Trust – As Good as Gold
Or
BRINGING THE TRUST AND INDENTITY OF THE BANKING WORLD TO INTERNET INFORMATION COMMERCE

The ITA / Interform Initiative

By Bill Anderson
With contribution and editing
By Bill Densmore

Bill Anderson (wlanderson@qwest.com) is a retired banking-industry mainframe/networks SVP. He joined his first bank as a software developer in 1968. He helped develop the ATM, ACH and Visa network protocols at Seattle SeaFirst/Bank of America and successor banks. He also led technology at Rainier Bank. In this white paper, Anderson explains in detail why the credit-card system evolved and what it does. He then argues that its key value – the transfer of trust and identity – needs to be the core of a new "open market" for digital information – text, multimedia, news, entertainment – where payments can be aggregated among multiple websites and periodically settled.

In 1913, the United States guaranteed that U.S. coin and currency could be exchanged for gold. Then, in 1933, the U.S. abandoned the gold standard. At that time the U.S. Government guaranteed that: "United States coins and currency (including Federal Reserve notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues." Thereafter the U.S. Government guaranteed that the coin and currency printed and minted by the Bureau of Engraving and Printing was as "good as gold". The critical feature of the system is trust.

Today, the lack of a universal system for exchanging trust or individual identity on the web is inhibiting the development of a convenient, simple payment system for news and digital information. In this essay, I will lay a foundation for this argument by explaining how the credit-card system evolved, how it has become compromised by the internet, and what can be done. I then propose that a non-profit Information Trust Association (ITA) be established to research and promulgate standards and protocols for a ubiquitous shared-user network for trust, identity and information commerce, along with a for-profit operating company, Interform (working title) to run the system under the ITA's authority.

The monetary system in the U.S. is based on trust:

The Federal Reserve is the only entity with the U.S. Government's permission to introduce U.S. coin and paper currency into circulation. The Federal Reserve System (the Fed) was conceived by several of the world's leading bankers in 1910 and enacted in 1913, with the passing of the Federal Reserve Act. In short, the U.S. government has identified and certified that the Federal Reserve System is the only entity that can introduce coin and currency into circulation. The Fed in turn, identifies and certifies that certain

banks can administer the distribution and collection of coin and currency. The Fed grants these certain banks a federal charter – certifies them - and opens an account for them at the Federal Reserve Bank (FRB) after a very rigorous and detailed due diligence process. In short U.S. banks are identified and certified to have permission to manage the flow of cash payments in the U.S. on behalf of the U.S. government and are obligated to operate under the Fed's rules.

In 1913, the United States guaranteed that U.S. coin and currency could be exchanged for gold. Then, in 1933, the nation abandoned the gold standard. At that time the U.S. Government guaranteed that: "United States coins and currency (including Federal Reserve notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues." Thereafter the U.S. government guaranteed that the coin and currency printed and minted by the Bureau of Engraving and Printing was as "good as gold".

Since coin and currency don't last all that long and are cumbersome, federally charted banks use transaction accounts - their technical name is "demand deposit account" (DDA); common name is checking account - to simplify and speed up the transfer of funds from one person to another. Banks guaranteed that their own official checks (called cashier's checks) are backed by U.S. coin and currency and therefore are also "good as gold". That meant that a merchant can trust that if he "takes it (cashier's check) to the bank", he will be given coin and currency, which is in turn is as "good as gold". Consumers can also open a checking account and deposit their own coin and currency. The consumer can then write a check to a merchant that allows that merchant to "take it (consumer check) to the bank", because it is as "good as gold".

