ceBerg™

Innovative Solutions To Everyday Challenges

White Paper

Author: Lester Sussman
CEO
ceBerg, Inc.
ipAVS@ceberg.com

Internet Address Verification System (I-AVS)

Preventing Fraudulent Use Of Confidential And Private Information (Patented)

VERIFY

AND

TRUST

I-AVS verifies the registered, lawful physical location from which online parties transact business.

Executive Summary

Trust is at the heart of all successful transactions, including online commercial transactions, as well as other confidential online transactions.

It is therefore imperative to the continuing growth and success of the Internet as a viable marketplace, that all parties involved in an online transaction can be irrefutably verified as the lawful participants.

The patented Internet Address Verification System (I-AVS) provides this *trust between online transaction parties* ***by verifying the lawful, pre-registered physical location*** *from which they transact business*.

The I-AVS implements, to paraphrase a quote from Ronald Reagan: "**Verify And Trust**".

This system is much needed in the online world to counter the growing explosion of online fraud.

Introduction

The Internet Address Verification System (I-AVS) is a patented[1] business service for resolving the escalating problem of Internet security and fraud.

I-AVS can be expected to have at least the same market potential as other systems and tools for addressing the problem, including web site digital certificate issuers (Verisign, GTE CyberTrust, GlobalSign, etc.) and the various credit card verification services (Visa[2], MasterCard[3], American Express, etc.). This is because of the very growth of the Internet, its basic design features and the explosion of financial and personal profile data transferred over it [4].

There is a growing sense of crisis in the attacks on privacy, fraud, theft of personal information and criminal misuse of the web. Rarely a week goes by without TV and press news items about some identity theft, error by a credit card processor in releasing confidential information, or the prosecution of spam and phishing artists.

I-AVS is a simple and highly effective vehicle that operates on the following principles:

1. Automatic registration by a user of an online service for various confidential services including credit card purchases and access to restricted web sites.

[1] US Patent 6,560,320
[2] In 2004, "Visa's total volume surpassed $1 trillion..", Visa USA Annual Report 2004
[3] In 2004, MasterCard's purchase volume "grew to more than $1 trillion", MasterCard Inc. Annual Report 2004
[4] "Hacker Hunters", BusinessWeek, May 30, 2005

2. The registration data includes all of the physical locations where confidential online transactions will be transacted. These locations will typically include a consumer's home PC connection, or office PC connection.

3. Automatic activation of a real-time authentication check on the validity of where the user is executing a confidential online transaction.

4. Immediate authorization or preventive action.

I-AVS will be implemented as a trusted third party Internet service provider similar to the services that digital certificate providers, such as Verisign offers.

The distinctive advantage of I-AVS is even if private data falls into the hands of unauthorized users, it cannot be used fraudulently except at the registered physical locations that a lawful user authorizes for transacting confidential business on the Internet.

Online Confidentiality Challenges

The Internet is providing consumers, businesses and governments with a huge market opportunity.[5]

In 2004 identity theft cost US consumers between $50 billion and $60 billion.

Unfortunately this opportunity is accompanied by rising fraud threats to confidential information[6]. These confidential threats take a variety of forms including phishing, computer worms, social engineering of identity theft, as well as other threats.

In 2004 alone according to the US Federal Trade Commission, identity theft via phising and social engineering cost U.S. businesses and consumers between $50 billion and $60 billion. Banking activity accounts for 56% of the reported incidents.[7]

These thefts' costs and incidents are increasing every year, so much so, that U.S regulators have ordered banks to develop systems to quickly warn federal officials and customers of suspected incidents of identity theft.[8]

More and more Americans are increasingly using credit cards instead of cash.[9] In 2003, U.S consumers used credit cards to buy $2.2 trillion in goods and services – roughly 20% of the U.S GDP. This is matched by an increase of consumers[10] who purchase goods and services on the Internet. Therefore, it is close to certain that there will be a comparable increase in the volume of online fraud in the immediate future.[11]

