

January 1998

## Generating an Online Bottom Line

Michael L. Kasavana

*Michigan State University*, shbsirc@msu.edu

Wonae Cho

*University of Kentucky*, null@uky.edu

Follow this and additional works at: <https://digitalcommons.fiu.edu/hospitalityreview>



Part of the [Hospitality Administration and Management Commons](#)

---

### Recommended Citation

Kasavana, Michael L. and Cho, Wonae (1998) "Generating an Online Bottom Line," *Hospitality Review*: Vol. 16 : Iss. 2 , Article 6.  
Available at: <https://digitalcommons.fiu.edu/hospitalityreview/vol16/iss2/6>

This work is brought to you for free and open access by FIU Digital Commons. It has been accepted for inclusion in *Hospitality Review* by an authorized administrator of FIU Digital Commons. For more information, please contact [dcc@fiu.edu](mailto:dcc@fiu.edu).

---

## Generating an Online Bottom Line

### **Abstract**

E-commerce is an approach to achieving business goals through information technology and is quickly changing the way hospitality business is planned, monitored, and conducted. No longer do buyers and sellers need to engage in interpersonal communications for transactions to occur. The future of transaction processing, which includes cyber cash and digital checking, are directly attributable to e-commerce which provides an efficient, reliable, secure, and effective platform for conducting hospitality business on the web.

# Generating an online bottom line

by Michael L. Kasavana  
and Wonae Cho

*E-commerce is an approach to achieving business goals through information technology and is quickly changing the way hospitality business is planned, monitored, and conducted. No longer do buyers and sellers need to engage in interpersonal communications for transactions to occur. The future of transaction processing, which includes cybercash and digital checking, are directly attributable to e-commerce which provides an efficient, reliable, secure, and effective platform for conducting hospitality business on the web.*

The world wide web (www) is becoming an essential business element. According to *Business Week*, some 90 million people from more than 150 countries gather news and information and transact business on the web.<sup>1</sup> The eStats organization projects that global user growth will approximate 142 million by the year 2002. Even though a majority of web users gather news and information, an increasing number of surfers are going online for shopping and travel planning.

The web has been developed and expanded through several progressive stages. Initially, it allowed users to access a vast amount of text information any time, any place. This phase referred to as the "access" stage led to the "presence" stage that enabled participants to present streamlined information to a broad array of surfers. Allowing organizations to integrate their internal systems (e.g., databases) into the information, the web evolved into its next segment, the "integration" stage. Examples in the hospitality industry include allowing guests to check room availability, rate plans, and frequent guest program account balances. In turn, the integration stage has led to the current stage, e-commerce (electronic-commerce). E-commerce provides the opportunity to transact business on the web. The impact of e-commerce on the hospitality industry, like so many other industries, has

significantly influenced the way online business is conducted.

E-commerce is defined as "a modern business methodology that addresses the needs of organizations, merchants, and consumers to cut costs while improving the quality of goods and services and increasing the speed of service delivery."<sup>2</sup> E-commerce is an approach to achieving business goals in which information technology enables or facilitates activities in and across value chains, as well as decisions that underlie those activities. A recent U.S. Commerce Department report indicates that information technology has positively influenced the growth of the U.S. economy, and concludes that e-commerce is a cost effective business platform capable of continuously driving economic growth.<sup>3</sup>

#### **E-commerce reduces expenses**

A number of global companies have adopted e-commerce as a means of reducing transaction related expenditures, connecting with current and potential customers, and enhancing revenues and profitability. Numerous U.S. companies have embraced the world wide web for conducting commercial transactions with both purveyors and customers. In 1996, 80 percent of Fortune 500 companies supported a company web site, while fewer than half these same companies had a web site in 1995. Forrester Research, Inc. estimates current online sales of \$2.4 billion, and projects that nearly 46 million Americans will

significantly contribute to the \$6.6 billion worldwide online revenues expected in 2000, spending an average of \$350 per capita annually. E-commerce appears well suited to service industries (e.g., hotels) where traditionally there has been limited general access to information.<sup>4</sup>

#### **Hospitality industry is leader**

The hospitality industry has been a leader in online web sales. Forrester Research, Inc. found that in 1997 online sales related to the travel industry totaled \$276 million, which ranked it second behind online microcomputer (PC) hardware and software sales. Total travel-related online sales were more than 25 percent of all online sales across all industries (\$1.1 billion). It is anticipated that customers will buy more travel-related products and services through online transactions than any other industry. Within four years online sales are expected to account for more than 8 percent of all travel-related products and services. According to a recent survey by Yankelovich Partners, hotel reservations were one of the items web users who had not yet purchased online claimed they would consider as a first time transaction.<sup>5</sup>