Let me summarize: Whether you like the government or banks or trust either of them explicitly, the fact is, you are giving them your implicit ***trust*** when you pay a merchant using a $10 bill or a check. And the merchant ***trusts*** he can ***take the payment to the bank*** and exchange it for coin and currency, therefore it's as ***good as gold.***

The scenario just described provides the basis of the system of trust that is used to make the payments system work. U.S. banks hold all of the money not in circulation in central (central to each individual bank) electronic vaults called the demand deposit accounting databases of record. The data center that houses the computers that manage the databases of record can be thought of as a virtual Fort Knox. Identification and access to a checking account is made through a standard formatted number. This number is variously called the ABA number, the routing and transit number (RTN), the checking account number or the DDA number. The checking account number is the ***key*** (noun) to the customer's individual financial record. The checking account number is a two part number. The first part is the routing and transit number (RTN) assigned to the bank of account by Accuity, a semi-autonomous unit of SourceMedia. The RTN tells all of the various networks which bank will post the check. The second part is the internal account number is assigned by the bank of account. Together they contain information needed to route the check to the payer's bank and to apply it – post it - to the payer's account. The good news about DDA numbers is that the banking industry is able to reliably move money from one account in one bank to another account in another bank because they trust the assignment process is strictly controlled. The bad news is that once disclosed to the general public, a DDA number can lead directly to valuable customer information that criminals can use to defraud innocent customers. Forging a check is an example of fraud.

Checks can take the form of paper, plastic (gives new meaning to the paper or plastic question!) or electronic bytes of data. The form-factor determines the network that is used to deliver the check to the demand deposit accounting system. For paper checks the network is the various check routing and transit clearing houses. For plastic, it's the debit card networks (separate from the credit card networks). For electronic, it's the various EFT systems: Fedwire, Bankwire, ACH, Swift, Chips, etc. All of these networks are owned and operated by banks, their agents or associations of banks and operate over private telecommunication lines.

Once checks are encoded and recorded electronically in the data center, they are called items. Banks have been electronically posting items to commercial and consumer DDA accounts domiciled on mainframe computers since the 1960s. Banks will continue to post to these accounts using the same mainframe architecture for the foreseeable future. Because of this critical role in the payments system, banks manage their back office operation and their data centers with exceptional care and security; at very great expense and under the intense scrutiny of federal regulators. Bank IT experts, along with major hardware and software vendors such as IBM, NCR, CSC Hogan Systems, ACI-Base24 and many others have created intricate programs and processes to keep banking computer systems safe and sound. Security and auditability are job-one in a commercial bank's enterprise data center.

Banking computer systems are among the safest and most secure in the world and would pose the most daunting challenge to any outsider wishing to defraud a DDA account. In fact, defrauding a bank is almost always done with help from an insider, rarely by an outsider. That's why banks spend so much time and effort policing against collusion. And that's why the Fed and the Office of the Comptroller of the Currency (OCC) are exceptionally rigorous as they audit banks for operational risk mitigation and management using the Basel II Pillar 1 Operational Risk Management Framework.

Let me summarize: U.S. banks are identified and certified to manage the flow of cash payments in the U.S. on behalf of the U.S. government and must operate under the strict rules of the Fed. Banks have built elaborate systems and procedures that allow them to operate according to the rules established by the Fed. The Fed and the OCC regularly and rigorously audit banks for adherence to those rules. Therefore, the Fed ***trusts*** that merchants can ***take checks to the bank*** and the bank will exchange the checks for coin and currency, and therefore the check is as ***good as gold.***

On-line bill paying

Among the many acts of congress that direct the FRB to develop rules for banks to adhere to is the Foreign Corrupt Practices Act of 1977 and its follow-on act, the Patriot Act. Section 326 of the USA PATRIOT Act requires financial institutions to have a Customer Identification Program ("CIP") to verify customer identification in connection with the opening of checking accounts… What this means is that banks must be diligent in the identification processes they employe when they are opening checking accounts for new customers. This the cornerstone in guarding against money laundering that can support illegal activity such as financing terrorism or hiding the source of a person's income from the IRS. It also means the FRB and the OCC will audit banks for compliance with these rules.

Banks have gone to great lengths to provide legitimate and properly identified customers access to self-initiated banking transactions by developing On-Line Banking (OLB) systems. The setup procedure for a new OLB customer provides customers with a user id/password/site-key protocol that insures that someone logging into an OLB account is who they say they are. Further the customer can establish a list

of trusted merchants that they wish to pay for goods and services. OLB systems are "front-end" computers that allow properly identified customers access to the "back end" banking systems which perform various funds transfers, all at the sole direction of the customer. Only the properly identified customer can release funds to pay a merchant bill and only the customer can identify which merchants they trust.

