardholders are able to participate in a STT-based secure transaction, electronic commerce merchants will be expected to participate as well.

### Conclusion

Secure Transaction Technology (STT) is an enabling vehicle for assuring the safety of bankcard purchases over computer networks such as the Internet. It works with all kinds of software and hardware, with no preference for any particular company's products.

STT will provide a vital utility to banks and merchants that seek to establish a presence in the on-line world. And STT does not in any way restrict the endless possibilities for software that facilitates electronic commerce. It won't hinder banks or merchants from finding their own ways of competing in cyberspace, whether by offering innovative products and services or just by creating a distinctive look to the custom-made software that the consumer sees on his personal computer. Moreover, STT directly provides cardholders with a safe way of doing business over the Internet, alleviating that major concern.

Visa hopes to establish Secure Transaction Technology as a new standard for electronic commerce, eliminating a major barrier to the growth and prosperity of a truly exciting new medium.



# Securing the 'Net: An STT Primer

Visa International  
September 1995

UNCLASSIFIED//FOR OFFICIAL USE ONLY



**INTRODUCTION:  
THE PROMISE OF  
ELECTRONIC COMMERCE**

Electronic commerce is coming to the home consumer. Not in five years or ten years, but ~~now~~. And not only for the trendiest "techie," but for the everyday person. Every bank will be affected. Every merchant. Every consumer.

The PC has become an essential part of daily life for tens of millions of people. More than one-third of American families have PCs at home. Virtually all new PCs are sold with modems for hooking up to the phone lines and exchanging information with other computers. Popular services such as America Online, CompuServe, and Prodigy, which make it easier for people to enjoy the benefits of computer networks, have already attracted millions of subscribers. And more than 30 million people worldwide are hooked up to the Internet, a sort of super-network that connects literally tens of thousands of smaller computer networks around the world.

In this new wired world, the possibilities for electronic commerce are clear and compelling. More and more, people will want to browse for merchandise "on-line." They'll use their PCs to shop around for loans or insurance policies. They'll buy all kinds of things. And they'll pay with the swift click

of a mouse, which is appealingly simple, immediate, and convenient.

If the potential for electronic commerce is so obvious, why hasn't it really taken off yet?

One thing has gotten in the way up to now. There hasn't been a readily-available, fool-proof way of preventing fraud and theft when people give out their bankcard account numbers or other sensitive financial and personal information over certain kinds of computer networks, such as the Internet. A way of creating an atmosphere of trust for both consumers and merchants.

That's about to change.

In this primer, we'll talk about a solution devised through a collaboration of Visa International and Microsoft. It's called Secure Transaction Technology, or STT. We'll explain why it's needed, how it works, and what it means — for banks, merchants, customers.

**This isn't a product...It is an enabling technology that banks and other companies can incorporate in their own software...**

This isn't a product that Visa or Microsoft are trying to sell. Rather, it is an enabling technology that

banks and other companies can easily incorporate in their own software that they create for their forays in cyberspace. It will help them compete in their own ways, no matter how they decide to enter the burgeoning electronic marketplace.

Secure Transaction Technology is an effort to

**VISA**

set a new, widely-accepted standard to aid the growth of an emerging industry.

It will make cyberspace a truly safe place for doing business.

The trail, which is traced in all that gobbledygook that gets attached to your message as a header or footnote, can be long and circuitous. It's all part of the Internet's highly decentralized setup.

**WHY DO COMPUTER NETWORKS NEED TO BE SAFER FOR COMMERCE?**

As the Internet spreads, the media is calling attention to a glaring problem — privacy. Up to now, there have been no real safeguards to ensure that the messages you send and receive haven't been intercepted, read, or even altered by some unknown interloper.

It's one thing for a corporation to guard its internal electronic mail from outside prowlers, since the organization operates its own computer systems. But no one really runs or controls the Internet, which is an unwieldy agglomeration, a patchwork of thousands of computer networks spread around the world.