[5] "Online Ad Dollars Set to Match, Then Go Ahead of Magazines'", The Wall Street Journal, July 27, 2004
[6] "Symantec Internet Security Threat Report Highlights Rise in Threats To Confidential Information", Symantec, March 21, 2005
[7] "Phishers Try To Reel In Small Businesses", InformationWeek, March 21, 2005
[8] "Fed orders U.S. banks to guard against ID theft", Reuters, March 23, 2005
[9] "As Cash Fades, America Becomes A Plastic Nation", The Wall Street Journal, July 23, 2004
[10] "Crowned at last", The Economist, April 2, 2005
[11] "IC3 2004 Internet Fraud – Crime Report", 2005, National White Collar Crime Center
[12] "Travel Manager's Lament", The New York Times, August 16, 2005
[13] "ATMs Highly Vulnerable to Fraud, Analysis Finds", USA Today, August 15, 2005
[14] "Verisign Unified Authentication", Verisign White Paper,
[15] "Banks Test ID Device for Online Security", The New York Times, December 24, 2004

It is important to note that not only is the credit card industry at risk here, but so are other businesses that rely on confidential web sites.

For example, in the managed business travel market, over 30% of all transactions now occurs on the Internet. This is a $30 Billion market [12].

Another reported example of a market at risk by online Identity Theft is the ATM (Automated Teller Machine) industry. It is reported that fraudulent ATM card information is obtained via phising on the Internet [13], which is then used to commit fraud at an ATM.

The Need for Better Online Authentication

> "*Even as business models and impressive advances in technology fuel industry's vision of the Internet as a dynamic medium for commerce and communication, security issues continue to weaken confidence in online business.* ***One of the most vexing and serious issues is related to identity verification.*** *If users and devices accessing the network are not properly identified, enterprises risk exposure to threats like fraud, phisihing, identity theft, IP spoofing, and denial-of-service attacks.*" [14]

"One of the most vexing and serious issues is related to identity verification.", Verisign White Paper

Various proposals require the use of an electronic token, e.g. that attaches to a key ring, to be used in conjunction with passwords, etc. when entering a commercial online transaction.[15] Use of this technology has been around for about twenty years, but it has never been broadly adopted in the marketplace. Such tools are cumbersome, easy to lose and incompatible with the basic principles of online services: convenience, seamless access and simplicity.

Other services provided to combat online Identity Fraud include;

- "Verified by Visa" and MasterCard SecureCode
- The Payment Card Industry (PCI) Data Security Standard
- Internet Address Geo-location verification
- Fraud Protection services by various online providers such as Verisign.

The problem with the "Verified by Visa" and MasterCard SecureCode is that these solutions are vulnerable to (a) phishing and (b) Trojan Horse malware (malicious software) such as keyboard loggers that record every keystroke that is entered on a computer, and which then sends that data to an Identity thief.

The PCI Data Security Standard should be implemented on all web sites, etc. that handle confidential information. Unfortunately, many companies and organizations do not implement this standard, as is revealed in the media almost every week.

The Geo-location address verification service is similar to I-AVS, except that is it limited in the level of its verification. Geo-location can only verify an Internet address to a city level. But, there are hundreds, if not thousands of ID thieves, for example in Manhattan, New York, Los Angeles, California, etc. Geo-location is insufficient to stop online ID Fraud.

A number of Internet companies, such as Verisign and RSA Security, offer a suite of anti-Fraud services. These suites are generally an amalgamation of the previously mentioned anti-online fraud services. Also included as an option in most of these suites, is a service that looks for patterns of purchasing behavior,

i.e. a software driven rules-based filtering process. American Express has long implemented such a service for its cardholders, even before the Internet took off commercially.

The table below highlights the above features of today's existing anti-Identity Fraud services on the Internet.

Immunity to ID Fraud	I-AVS	Secure-Code, etc.	Site Protection	Anti-Fraud Suite	Geo-location	Electronic Token
Phishing	√	x [1]	x	√	√ [1+2]	√
Trojan Horses	√	x [3]	x [3]	x [2 3]	√ [1+2]	√
Weak Data Protection	√	x	√	√	x	√
Con-Artists	√	x [1]	x [1]	x	√ [1+2]	√
Bin-Diving	√	√	x	x	x [2]	√
Stolen Wallet, etc.	√	√	x	x	x [2]	x
Credit Report Misuse	√	√	x	x	x [2]	√
Lost item, e.g. token, password, etc.	√	x	x	x	x [2]	x
Ease of Use	√	x	x	x	√	x

Table 1 Today's Anti-Identity Fraud Online Measures

Table 1 Notes:

[1] Susceptible to being hoaxed into giving confidential data
[2] Thief can still use proxies to simulate same city, state and country
[3] Key-loggers can capture and criminally share the SecureCode
√ Anti-Identity Fraud protection good
x None, or too little effect

Today, parties involved in an online commercial transaction usually execute the transaction from a fixed, physical location. For example, a consumer would use his bank to pay his bills online, either from home or from work. Phishing and other fraud techniques, such as keyboard logging, steal a user's online identity and then execute a fraudulent transaction at another location. It is extremely rare that the thief would execute the fraudulent online transaction at the location where the party normally transacts online business.