OLB systems usually run on large scale servers which are directly connected to the mainframes through closed circuit communications lines. Think of an On-Line banking server as an intelligent agent that prepares data requests which in turn cause the mainframe to perform a customer initiate transaction such as pay a bill or transfer funds from one of the customer's accounts to another of the same customer's accounts. The customer cannot directly deposit funds into their accounts using On-Line banking because there is no way for the bank to verify that the customer has permission to perform an inbound deposit.

Let me summarize: Banks use OLB portals to provide properly identified customer with the ability to direct that a payment be made from their accounts to a properly identified merchant account. The bank can ***trust*** that a merchant has ***taken a payment to the bank*** with the customer's authorization and the payment is as ***good as gold*** because the bank and the customer followed the rules for proper customer identification.

Credit Card identity:

You'll notice that the credit card hasn't been mentioned here. That's because credit card charges are not payments, they are loan advances made by credit card issuers. Diners' Club issued the first credit card in 1950. The Diner's Club credit card was a way to pay for a meal without using cash and was presented to the merchant in person by the card owner. Balances that built up during a month had to be paid each month in full, so the card offered only a convenient payment method rather than a way to obtain long-term financing. Bank of America followed in 1958 with the first general-purpose credit card on which only a portion of the balance needed to be paid each month. Merchants doing business with BofA would display a logo telling customers that they would accept the BankAmeriCard as payment.

Identification and access to a credit card account is made through a standard formatted number. Much the same as a checking account number, the credit card number is a two part number. BofA established this format for its BankAmeriCard, making it the de facto standard for the future. The first part is called the Issuer Identification Number (IIN). IINs are assigned by the American National Standards Institute (ANSI) using the ISO/IEC 7812 Numbering System. The purpose of the numbering system is to uniquely identify a card issuing institution in an international interchange environment by a trusted identification service. All IINs assigned are six digit numbers and each card issuer is entitled to one. Therefore only one IIN will be assigned to each card issuer. The second part of the credit card number is called the primary account number (PAN) and is assigned by each individual credit card issuer.

The good news about credit card numbers is that the credit card industry is able to reliably identify who the card issuer is and who a loan customer is because they trust the assignment process is strictly controlled. The bad news is that once disclosed to the general public, a credit card number can lead directly to valuable customer information that criminals can then use to defraud innocent customers.

The majority of identity theft and fraud in the credit card business results from disclosure of credit card numbers combined with names and addresses associated with the disclosed card numbers. The reason this information is gathered and stored by merchants is the merchant is required by card network rules

to positively identify the credit card presenter. If the merchant cannot prove that he verified the customer's identity and the customer requests a chargeback, then the merchant is stuck with the chargeback. If chargeback occur often enough for a merchant, that merchant may be expelled from the network.

When presented with a BankAmeriCard credit card, the merchant, taking care to fully identify the customer, fills out a paper draft that is signed by the customer as proof that the customer authorized the bank to deposit money in the merchant's BofA checking account and increase the customer's loan balance by an equal amount. The drafts are a form of script or IOU that the merchant fills out on behalf of the card presenter. One of the carbon copies of the draft goes to the customer, one is kept by the merchant and one goes into the merchant's nightly deposits along with any checks the merchant took in. While customers still sign an electronic or paper draft at the POS, the BofA network has evolved to the point of eliminating the need to send the paper to the bank. All paper stays with the merchant, everything else is electronified and sent to the bank.

Let me summarize: If the merchant follows all of BofA's rules for identifying the customer, then the merchant can ***trust*** that when he ***takes the payment to the bank***, the payment is as ***good as gold***. If a merchant, by his own actions, proves he cannot be ***trusted*** to verify the customer's identity, than that merchant can be expelled from the network and will be barred from accepting credit cards.