Let's say you work for a company and you want to send an electronic mail message over the Internet to someone at another company. Your message isn't transmitted directly, as if you were dialing a direct phone call, point-to-point. Rather, the mail could be bounced around from one computer network to another. It might get routed to a nearby university's computers, which send it on to a military base, which then pass it along to a government agency or another private firm before it reaches its final destination.

The problem is that a lot of unseen people along that zig-zagging, indirect, "pass-along" route could possibly get their hands on your private e-mail. And you have no way of knowing for sure whether someone has read your messages — or changed them.

Of course, unwanted eavesdropping has long been something

of a problem for voice telephone callers, who occasionally have troubles with so-called "hackers."

But in the emerging realm of cyberspace, the potential for fraud and deception is far greater.

**When the other person is merely a blip on a computer screen, how do you know that he holds a valid account?**

When confidential information is converted into the 1s and 0s of digital communication, then it's possible for criminals to exploit the power of computers to sort through that data with frightening speed and efficiency. In essence, fraud can become automated, accelerated, and its incidence increased dramatically. For instance, special electronic "filters" can pick out bankcard account numbers out of a long stream of data traveling across a computer network.

**VISA**

So far, we've talked only about the Internet, but these same problems can exist on many other types of computer networks, especially if those networks rely on commonly-used phone links rather than communications lines specially geared for high security.

For instance, wireless technologies enable people to send and receive information from all kinds of portable devices, whether cellular phones or pagers, laptop computers or other kinds of hand-held computing devices. But wireless messages are prone to eavesdropping, as cellular phone customers ranging from President Clinton to Prince Charles have learned from personal experience.

There are other barriers to the widespread acceptance of electronic commerce in today's world. Many of the greatest advantages of banking and shopping in cyberspace also hold potential pitfalls that need to be addressed in a decisive way.

Let's take one advantage as a case study: More and more, computer networks will liberate people from the age-old constrictions of time and place. PCs can tap into information around the clock, from virtually anywhere in the world. Commerce can proceed apace without the need to bring people face-to-face in the physical space of the "real world."

While many people will perceive this as a great benefit, it has some practical drawbacks.

When the other person is merely a blip on a computer screen, how do you know that he holds a valid account? How do consumers know they can trust a merchant they've never actually seen, whose

"store" may exist only on the disk drive of a computer in some unknown location? How can the merchant feel comfortable accepting a bankcard number without seeing the actual

card, with its holographic image, in the hand of a real live customer?

For electronic commerce to flourish, all parties need a way of verifying each other's identities — and establishing trust.

Secure Transaction Technology addresses all of these issues by promoting a set of solutions — and by aiding the creation of software by companies that are gearing up to compete in this new market.

This is how:

**THE KEY TO SECURITY IN AN ELECTRONIC WORLD**

What's the most effective way to make a message safe from nefarious snoops? Simple. Put it in code.

Although to many people this might sound a bit like the stuff of spy novels, electronic commerce will rely heavily on cryptography, the art of secret codes.

**Secure Transaction Technology addresses all of these issues by promoting a set of solutions**



**VISA**

Cryptography has been around for centuries, of course, and played an important role in influencing the tides of history. In World War II, for example, breaking codes helped the Allies deceive the Axis forces about the location of the D-Day landing.

Since then, the advent of fast, powerful, inexpensive computers, which can make literally millions of mathematical calculations in a second, has revolutionized cryptography. In a mere instant, the ordinary, off-the-shelf PC on your desk or in your home can generate codes that the world's most expensive supercomputer would take years to crack. (Assuming you have the right software, that is).

Banks have long used cryptography as one way of helping protect their electronic transfers with other financial institutions. That same kind of technology has already come to everyday consumers, who now own their own PCs. These inexpensive computers, despite their diminutive size, are just as powerful as the lumbering old mainframes that cost millions of dollars and took up entire rooms.

There are two main kinds of cryptography in common use today. The older and simpler one is called "single key" or "secret key" cryptography. In its crudest form, this is the kind of code-making that most people are familiar with (and may even have tried for fun).