The patented system outlined in this paper, i.e. the Internet Address Verification System (I-AVS) greatly reduces the possibility for thieves to use stolen identity and credit card information at other online locations, which are not authorized by the lawful customer.

How Does The Patented Address Verification Work On The Internet?

The primary principal behind the Internet Address Verification System (I-AVS) is similar to the process that credit card companies use to activate and verify a consumer's credit card.

I-AVS is similar to the process that credit card companies use to activate and verify a consumer's credit card.

For example, when a consumer receives a new credit card, she must activate the card from a pre-registered telephone number, which is directly associated with her credit card's application. This is usually either the consumer's home phone number, or her work phone number. The credit card company uses a Touch-Tone® data entry system, combined with the telephone company's caller-id feature to verify, that the lawful owner of the card is verifying the credit card.

The consumer's telephone number's caller-id verifies the physical location from where the consumer is calling. This is central to the patented I-AVS solution, but is applied to the online parties using the Internet.

The Internet Service Provider's RADIUS Database

So, where does the caller-id feature come from on the Internet? Every customer connects to the Internet via an Internet Service Provider (ISP). Virtually all ISPs use a database system called RADIUS (Remote Authentication Dial In User Service) to authenticate, authorize and provide accounting information on its customers. Broadband ISPs also use RADIUS.

RADIUS[16] is an open Internet standard adopted by the Internet Engineering Task Force (IETF), which is responsible for the adoption and dissemination of all other protocols that currently make the Internet work universally.

User's physical location during an online transaction is central to I-AVS. RADIUS provides this information.

Table 1 illustrates a number of the key RADIUS data that are used by the I-AVS. As can be seen from the Table, RADIUS maintains information of, from where the customer is connecting to the Internet, which of the ISP's physical line numbers was called to connect to the Internet, as well as the status of the customer's online connection.

RADIUS Attribute	Description
`User-Name`	The name of the electronic commerce party
`Called-Station-ID`	The phone, or line number that the online party called to connect to the ISP.
`Calling-Station-ID`	The phone, or line number that the call came from.
`Acct-Status-Type`	Indicates whether this accounting request marks the beginning of the online service, or the end.
`Acct-Terminate-Cause`	Indicates how the session was terminated

Table 2 RADIUS Database Attributes Used in the I-AVS

At any given moment in time, the ISP's RADIUS database knows exactly who is connected to the Internet using its facilities, as well as the physical location from where the customer is electronically connected to its facilities.

[16] RADIUS, IETF RFC 2138 and RFC 2139 – www.ietf.org

I-AVS maintains its own secure database system that lists all online parties statuses, i.e. whether or not they are currently logged onto the Internet, as well as the physical location of the various online parties.

Information is securely shared between the ISP and the I-AVS Service Provider.

The Relationship Between The ISP And The I-AVS Service Provider

Figure 1 illustrates the sharing of data between an ISP and the Internet Address Verification System (I-AVS) Service Provider.

Whenever a customer, or merchant connects to the Internet, the ISP provides the relevant RADIUS data to the I-AVS.

The I-AVS maintains its own secure database system that lists all online parties (e.g. the customer and online merchant) statuses, i.e. whether or not they are currently logged onto the Internet, as well as the physical location of the various online parties. Whenever the status of the online party changes, for example they log off from the Internet or their connection is inactive, then this change is provided by the ISP to the I-AVS database. Hence at all times, the precise status of all participating online parties is tracked in the I-AVS database.