Why did BofA build a credit card network:

Bank of America built the original credit card authorization network to eliminate the printing and distribution of the bad-card book that it mailed to each of its merchants once a month. The bad-card book was used by BofA merchants to screen out customer credit cards which were lost or stolen or had been deactivated by BofA. BofA built the BankAmeriCard network solely for the purpose of collecting documentation memorializing a transaction to extend the balance of a loan held by BofA; thus minimizing the possibility that its customers would not repay their loans.

At the time BofA was building its card-accepting merchant base, other banks in other states were also building their own merchant-to-bank networks for extending their loans using their bank-named credit cards at the point of sale. But, merchants doing business with say, SeaFirst Bank in Washington State would only take SeaFirst labeled credit cards. A BofA employee named Dee Hock had the brilliant idea to franchise the name and numbering scheme of the BankAmeriCard to banks in other states. That meant that a bank in another state, SeaFirst in Washington in our example, could issue a credit card with the name BankAmeriCard on it; convince its merchants to accept the card; keep the loan on its books domiciled in the state of Washington. That way, when a BofA-BankAmeriCard holder had their card swiped by a SeaFirst merchant displaying the BankAmeriCard logo in Washington, SeaFirst would route the loan advance documentation to the BofA data center over private leased telecommunications lines. And vice-versa for a SeaFirst-BankAmeriCard holder getting their card swiped at a BofA merchant in California.

Let me summarize: BofA created the name and numbering format that became the de facto standard form for a credit card payment and called it the BankAmeriCard. When a merchant does business with its local bank and its local bank offers credit cards with the name BankAmeriCard on it, the merchant can ***trust*** that when he ***takes the BankAmeriCard payment to the bank***, the payment is as ***good as gold***.

At the same time all of this was happening, MasterCharge was created by several California banks as a competitor to the BankAmericard, The original banks behind MasterCharge were United California Bank

(later First Interstate Bank and subsequently merged into Wells Fargo Bank), Wells Fargo, Crocker National Bank (also subsequently merged into Wells Fargo), and the Bank of California (subsequently merged into the Union Bank of California). Just as BankAmeriCard became VISA, MasterCharge became MasterCard. Banks all over the U.S. joined either the VISA or MasterCard association and seemingly overnight a new form of paying for goods and services appeared. Keep in mind, it didn't happen overnight, it was started 60 years ago by the Diner's Club.

Let me summarize: Banks who franchised the name BankAmeriCard or MasterCharge could use those names on their credit cards and have merchants accept them as payments anywhere in the US. The banks agreed to use a common name and number format for their loans so they could entice their customers to use their credit card anywhere in order to increase the customer's loan balance and therefore increasing the bank's profit. Sweet deal!

Network members have obligations too:

Banks can't just buy a ticket on the VISA/MasterCard train to higher profits, they have significant obligations once they join the network. In order to become a member of the VISA network association a potential card issuer or merchant acquirer must file for entry and must undergo a rigorous due diligence process, much the same as Federal bank regulators perform on companies who are filing for a new bank charter. The filing process is intended to identify only potential members who are demonstratively able to uphold all of the association's tenets and code of ethics and abide by the Association's rules.

Once an issuer or acquirer is admitted to the association, they must sign a contract obligating them to follow the rules and regulations of the association. The rules are spelled out in great detail (670 pages worth) in the Operating Guide. Penalties for non-compliance are listed right along with each rule. The Member, Visa U.S.A., or their designees may conduct financial, procedural, and Cardholder Information Security Program audits and/or reviews at any time.

The Operating Guide also specifies the procedure for allegation, investigation and notification of violations, the schedule for fines, and the rights to appeal. These procedures and fines are in addition to enforcement rights available to Visa U.S.A. under other provisions of the Operating Regulations, the Visa U.S.A. Inc. Certificate of Incorporation and Bylaws, or through other legal or administrative procedures.

An example of a rule is located in the end-notes.[i]

Let me summarize: an issuer or acquirer, who becomes a member of the VISA Association commits, by signing a legally binding contract, to behave in a manner that is consistent with the tenets and ethics of the association. The rest of the association members can ***trust*** the new member will behave properly because the new member signed a contract and their behavior can be audited. Cardholders of the new-issuer can ***trust*** that the new-issuer will honor their instructions to increase their loan balance when directed to do so by a merchant. Merchants can ***trust*** that the new-issuer's card transactions can be ***taken to the bank*** and are as ***good as gold***.