According to WorldRes, a prominent web-based hotel reservation network, more than 5,000 additional properties are expected to make online reservation services available in the near future. They report the number of bookable online hotels exceeds 2,200

properties located in more than 60 countries. Some hotel companies, such as Marriott International, Hilton Hotels Corporation, and Starwood Hotels & Resorts Worldwide, have significantly invested in e-commerce. Even though each of these three companies on average receives about 1 percent of its total reservation bookings through online transactions, the revenues received are impressive, given the size of each company.

Hilton's web site generates in excess of \$1 million in reservation revenue per month, Marriott receives \$14 million annually, and Starwood Hotels collects \$ 70 million in reservation revenue per year.<sup>6</sup> Some experts predict that hotels will experience 8 to 10 percent of reservation revenue through online transactions, while WordRes foresees hotel bookings expanding from 1 percent to 35 percent within the next decade.<sup>7</sup> Moreover, recent mergers within the hotel industry are expected to allow more lodging companies to offer online reservations more easily.<sup>8</sup>

In general, hotel companies have focused on two types of e-commerce: customer-to-business and business-to-business. E-commerce is often adopted as a means to bypass others in the value chain. Bypassing intermediaries helps companies reduce costs and fees, while generating sales through more efficient and effective customer service. After all, online transaction processing offers unparalleled opportunities at lower cycle speeds.

### **Direct links are focus**

Direct link to customers (customer-to-business) appears to be the primary focus of e-commerce for the hotel industry. Hotel companies provide current and potential customers not only with the services the customers can get by calling properties or dialing toll-free numbers, but also with unique and customized (personalized) products and services. Hotel company web sites provide customers with more streamlined services based on a customer's preferences as well as general information about the property's facilities, room availability, rates, amenities, and the like.

For example, a registered member of Hilton.com can create a personal preference profile at the site, resulting in faster and more personalized service. Following registration, customers begin receiving special news items, sales promotions, and advance notice of important web site changes as well as other relevant updates via e-mail. The Hilton Hotels registration feature provides the company with a competitive advantage arising through the development of one-on-one customer relationships. Such a direct and close relationship is expected to strengthen brand loyalty through its web site since web surfers tend to visit the same sites repeatedly so long as they find them useful. Thus, developing an effective customer pipeline and attracting a broader range of potential customers appear to factor in e-commerce success.

Moreover, hotel companies are beginning to implement emerging technologies that allow customers to interact with the web site on a real-time basis. Such emerging technologies as virtual tours, for example, enable a guest to select a property and room type after surveying a facsimile of the facility.

### **Hotels can link to suppliers**

Hotel companies have started implementing e-commerce as an electronic link to suppliers (business-to-business). This relationship enables online purchasing which presents real-time access to current product availability that cannot be matched by a static, printed catalog.<sup>9</sup> In addition, an online purchasing process allows both buyers and sellers the opportunity to customize product offerings. Being aware of these advantages, the hotel industry is beginning to more aggressively link to suppliers across the web or through formation of an extranet.

Promus Hotels Inc., for example, used cyberspace to transform a traditional procurement process from a manual process into an electronic online process. Promus' purchasing system, Preferred Supplier Network, allows purchasing personnel to access affiliated suppliers anywhere in the U.S. within 12 minutes to place orders. In addition to reducing costs, executing an automated purchase cycle helps streamline the company's overall business process.<sup>10</sup>

Online hospitality business transactions are projected to soar in the near future, and many

hotel companies are on the verge of implementing online buy and sell transaction interfaces at web sites. According to a recent survey on technology in the U.S. lodging industry by PKF Consulting and HITA, more than 66 percent of the surveyed hotel managers claimed their property had a web site. However, online reservation processing was only available at slightly more than half (56 percent) of the referenced web sites.<sup>11</sup> This result is primarily due to concerns related to network capabilities and secure transaction processing. It is not surprising that many consumers feel uncomfortable with online transactions for the same reasons. For online purchasing to succeed, consumers must have a higher level of confidence in the e-commerce environment.