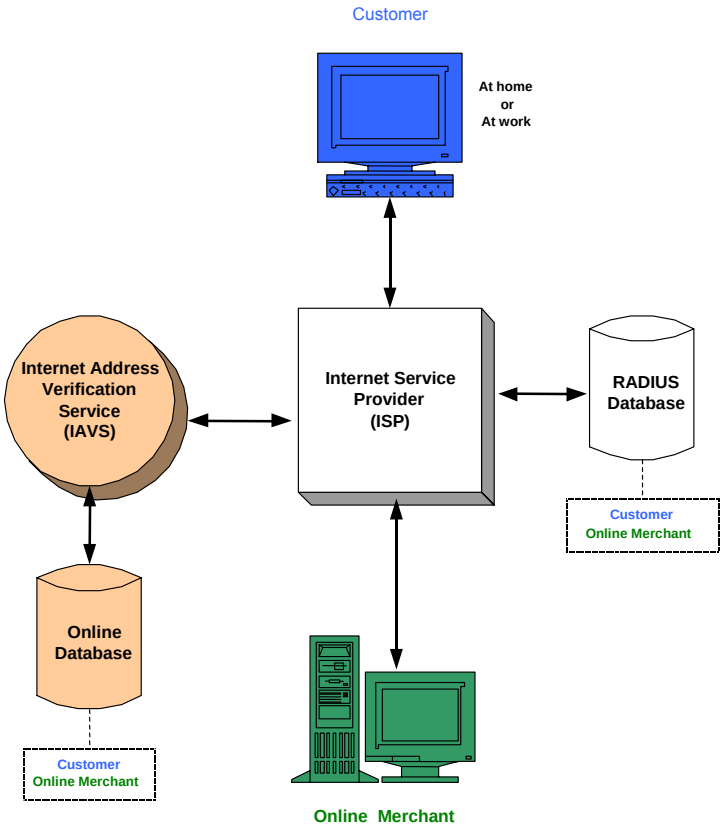

Figure 1: Internet Address Verification System's Core Components

The sharing of the information between the ISP and the I-AVS Service Provider is secure. For example, use of Digital Certificates[17] and SSL link encryption is used. The Digital Certificates prevent fraudulent connections to the I-AVS, for example, by thieves pretending to be an ISP. SSL is a standard technique used on the Internet to ensure that only the online parties have visibility to the data transmitted between them.

[17] "Applied Cryptography", Bruce Schneier

Secure online relationship between participating ISPs, banks and other organizations with the I-AVS Service Provider

Figure 2 illustrates the situation in which multiple ISPs participate in the Internet Address Verification System.