How do credit cards work with the card present (CP):

The process for handling credit-card transactions over a network began in simpler times many years ago. In the beginning of the modern payments era, only cash was as "good as gold". Then, the banks convinced merchants to take local checks if the merchant could positively identify the check presenter.

Checks became “good as Gold”. Then, banks convinced merchants to take credit cards if the merchant agreed to take the responsibility to positively identify the presenter (trust, but verify was the banking way long before Ronald Regan was president). Credit cards became as “good as gold”. The process goes like this when the credit card presenter is physically in the presence of the merchant:

1. The customer hands the merchant their credit card;
2. The merchant verifies the person presenting the card is the owner of the card by asking for photo identification;
3. After proper identification, the merchant swipes the card through a card reader.
4. The card reader sends the transaction details to the card issuer;
5. The card issuer approves the loan advance and sends the approval notice back to the merchant;
6. The customer signs the credit card receipt;
7. At the end of the day the merchant sends all of the days credit card receipts through the network to the credit card issuer;
8. The issuer “captures’ the receipt and sends the proceeds of the loan advance through the bank clearing and settlement system known as Fedwire, to the merchant’s bank.
9. At the end of the customer’s billing cycle, the card issuer sends the bill to the customer;
10. The customer pays the credit card bill with cash or funds from their checking account.

Therefore, the “payment” to the merchant is actually made at the end of the day through one of the Fed authorized banking systems and not at the point of sale (POS). The network serves as the data delivery medium for loan-advance documentation. The issuers have a good comfort level that the customer is who they say they are and therefore they have documentation that shows the customer owes them money, plus interest. This system works very well if the merchant is diligent in requiring adequate customer identification and the customer repays the loan. The customer is happy, the merchant is happy and the banks are really happy.

How do credit cards work with the card not present (CNP):

Telephone-based catalog sales presented the first opportunity to execute a credit card transaction without the consumer being in the presence of the merchant. Instead of the customer handing over their card, sales staff would ask the customer for their card number, name and address and sometimes driver’s license number or some other form of positive ID. After gathering all the information about the card presenter the sales staff entered it into a terminal linked directly to the credit card network. From that point on, the transaction moves through the network the same way as a card-present transaction. Since catalog sales companies are well known to their individual banks and they communicated over private communications lines, there is a trusted relationship between bank and merchant.

Credit-card transactions performed over the internet add a new and not so happy twist to the card not present method. There are no human beings in the equation, only computers. How can the banking-trust network know for sure who is operating the computer? There is no way to absolutely and positively determine if the consumer is who they say they are. The merchants are forced to gather as

much information about the consumer as they can and "trust" that the information is not stolen. The consequences of gathering so much private financial information is that there's no practical way to insure that a consumer's data isn't being disclosed to the wrong people because of a lack of care on the merchant's part. Despite years of security improvements and tougher, more coordinated law enforcement efforts, criminals still boldly siphon credit card account numbers and whole buckets of consumer information from unwitting merchants. The data is invaluable to thieves due to its ready conversion to online purchases, creation of counterfeit cards, or more elaborate identity theft schemes.

In an effort to rein in identity theft, Visa launched the Cardholder Information Security Program and Account Information Security Standards Program in 1999. Visa published data requirements for the protection of sensitive data. In 2004, Visa and MasterCard collaborated to create a single set of worldwide data security requirements called the Payment Card Industry Data Security Standard (PCI DSS). This standard is designed to help all entities that process, store, or transmit customer transaction data to implement better data security practices. The PCI DSS is now accepted as a standard and if practiced diligently, provides security, but it lacks the force of law. As a comparison, the Patriot Act is an enforceable law that regulates how financial institutions operate and how they protect customer information. There are significant consequences if a financial institution fails to follow Patriot Act rules. Merchants are required to follow the PCI DSS, however, it would be nearly impossible to audit the security measures in the everyday-operations in back offices of millions of worldwide Internet merchants. Therefore merchants have little incentive to spend money on better security. It is only after a breach in security takes place that bad merchant operating practices come to the fore.