### **Security is big obstacle**

Security is one of the biggest obstacles impeding the popularity of e-commerce. As indicated in a recent technology report entitled, "A Framework for Global Electronic Commerce," safety and reliability of communications and data through the Internet must occur before e-commerce can flourish.<sup>12</sup> Information transmitted over a network has a higher degree of security risk than information stored on a local computer. Comparatively, worldwide Internet transmission carries an even greater risk since every computer along the data route has potential access to proprietary information. Data equals dollars in cyberspace,

and the Internet offers access to a vast array of data. In order for Internet commerce to approximate its potential, the Internet must provide reliable data security while minimizing inherent vulnerability. Reliable transaction processing technology must keep data safe from cyberthugs and web thieves.

There are at least four elements involved in securing electronic transactions, confidentiality, authentication, integrity, and non-repudiation.<sup>13</sup>

- **Confidentiality:** Confidentiality deals with the concealment of data and/or information from unauthorized users or reviewers. This is an important element to protect privacy and proprietary information. The privacy problem of the world wide web originates from one of its greatest features, open architecture. Encryption and virtual private network extensions can be used for satisfying this element. Encryption can be used to protect proprietary information from improper handling or interruption as it is moved across the web. Cryptography, the practice of encryption, can be used to automatically secure data using numeric keys and mathematical algorithms (i.e., formulas). Cryptography allows the user to apply an encryption protocol to a message being sent over the web.

- **Authentication:** Authentication is to ensure that all parties involved in a transaction are communicating only with those persons properly authorized. Authentication is critical to preventing fraudulent transactions. A digital signature is one of the primary methods for authentication. Simple passwords, callback systems, and challenge/response tokens can also be used to validate authentication.

- **Integrity:** Integrity assures transaction participants that exchanged data has not been modified during transmission over a network. Two key methods are encryption and authentication. While both ensure that data has not been modified, neither ensures that an unauthorized user ("netlurker") might have read the transmission content. A browser-based security measure involves use of a digital signature and certificate authentication. By exchanging private keys, participants with compatible browsers can gain confidence in secure electronic transactions (SET). Another browser technique provides a warning system advising the user when possible security problems are encountered, for example, discovery of a web cookie file.

• **Non-repudiation:** Non-repudiation relates to accountability. Non-repudiation is designed to ensure that participants adhere to previously established e-commerce agreements. Audit trails, web server logs, processing procedures, and data receipts are examples of low cost non-repudiation techniques.

### **Private network is secure**

One development enhancing electronic commerce involves the implementation of a Virtual Private Network (VPN). A VPN allows business-to-business transactions employing a secure tunnel through the public Internet. A VPN tends to be more attractive than traditional methods of electronic data interchange (EDI) since EDI usually involves expensive and highly proprietary leased private communication channels. While EDI employs network systems that allow output from one system to be processed directly as input to another system, e-commerce supports a wider set of technologies, standards, and protocols.

### **Encryption protects documents**

Encryption provides a method of protection for private documents (e.g., e-mail messages, business transactions) during network routing. An encryption algorithm is a mathematical equation that transforms data into an undecipherable format without a decryption key, which is used to convert encrypted data back into a read-

able format. The objective of the algorithm is to ensure privacy by having the data hidden from neturkers (persons for whom the data is not intended). Sending an encrypted message is similar to putting a scrambled letter in an envelope and distributing it.

In an encryption process, the message is encoded so that its contents remain disguised and protected during transit. Encryption is a popular data security method automatically available in many web browser software packages. Cryptography, the practice of encryption, can be used to automatically secure data using numeric keys and mathematical algorithms (i.e., formulae). Essentially, cryptography allows the user to apply an encryption protocol to a message being sent over a network. Two popular cryptographic methods are private-key encryption and public-key encryption.

In a private-key scheme both the sender and receiver use the same key to encrypt and decrypt a message (Figure 1). It is for this reason that the methodology is often described as symmetric. Private-key encryption is a traditional method of rapid cryptography accompanied by some measure of risk. Private-key encryption involves transmitting a secret key (private key) to the receiver and provides an opportunity for interception or deception. Such insecurity tends to defeat the reliability and privatization of the private-key scheme.