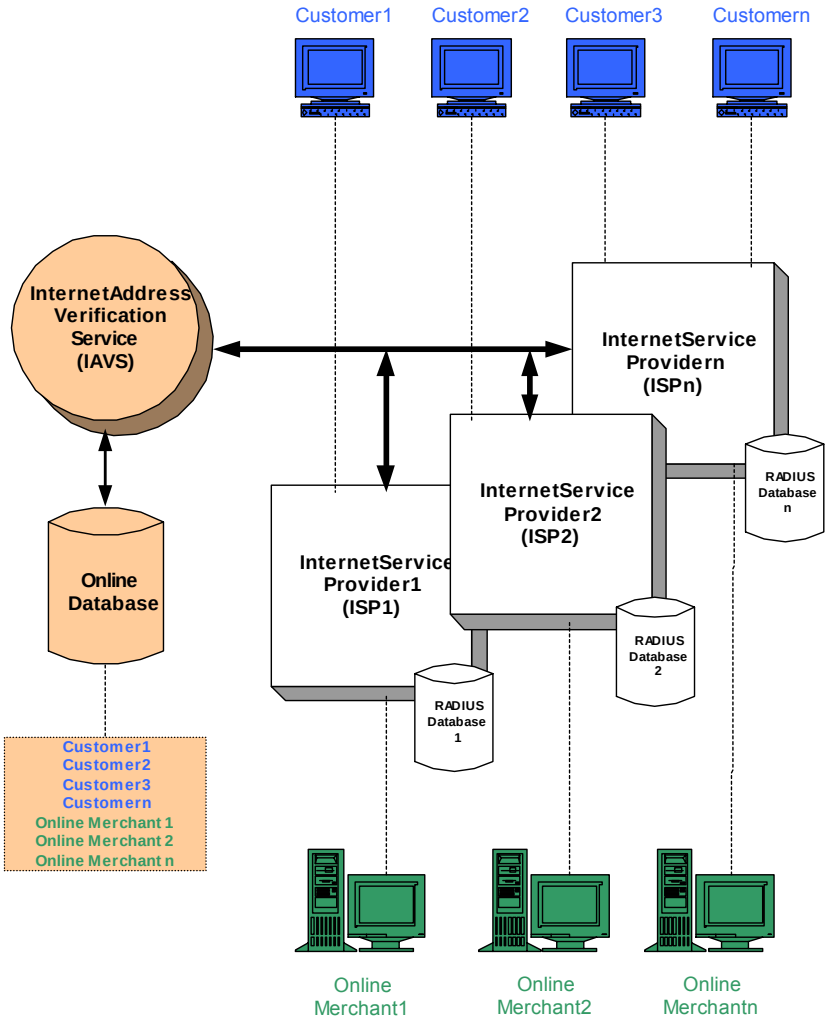

Figure 2: Internet Address Verification System In Use

Registration With The Internet Address Verification System Service Provider

I-AVS users are initially registered in the system.

Before the I-AVS can be used, users, i.e. consumers and merchants, need to initially register themselves in the system. This can be accomplished in a number of ways, including direct registration with the I-AVS Service Provider, or via another party, for example the user's credit card company.

Let us consider a consumer registering via his credit card company, because he primarily uses his credit card to purchase goods and services on the Internet.

Figure 3 illustrates an example of how a consumer and an online merchant (i.e. customers) register with the Internet Address Verification System.

Initially the customer logs onto a secure web site using SSL. The web site in this example is the customer's credit card issuing bank.

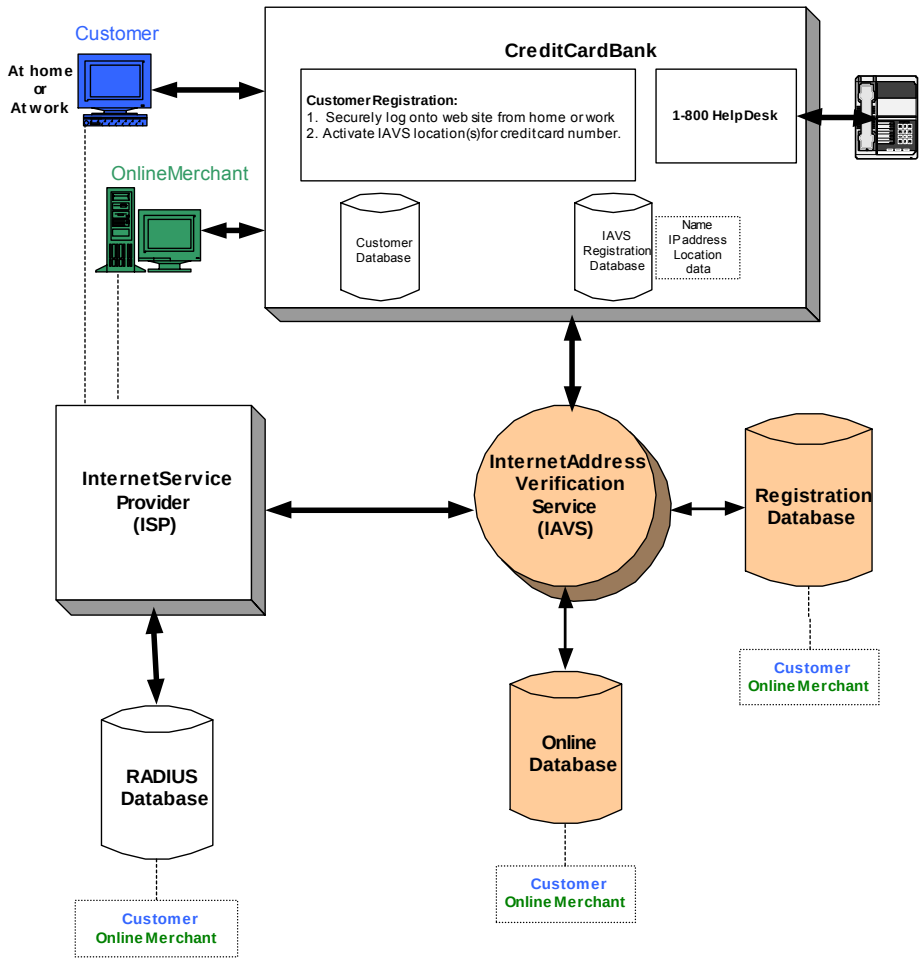

Figure 3: Registration in the Internet Address Verification System

I-AVS users register using a secure link and web site from a known physical

The bank provides a secure online I-AVS registration form, which is obtained from the I-AVS Service Provider and integrated into the bank's credit card online customer service. The customer fills in the web form, which is verified by the bank, in real-time against the bank's customer database.