An even bigger issue for on-line purchasers is privacy.

What's wrong with this picture?.

There are over 205 million individual and independent web servers worldwide. There are over 1.8 billion individual internet users worldwide. All of these web sites and all of these internet users are connected over the public TCP/IPv4 internet. TCP/IPv4 refers to the addressing scheme that allows internet users and web sites to be located as they interact on the web. The IP address, as it is called, identifies the location of the internet user. Think of an IP address as a routing number for a web site hit. Another way to think of an IP number is it is similar in function to a cell phone number. However, the IP addressing scheme lacks the needed granularity to identify all the individuals accessing the web, so Internet Service Providers assign an internet user a dynamic IP address each time the user powers on their in-home modem or logs on to a Wi-Fi network. The dynamic IP assignment method allows internet users to share IP addresses without knowing it. Dynamic IP addresses also mean that there are limits on the ability to track a user's location. That means internet users are nearly always anonymous or at least semi-anonymous. Think of the usefulness of a cell phone number that changes every time you turn the phone on.

There is no way to assign a unique identity-address because the existing TCP/IPv4 addressing scheme has a limited number of addresses available. Therefore people are assumed to be anonymous. Further, even if such a scheme existed – TCP/IPv6 might fill part of the bill - there is no trusted identification service to administer the assignment of IP numbers.

It is conventional wisdom that on-line sales are exploding; maybe not so much. Forrester Research reports that on-line retail sales were about 6% of all retail sales in the U.S. in 2009. Forrester expects that to grow to only 8% of all retail sales by 2014. What is growing is called web-influenced buying.

Consumers do research for a product on-line and then buy in a real store. Forrester reports that 42% of all retail sales in the U.S for 2009 were a combination of on-line sales and web-influenced sales. That total is expected to rise to 53% of all U.S. sales. So the truth of the matter is that the Internet has a lot of lookers and tire kickers, but not so many actual buyers. While not wanting to jump to any conclusions on this, it would be a fair bet that trust enters into the equation.

Let me summarize: eCommerce on the internet operates semi-anonymously and without borders. The internet marketplace is where caveat emptor meets head-on with Laissez-faire. Without a trusted identity service that creates and manages an identity process, merchants are forced to gather significant financial information from customers in order to verify the identity of a web purchaser. Without enforceable consumer protection laws, customers are forced to rely on other people's opinions about the quality of service provided by any given merchant. There is an apparent reluctance to accept the word of complete strangers and or customers are just window-shopping on the web and they go offline to buy.

Journalistic eCommerece doesn't stand a chance:

Without a way to positively identify an internet user, merchants on the web must rely on the honesty of their customers. Frankly, merchants don't "trust" customers to be truthful because they can't be sure the customer is who they say they are. Merchants are afraid that when they "take a payment to the bank" the payment won't be as "good as gold". Customers don't "trust" that the eCommerce merchants will protect their financial information from unlawful disclosure and misuse, so they are reluctant to give information to the merchant and therefore limit their shopping on the internet. Journalists are reluctant to engage in constructive dialogue with internet users who wish to remain anonymous, because people who hide their identity have not proven that they can be trusted. If all of this wasn't bad enough, the newspaper advertising business is slowly withdrawing from mass marketing as it used to be practiced in the good old days of paper-newspapers in favor of targeted advertising as provided by Google.

The "trust" dilemma has stopped journalism dead in its tracks. On one horn of the dilemma, journalist and publisher don't "trust" that the customer will pay for content and therefore they erect pay-walls so they can collect a fee. Further they don't trust that anonymous comments are truthful or accurate so they limit or severely restrict consumer involvement in the journalistic process. The choice is either erect pay-walls or continue to give content away and hope advertising will return to save the day. On the other horn of the dilemma, the customer doesn't "trust" the journalist or that the publisher has any content worth buying since there is so much "free" content on the internet. Unfortunately for the customer, all that free content may be worth exactly what they pay for it; nothing. Or worse yet, it may be misinformation, slander, plagiarism, rumor or bald-faced lies.