The message is converted into code using a so-called "key," which is a metaphor for a particular method of translating the characters into other characters that make no sense to the uninvited interceptor. This process is "en-

crypting" a message. A very simplified example: the key might be replacing each letter

with next letter in the alphabet, so VISA would become WJTB. To decipher the message, or "decrypt" it, the recipient simply needs to know the secret key.

Of course, in actual practice, the keys are far more complex. One real-world example: financial institutions use this form of cryptography to protect the transmission of personal identification numbers (PINs).

Although single-key encryption is useful in many cases, it has significant limitations. Both parties must know each other in advance, trust each other completely, and already have in their possession a copy of the key — a copy that has been carefully protected from the eyes of others. The single-key method is no good if you want to send a secure message to someone you've never met before, for instance.

On its own, then, this kind of encryption isn't enough to realize the full potential of electronic commerce, which must bring together countless buyers and sellers from around the world. For one thing, it's impractical for a big corporation to exchange keys with thousands or even millions of customers — or, worse yet, potential customers they've never dealt with before. And there's no completely safe way to transfer the keys, anyway, and certainly not over networks like the Internet.

**The two keys work together as an intriguing kind of matched set...**

# VISA

The solution is a newer, more sophisticated form of codemaking, first developed by mathematicians at MIT in the 1970s, known as "public key." In this approach, each participant creates two unique keys. You would have your own "public key," which you publish in a sort of directory available to all, as well as your own "private key," which you make sure to keep secret from everyone.

The two keys work together as an intriguing kind of matched set. Whatever one of the keys "locks," only the other can unlock.

So, let's say that you want to send a snoop-proof message to a friend. You simply look up his public key and then use that key to encrypt your text. Later, when your friend receives the e-mail, he takes his private key and converts the gibberish on his computer screen back to your original message in clear, elegant English.

Even if a would-be criminal intercepts the message on its way to your pal, the bad guy has no way of deciphering it. The code is much too hard to break, even with the most sophisticated computers.

To be sure, the "keys" in these examples are merely metaphors. In reality, they exist as series of electronic signals stored on the disk drives of personal computers or transmitted as

...Whatever one of the keys "locks," only the other can unlock.

blips of sound over phone lines. The really hard work —

the dazzlingly complex math of encrypting and decrypting messages — is handled by the computer, which shields the person from all the messy complexities. To the real, live individual, the process of sending coded messages will be simple, just as it is with PINs at Automated Teller Machines.

Banks, merchants, and other participants in the new world of electronic commerce will be able to tailor the "look and feel" and other vital features of the software that their customers actually use to do business with them. Underlying this software, operating "behind the scenes," will be a layer of software code that conforms to the Secure Transaction Technology specifications. This layer will employ public-key encryption to ensure that messages containing bankcard numbers and other information are strictly confidential.

Aside from scrambling data, cryptography will play another essential role in the field of electronic commerce. It will help buyers and sellers make sure that the other party is whom they claim to be.

In cyberspace, this can be a real problem. When you receive a message, how do you know it was sent by your friend Bob rather than a malicious criminal who's pretending to be Bob? And how does a merchant know that an order is coming from you rather than some nefarious hacker out to defraud them of a lot of money?

There's even a relatively new slang term for this alarming phenomenon. Impersonating someone online is called "spoofing."

**VISA**

Fortuitously, the public-key system can address this problem in a simple and highly reassuring way. Let's say that I'm talking to my bank — in cyberspace, that is — and I want to prove to them that I'm, well, me. I simply lock a message with my private key. Then, the bank can unlock the text with my public key, proving that I was the only person who could have locked up the message in the first place.

This process creates what cryptographers call a "digital signature" — an effective way to verify someone's identity. Actually it's much harder to forge than a real, handwritten signature on a personal check, say, since the digital version takes advantage of highly sophisticated mathematics and the full power of computers.

Secure Transaction Technology takes this concept one step further. Again, an analogy to "real life" (or RL is cyberspeak) might be useful here. In the physical world, a merchant can look at and inspect a would-be customer's Visa card, checking the holographic image, for instance, to ascertain that it is a real Visa and not a forged imitation. And the consumer can spot the Visa decal on the store's window, which provides reassurance that the merchant has a working relationship with the bankcard association.