Information that is collected by the bank and stored in its secure, temporary I-AVS database includes the customer's name, Internet Protocol (IP) address and other location data, for example contact telephone number, etc. A device, which is connected to the Internet, has an IP address which the customer's ISP uniquely assigns. The IP address is obtained from the customer's web browser and is used to locate the customer's Internet Service Provider (ISP). Other contact information is also collected to verify the customer, as well being able to contact the customer in the event of any questions.

The bank securely transmits the customer's registration information to the I-AVS Service Provider, which securely stores the information in an I-AVS Registration Database.

The I-AVS Service Provider uses the registration information to contact the customer's ISP online to establish the necessary relationship for the new customer. The customer's ISP confirms the registration information for the new customer and transmits the online status of the customer to the I-AVS Service Provider. The I-AVS Service Provider stores this information in its real-time Online Database. All communication between the I-AVS Service Provider and the ISP is secure, for example by using Digital Certificates and an SSL encrypted link. This completes the registration process.

Registering Additional, Alternate Locations with the I-AVS

I-AVS users can register additional, alternate transaction locations.

If the customer wishes to use an additional, alternative location to transact business on the Internet, he would reapply, for example in this application, to the bank, but from the new location. The new location could be the customer's work place. The registration process is then repeated. A further level of customer verification may be necessary for registering an alternative location. The added level of verification could include a request by the bank for the customer to confirm the new location from the initial registration location, for example, from home. Or confirmation via telephone, from the initial I-AVS registration location could also be accepted.

Automatic Verification of the Identities of Parties in an Online Transaction

We now consider the scenario in which I-AVS is used during an online transaction. Referring to Figure 4 below, Customer1 is already registered in the I-AVS. Whenever Customer1 logs onto the Internet via his ISP1, his online status is automatically logged in the I-AVS Service Provider's Online Database.

Customer1 wishes to log onto Online Merchant2's web site to purchase goods. The Online Merchant2 is already registered in the I-AVS. At all times that her web site is connected to the Internet, her ISP2 provides real-time status data to the I-AVS Service Provider, which logs this data in its Online Database.

When the Customer1 initiates payment for the goods that he wants to buy from the Online Merchant2 by using his appropriate credit card, a number of checks are executed:

I-AVS provides automatic verification of the online transaction parties, using their registered known physical locations.

1. The Online Merchant2 verifies with the I-AVS Service Provider that Customer1 is the lawfully registered user of the credit card.

2. The I-AVS Service Provider simply transmits, over a secure link, a "yes" or a "no" response to the merchant's query.

3. If the I-AVS response is "yes", then the transaction is executed. On the other hand, if the response is "no", then the merchant can deny the transaction.

A second layer of credit card I-AVS verification can take place. This layer is activated during the credit card verification process. This time it is the Credit Card Verification Service Provider that checks with the I-AVS Service Provider that both the Customer1 and the Online Merchant2 are who they claim to be. This requires that the Online Merchant provides the Credit Card Verification Service Provider with the relevant information about the Customer1. Depending upon the response from the I-AVS Service Provider, the Credit Card Verification Service Provider can either allow or deny the online transaction.

I-AVS verification of lawful web sites.

I-AVS data can be used to prosecute criminals.