What is a poor journalist to do:

I propose that the journalism community unite and form the Information Trust Association and contract with Interform to build a trusted network complete with a new way to pay for content.

ITA: The Information Trust Association can develop a set of rules and regulations that govern the behavior of its members, similar to what the VISA Association has done. The purpose of the rules would be to prove to consumers that the content provided for sale by the members is worth something, offering value to the consumer. Rules would cover all the attributes that are important to journalists;

honesty, integrity, trustworthiness, etc. The rules can describe in detail what is expected behavior for a member and what the penalties are for non-compliance. The ITA can develop a strong set of entrance requirements that would only allow trusted publishers and journalist into the association. By following this path, a journalistic web site could display an ITA logo to signify they adhere to the ITA code of conduct and they will be audited by the ITA to prove it. ITA can create its own trusted network

Interform: I propose we build a network based on both non-internet and internet technology that will do a similar data collection function that BofA used to capture credit card data at the point of sale. Further, I propose we develop a micro accounting system similar to the micro-account systems that are used by the cell phone industry. And finally, I propose we build a totally new and ultra-secure process for ITA members to "take the payments to the bank". The new payments method is unlike anything on the market today. It creates a gateway to the bank payments systems that would not require that ANY customer financial data EVER be viewable on the Internet. That means there would be an end to financial data disclosure and mis-use via the Internet.

Let me summarize: An ITA/Interform collaboration will enable journalists and publishers to collect consumption information at the point in time when a customer consumes the journalistic product (page views); memorialize that data and bill the customer at the end of a billing cycle. The systems and physical infrastructure are mostly in place, we just need to integrate them.

--- END ---

Visa [1]Member Responsibilities [Overall]

A Member must:

- Comply with all of the following:
  - Visa U.S.A. Inc. Operating Regulations
  - Visa U.S.A. Inc. Certificate of Incorporation and Bylaws
  - Visa International Operating Regulations
  - Visa International Card and Marks Specifications (for Cards bearing the Visa Flag
  - Symbol)
  - Visa Product Brand Standards (for Cards bearing the Visa Brand Mark)
  - Appropriate VisaNet User's Manuals

- Perform all obligations imposed on Visa U.S.A. under the Visa International Operating Regulations that arise out of Interchange or a Transaction resulting in Interchange, between the Member and a Foreign Licensee

A Member must not do anything to cause Visa U.S.A. to violate the Visa International Operating Regulations.

1.3.A Visa Member Responsibilities [Individual rule for anti-money laundering]

A Member must:

- Implement and maintain an Anti-Money Laundering Program by:
  - Creating internal policies, procedures, and controls to prevent money laundering and terrorist financing
  - Designating a compliance officer to overlook the operations of the program
  - Training employees of the program on an on-going basis
  - Hiring an independent audit company to monitor the program, as applicable

- In a timely manner, block the Authorization of Cardholder Transactions or terminate all Merchants that engage in the following activities:
  - The introduction of illegal funds into the Visa system
  - The laundering of money through the Visa system
  - The financing of terrorist activity through the Visa system
- Accept responsibility for the Anti-Money Laundering Program of any Agent used by the Member in connection with its Visa Program
- As requested by Visa U.S.A., provide an independent assessment of the effectiveness of the Anti-Money Laundering Program of the Member or any Agent used by the Member
- Cooperate with Visa in the application of the Anti-Money Laundering Program, including:
  - Assisting Visa in guarding against money laundering and terrorist financing
  - Supplying Visa with a copy of its Anti-Money Laundering Program plan upon request

1.3.B Noncompliance [Individual penalty for anti-money laundering]

If Visa determines that a Member or its Agent failed to comply with the Anti-Money Laundering Program requirements, as specified in *Section 1.3.A*, Visa may impose conditions on the Member or its Agent, including:

- Implementing additional policies, procedures, or controls
- Requiring the termination of its agreement with its Merchant, its Agent, or its Cardholder
- Imposing fines or other penalties, as specified in Chapter 1, "*General Regulations*,"
- Terminating the Member's membership