In the electronic world, Visa and Microsoft will use the power of cryptography to provide the same kind of reassurances.

Visa will put its own digital signature on an electronic representation of the bankcard, which will contain the same information that's on the actual piece of plastic — the customer's name, account number and the card's expiration date. The digital version will actually be harder to forge than the real one.

Similarly, Visa will put its digital signature on an electronic substitute for the merchant's store-window decal. Thus, customers will have an easy, foolproof way of knowing that they are doing business with a real merchant and not a false front in cyberspace.

**HOW A TYPICAL TRANSACTION WORKS**

The cardholder, merchant, issuer, acquirer, and Visa all have simple and clearly-defined roles to play in a transaction using STT.

**Visa will put its own digital signature on an electronic representation of the bankcard...**

To begin, cardholders must register their account with Visa. The consumer simply fills out a form

on the PC screen with basic information — name, account number, expiration date, billing address, and whatever else is needed for purposes of identification. All this information is encrypted and sent over to Visa's computers.

Visa checks with the bankcard issuer to make sure the account is authentic. Then it issues a kind of electronic credential by putting its

**VISA**

digital signature on the cardholder's public key. This credential proves the card is valid. The cardholder stores it on his PC for future use.

Similarly, merchants will have to register with Visa to use Secure Transaction Technology. They'll simply fill out basic information on the PC screen, including their merchant IDs. Visa checks with the Acquirer, then gives its credential to the merchant.

Now we're ready to describe the steps of an actual transaction. First, the merchant needs to show the customer its Visa credentials. The merchant can do this in variety of ways, such as sending a copy to the cardholder by electronic mail, for instance, or by publishing a copy on the Internet that anyone can easily inspect.

Seeing that the merchant has Visa's approval, the cardholder begins shopping. Ready to make a purchase, he sends an order electronically to the merchant, who sends back an acknowledgement, asks for authorization from Visa for the dollar amount of the purchase, and then puts through the order and delivers the goods.

### CONCLUSION: SECURING THE 'NET

Secure Transaction Technology (STT) is an enabling technology for assuring the safety of bankcard purchases and other financial transactions over computer networks such as the Internet. It can be incorporated into all kinds

of software and hardware, with no preference for any particular company's products.

STT is a kind of under-the-hood technology. It will provide a vital utility to banks and merchants that seek to establish a presence in the on-line world. And STT does not in any way restrict the endless possibilities for software that facilitates electronic commerce. It won't hinder banks or merchants from finding their own ways of competing in cyberspace, whether by offering innovative products and services or by tailoring the distinctive "look and feel" of their custom-made software that the consumer sees on the PC monitor.

Visa and Microsoft hope to establish Secure Transaction Technology as a new standard for electronic commerce, eliminating a major barrier to the growth and prosperity of a truly exciting new medium. ♦

EXHIBIT 10



**Date**  
September 28, 1995

**To**  
Global and U.S. Region Board of Directors

**From**  
H. Eugene Lockhart

**Memorandum**

**Subject**  
Internet Specifications

**Copies to**

**Privileged & Confidential**

Summary

As you know, on June 23, MasterCard and Visa announced an agreement to work together to produce a universal, open standard for securing electronic commerce that would not advantage any single entity nor disadvantage any vendor. I have attached my letter to Ed Jensen on this commitment, his response, as well as the June 23 joint announcement.

Contrary to this agreement, yesterday Visa and Microsoft announced that they will jointly own and publish a specification called STT to secure payments over the Internet.

MasterCard did not participate in this announcement because:

- A. The Visa/Microsoft announcement violates our joint June 23 announcement to publish a jointly agreed upon open standard for the industry.
- B. The specifications published by Visa and Microsoft do not represent an open standard because
  1. they are incomplete and not programmable as they currently stand
  2. the software behind these specifications is still "owned" by Microsoft who remains in control of future changes to that software; this software will be licensed by Microsoft to banks and others with fees paid on a transaction basis.