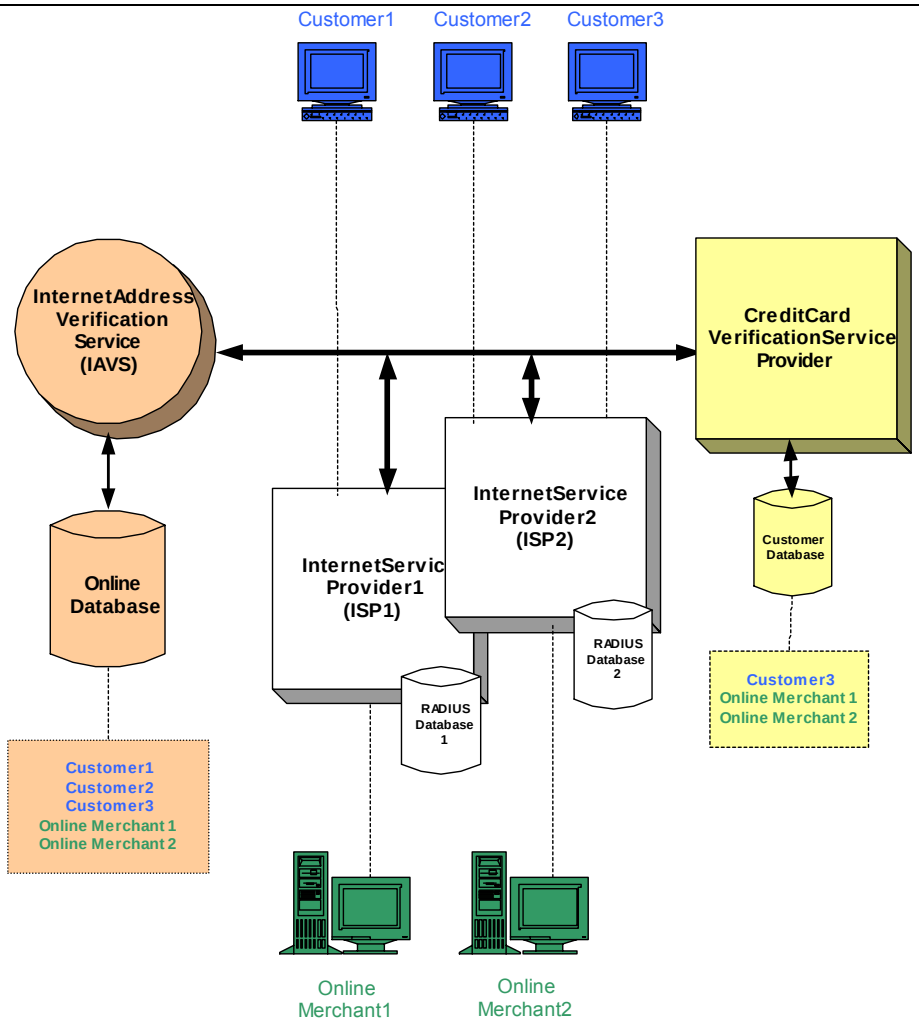

Figure 4: Internet Address Verification System In Use With A Credit Card Transaction

It is also possible to provide an enhancement to web browsers, i.e. a web browser “plug-in” application, that would automatically verify the Online Merchant’s I-AVS status. This would assist the customer to determine if a web site is lawful or not. As mentioned previously, it is common practice amongst Phishers to use fraudulent, look-alike, web sites to obtain a customer’s confidential information, such as credit card details, online banking logon credentials, etc.

Note that if the I-AVS Service Provider’s response is negative for any I-AVS request, then the information provided to it and stored in its Online Database, can be used by law enforcement to trace and possibly prosecute the abusers of the online transaction.

Verify and Trust

Conclusion

Trust is at the heart of all successful transactions, including online commercial transactions, as well as other confidential online transactions.

It is therefore imperative to the continuing growth and success of the Internet as a viable marketplace[18], that all parties involved in an online transaction can be irrefutably verified as the lawful participants.

The patented Internet Address Verification System provides this *trust between online transaction parties by verifying the lawful physical location from which they transact business*.

The I-AVS implements, to paraphrase a quote from Ronald Reagan: "**Verify And Trust**".

This system is much needed[19] in the online world to counter the growing explosion of online fraud.[20]

Contact Information

Lester Sussman
CEO
ceBerg, Inc.

9213 Bulls Run Parkway
Suite 100
Bethesda, MD 20817-2403

Ph: 240.447.3122
Fax: 301.897.0016

Email: ipAVS@ceberg.com

Lester Sussman

Digitally signed by Lester Sussman
DN: CN = Lester Sussman, C = US, O = ceBerg, Inc.
Reason: I am the author of this document
Date: 2005.09.01 10:29:31 -04'00'

[18] "Online Finance Hits Its Stride", Business Week, April 22, 2002
"E-Commerce starts To Click", Business Week, August 26, 2002

[19] "180,000 get credit fraud warning", USA Today, February 23, 2005
"The Soft Underbelly Of Offshoring", Business Week, April 25, 2005

[20] "Internet crime soars by over 350%", The New Zealand Herald, March 22, 2005