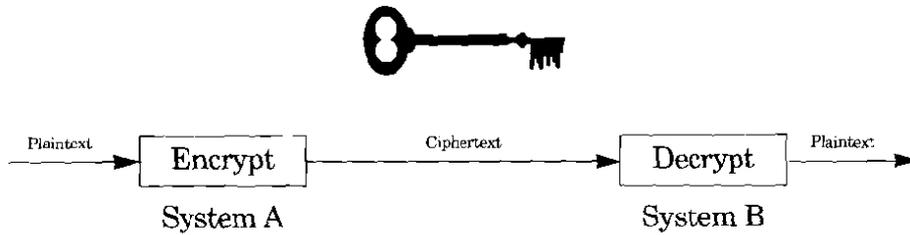
Asymmetric encryption, commonly known as public key cryptography, involves the use of a pair

---

**Figure 1**  
**Encryption**

---

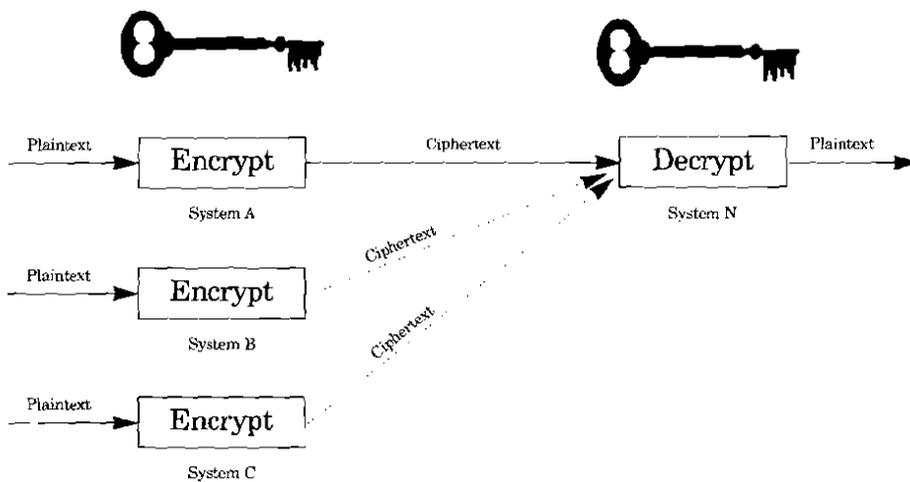
**Private-Key Encryption**



---

*Reference: Ford & Baum (1996)*

**Public-Key Encryption**



---

*Reference: Ford & Baum (1996)*

of keys. Data encrypted with one key cannot be decrypted without the pair key since the two keys are arithmetically connected. One key is called a public key and can be found published in a public directory. The assigned mate or other

key is a private key that is secretive and known only to its owner. RSA (named after its inventors Rivest, Shamir, and Adleman) is the most popular algorithm using public-key encryption. In the RSA method, the sender creates two

**Exhibit 1**  
**Sampling of encryption methodology**

Type	Encryption	Plaintext	Ciphertext	Technique
Transposition	Character Reordering	Hospitality	ohpstlatiy	Adjacent characters switched
Substitution	Character Replacement	Casino	ecukpr	Characters replaced by others
Expansion	Character Insertion	Hotel	hrortrerlr	Insert "r" after each character
Compaction	Character Removal	restaurant	resaurnt	Every fourth character removed

unique keys, a public key and a private key. As Figure 2 illustrates, the sender uses one key (private key) to lock the message and the receiver uses a different key (public key) to unlock it. Public-key encryption is an effective method for securing e-commerce transactions since the buyer and seller do not share a common single key. See Exhibit 1 for examples of encryption methods.

**Signatures ensure authenticity**

Another public-key method frequently used in the conduct of e-commerce is referred to as digital signature, used to signify that a document originated with the person signing it and that it has not been tampered with after the signature was applied. The digital signature process operates similar to paper and pen signature in that it assures the recipient of the authenticity of the origin and content of an electronic document. A

digital signature provides the recipient with confidence the sender is authentic and the message originator. This procedure prevents the sender from purposefully denying his or her signature on the document. Furthermore, it enables the computer to notarize the data that is transmitted and warrants it forgery-free.<sup>14</sup> Authentication through a digital signature is further strengthened by the use of digital certificates that ensure the sender is the owner of the public key, not someone attempting to commit fraud.

Digital certificates are used to authenticate the source of a document by ensuring the identity of a public key holder. For example, before two parties exchange digital signatures, each wants to be assured that the other is the entity identifying itself in the transmission. A trusted third party, also known as a certificate authority (CA), is used to validate and

authenticate that a public key belongs to its rightful owner through the issuance of a digital certificate. In other words, a digital certificate certifies that a CA has digitally confirmed an owner's public key.

### **Verification is critical**

To verify that a message was actually sent by the person claiming to have sent it requires a digital signature that is issued by a certification authority. The digital certificate is sent along with an encrypted message to verify that the sender is truly the entity identifying itself in the transmission. A digital certificate normally contains such data as owner name, company, and address; owner public key; owner certificate serial number; owner validity dates; certifying company ID; and certifying company digital signature.