MasterCard is disappointed by Visa's actions as we believe such standards should be open and create a level playing field for all our members and software suppliers. We have offered to continue our work with Visa, Microsoft, IBM, Netscape and others to create such an open standard. We remain in discussions with Visa on next steps.

Global and U.S. Regional Board of Directors  
Page 2  
September 28, 1995

### Background

On June 23, MasterCard and Visa announced that we would work together to produce open standards/specifications for the secure transmission of card transactions over the Internet. Based on this agreement, ourselves along with staff from Visa have been working with IBM, Netscape and others to develop an open standard for secure transmission of card transactions. Staff from both Visa and MasterCard played an active role in the development of the initial contents of the standard specifications. It had been our intention that this specification would be agreed to by Microsoft as well as Visa. This could then become the industry standard, open to all participants on a level playing field.

Instead, yesterday, Visa and Microsoft announced that they will jointly own and publish a specification called STT to secure payments over open networks such as the Internet. Apparently, concurrent with our efforts, Visa and Microsoft have been working on a proprietary basis for several months to develop this specification and software. Indeed, up until August 24, Visa regarded their standards work with Microsoft as "proprietary" and would not share the specifications with us. Over the last two weeks, MasterCard was invited to participate in this alliance, and in a good-faith effort to honor our commitment to Visa, we gave serious consideration to the opportunity.

After thorough review, we determined that the Visa/Microsoft specification is not currently open; meaning that any software vendor or financial institution cannot adequately write their own transaction-processing code from the document for purposes of interoperability. In other words, the document as it stands provides inadequate detail, and as such, is not something we are willing to support at this time. Please also note that while the specifications for STT have been made available, the software has not. Microsoft has been quite categorical with us that they own the intellectual property rights to the STT software and that they expect to license this software to banks and others. License fees would be paid to them on a transaction basis.

Last Friday, we were made aware of Microsoft's and Visa's intention to announce the STT specifications this Wednesday. Because we wanted to honor our agreement with Visa to develop a single, open specification for the industry to use, we proposed that Visa/Microsoft announcement be delayed by 1 month so the three companies could work together to match and complete the specifications so that the resulting standard would be open, non-proprietary and could be implemented by many software suppliers on a level-playing field basis.

Unfortunately, Visa and Microsoft decided not to agree with our proposal; rather, they gave us assurances that any issues we had with their document would be resolved at some unspecified later date. In essence, we were being asked to trust that after revisions, this specification would be open. In good business practice, we could not allow ourselves to base a major business decision on an act of faith.

MasterCard believes that any specification developed for the bankcard industry should not give preference to any one software provider, but should be open to all vendors to ensure that you have choice. For that reason, we are extremely disappointed that Visa and Microsoft have chosen to move forward in this manner.

Even so, our offer to work with Visa, Microsoft and other industry software suppliers to create a joint specification that is open to all vendors remains on the table. IBM, Netscape, CyberCash and others are supportive of this approach and are willing to actively participate.

In summary, we are disappointed that Visa has taken this step despite our best efforts. We remain convinced that member financial institutions, merchants and consumers would be better served by a common standard for security on the Internet, and we will not give up our efforts to

Global and U.S. Regional Board of Directors  
Page 3  
September 28, 1995

help the industry toward this direction. Be assured, however, that regardless of whether there is ultimately one standard or two, MasterCard will maintain excellent acceptance quality for electronic commerce on the Internet and all other electronic venues.

I have attached supplemental questions and answers which our staff is using to discuss this issue with our members.

Conclusion

Some of the newspapers today tried to portray this as "war of egos." For our part, this has nothing to do with ego; it's all about the development of common standards for the industry and ensuring that members stay in control of these developments.

We will continue to attempt to work with Visa to sort this out. We will keep you posted on these developments.

HEL/le

Attachments

MasterCard International  
888 Seventh Avenue  
New York, NY 10106  
212 649-5100  
Fax: 212 649-5510



August 1, 1995

H. Eugene Lockhart  
President and  
Chief Executive Officer

Mr. Edward P. Jensen  
President and Chief Executive Officer  
Visa International  
P.O. Box 8999  
San Francisco, CA 94128

Dear Ed:

I enjoyed the many matters we discussed last week and I continue to share your enthusiasm for the development of electronic commerce on the Internet. We will continue to have our Ed Hogan cooperate fully with your Dick Lonergan to reach a usable security standard.

However, there is one significant point that I believe needs to be clearly understood between ourselves. Ed Hogan assures me that the end product of the security effort will be a single document from the two associations that defines interoperability for interchange. That document will be vendor neutral to protocols such as Netscape's SSL or Microsoft's STT, and rather define what those protocols need do in order to comply with the bankcard standard.

Ed, could you please confirm that this is also your understanding of the goal of the effort. Again, I enjoyed our conversation and look forward to continuing it.

Sincerely,

A handwritten signature in cursive script, appearing to read "Gene".

HEL/le



7/28/95  
9/15/95



done ✓  
8/22/95

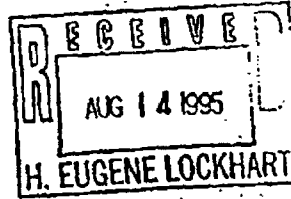
INTERNE

ccfy: to H. [VISA]  
file

Edmund P. Jensen  
President and  
Chief Executive Officer

August 15, 1995

Mr. H. Eugene Lockhart  
President and CEO  
MasterCard International  
888 Seventh Avenue  
New York, N.Y. 10106



Dear Gene:

Thank you for your August 1, 1995 letter.

As you requested, I can confirm that our understandings are mutual. A single document defining interoperability for interchange will be vendor neutral to protocols and define what those protocols need to do in order to comply with bankcard standards.

I am pleased that we can aggressively compete for member business while providing real value for members through common standards.

Sincerely,

VISA INTERNATIONAL Post Office Box 8909, San Francisco, California 94128-8909 (415) 432-3200 Facsimile (415) 432-8086



**Date**  
Oct. 5, 1995

**To**  
MasterCard Member Institutions Worldwide

**From**  
H. Eugene Lockhart

**Memorandum**

**Subject**  
A Draft Specification for On-line Bankcard Transactions

This week, MasterCard, IBM, Netscape, GTE and CyberCash published a draft specification for securing transactions over open systems like the Internet. I would like to take this opportunity to bring you up to date on the work that has taken place to produce a single, open industry specification.

In June we announced jointly with Visa that the two card associations would work together to develop one industry specification. We pursued this alliance because the development of electronic commerce is at a critical juncture:

- Consumer demand for secure access to electronic shopping and other services is very high;
- Merchants want simple, cost-effective methods for conducting electronic transactions;
- Financial institutions want secure, competitively priced, quality products designed to displace payments by cash and checks.

The next step to achieving secure, cost-effective on-line transactions at a rate fast enough to satisfy market demand, was the development of a single, open industry specification.

Last week Visa and Microsoft published their own specification called STT. Based on what we have seen, we cannot conclude that STT is open; meaning that any software vendor or financial institution cannot adequately write their own transaction-processing code from the document for purposes of interoperability.

We remain committed to achieving a single, open, non-proprietary standard for on-line transactions, and are continuing to follow the generally accepted process for developing a technical standard within an industry. This process is comprised of five key steps:

- Collaboration of interested parties;
- Preparation of the document;
- Availability of the document for comment;
- Modification of the document based on the comments;
- Publication of the document for implementation.

We are at the stage of making the document available for comment, and as such, this week published the draft specification on the Internet to encourage software companies, financial institutions and other interested entities to comment on the document.

Page 2  
A Draft Specification for On-line Bankcard Transactions

The draft specification -- called Secure Electronic Payment Protocol (SEPP) -- is open, vendor-neutral, non-proprietary and license-free. It is available for viewing on MasterCard Pointers, at <http://www.mastercard.com>. Also, we will mail SEPP to any member bank or other organization that wants it in printed form. Please also note that we have asked both Visa and Microsoft as well as others to comment on the specification.

Once interested parties have commented, SEPP will be modified, then published, free in the public domain. The specification will then be implemented by software companies, merchants and financial institutions, so that consumers will be able to perform secure transactions on the Internet beginning in April 1996.

We remain convinced that member financial institutions, merchants and consumers would be better served by one, common industry standard for security on the Internet. We will not give up our efforts to help the industry toward this direction.

Exhibit 12

## Memorandum

MasterCard  
International



To  
File

From  
Edward Hogan

Date  
November 27, 1995

Subject  
MasterCard/Visa Cooperation on the Internet

Copies to

Exhibit 9 is a member letter form Visa regarding the introduction of STT into the marketplace in cooperation with Microsoft. The announcement is relatively brief and advises that Visa and Microsoft have published an open specification that is available on their home pages on the Internet for the two companies. The emphasis is on the written specifications and implies that it is a finished product, sufficiently adequate to be characterized as an "open" specification. There is a large question and answer section attached to the announcement that is meant for staff to use in response only to questions about the announcement. Finally, there is an executive summary explaining STT.

My analysis of the announcement is as follows:

- The main emphasis of the announcement implies that the software specification provided is the foundation for security authentication for bankcard transactions over open networks such as the Internet. It clearly implies that the specification is adequate for all to use to create their own software. That is not the case as we believe anyone attempting to program from that specification will very quickly determine that there are many unknowns for which they need Microsoft assistance. Microsoft assistance will come in the form of a requirement to obtain their software rather than their assistance to write your own software. That software comes for a price, which is transaction related rather than resource related. By way of example the STT specification does not have any instructions as to what to do if one finds error conditions nor does it have any information as to the tools or system definitions needed to affect the programming. A specification that really wanted itself to be used by an industry would provide these kinds of information.

Exhibit 12

## Memorandum

*MasterCard  
International*



- In addition to Microsoft independently developing software applications for both consumers and merchants, both Visa and Microsoft are collaborating on developing acquirer software for a payment server and the credential authority server that are critically needed to make the specification work.
- While both Visa and Microsoft acknowledge that the fastest, easiest and safest way to build an electronic commerce market is to have one secure payment standard for all to use, they then proceed to characterize their cooperation as for the "good of the industry." They mainly ignore the reality of the commercial venture that the two have entered into to the disadvantage of all competition, including MasterCard and virtually all other vendors.
- They acknowledge in the question and answer that Visa is paying Microsoft for the development of STT through a usage based fee. They rationalize that fee because Microsoft need be reimbursed for the development of the payment server and credential server software. One has to assume that the only such Microsoft servers that will be allowed for Visa transactions is those provided by Microsoft.

This provides a major commercial advantage to Microsoft whereby they become virtually the software supplier for all Visa transactions on the Internet.

- They imply that they would like Netscape and other vendors to adopt STT as their standard for secure processing of transactions on the Internet. They say this despite the fact that know they are about to enter into guaranteed competition with those vendors as a result of their joint venture with Microsoft.
- In response to a question about MasterCard's absence in this announcement and questioning the fact that Visa already has an agreement with Visa to develop security on the Internet, they suggest that they have every hope that MasterCard and other payment card companies will use this specification to ensure a single secure transaction standard. They say this despite the fact that they clearly knew that we would characterize their activity as preemptive and proceed to introduce the SEPP, our own standard, with virtually the remainder of the vendor community.

Exhibit 12

## Memorandum

*MasterCard  
International*



- Throughout the executive summary Visa emphasizes that software developers will use their own specifications to develop products that meet their requirements without having to use the proprietary technology from Microsoft. They suggest that the openness of STT ensures that other software developers will also be able to build STT compliant software without the use of any Microsoft technology. The reality is that Microsoft is also providing cardholder/merchant software and is the exclusive provider of acquirer and credential software for Visa. The combination of this exclusive arrangement with Visa and competitive realities of the inadequacy of the software specification versus the use of Microsoft provided software at a fee, guarantee that the nature of the specification itself will have the effect of institutionalizing Microsoft software as the only realistic implementation of STT going forward.

Exhibit 12