A third party digital certificate is deemed critical to effective and secure e-commerce since it allows both buyer and seller assurance that the involved parties are in reality whom they claim to be. The main advantage of a digital certificate is that it cannot be fabricated or falsified. Hence, a digital certificate ensures that the sender cannot later deny placing an order, making a reservation, or committing to a purchase agreement. The only vulnerable aspect of this methodology is that the CA's secret key might be an uncovered and false digital certificate created.

There are several security protocols that have been developed to protect online transactions. A

security protocol is capable of encrypting and decrypting messages for online transmission. In addition, security protocols provide an authentication scheme. The security protocols most often used on the web are secure socket layer (SSL) and Secure Electronic Transactions (SET).

**Secure socket layer (SSL):** Perhaps one of the most popular web encryption methods is secure socket layer (SSL), an encryption method that provides two-way encryption. SSL provides authentication as well as encryption and is widely used for Internet transactions. SSL (developed by Netscape) is a high-level security protocol designed to automatically encrypt data as it travels over a network. Data is automatically encrypted before it is transmitted and then unencrypted on the receiving end. In between, the data is a meaningless jumble of zeros and ones to anyone without the decryption key. SSL provides for confidentiality, integrity, and server authentication, but few offer digital signatures that are needed for customer authentication. A new protocol called secure electronic transactions (SET) that provides digital signature capability has been developed by a joint effort by Master Card, Visa, and others to secure credit card payments over the Internet.

**Secure electronic transactions (SET):** Securing proprietary and confidential information during the conduct of an online transac-

tion can be a major concern. In addition to online reservations and commodity purchases, a hospitality firm may employ a shopping cart metaphor to allow users to browse merchandise, purchase products, and complete settlement at the web site. The SET protocol, which is based on public-key encryption and authentication technology, was developed to provide authentication of credit and debit cardholders by designating a trusted third party (CA) to provide authentication to both buyer and seller through the use of digital signatures and merchant certificates, to provide confidentiality of payment data by the use of message encryption, to preserve the integrity of payment data by the use of digital signatures, and to provide interoperability that can be applicable on a variety of hardware and software platforms by the use of standard protocols and message formats.

### **Reservations go online**

Global reservation networks enable self-reservations over the web. In order to provide this online capability, a lodging company must provide room type, room rate, and current room availability data. The online booking process at most web sites involves a lead-through series of search and selection procedures designed as a self-service exercise for the consumer. There are a variety of web sites featuring hotel reservation services (e.g., TravelWeb, Travelocity, Places to Stay, and Expedia) as well as individual

lodging companies supporting stand-alone reservation sites (e.g., Hyatt Hotels, Intercontinental Hotels, Holiday Inns, and Sheraton Hotels).

While it may create a burden for properties linked to online reservation networks to maintain current and future room availability information, many companies are attempting to blend property-level availability data with system-wide data to form a seamless database that ensures accurate information (i.e., single image inventory). Guests who make online bookings establish unique electronic linkages with a lodging company. In addition to the reservation transaction, the lodging firm can form an electronic relationship with the traveler by securing an e-mail address or other identity factor that may translate into a true competitive advantage in the marketplace. Buyers making online payments through SSL or SET protocols need only provide sellers with credit card information. This convenience is a value-added service that can also promote impulsive purchasing.

### **Online payment made**

Online payment systems are an integral part of electronic commerce. An online payment is a financial exchange that takes place in cyberspace between a buyer and seller. The content of the exchange is usually some form of digital financial instrument such as encrypted credit card numbers, electronic checks,

or digital cash that is supported by a bank, financial institution, or other intermediary that establishes legal tender.

Encryption is initiated when credit card information is entered into a browser or other electronic commerce device and sent securely (i.e., encrypted) over a network from buyer to seller. To make a credit card transaction truly secure and irrefutable, the following sequence of steps must occur before goods, services, or funds flow:

- Customer presents credit card information along with an authentic signature or other information (e.g. password) to the online merchant.
- Merchant validates customer's identity and ownership of the credit card account.
- Merchant relays credit card information and digital signature to bank or online credit card processor.
- Bank or processing party, in turn, relays the information to the customer's bank or credit card sponsor for authorization approval.
- Customer's bank or sponsor returns credit card data, charge authentication, and authorization to the merchant.<sup>15</sup>

CyberCash is a company that adheres to the process described above. CyberCash transactions involve three separate client soft-

ware packages; one program resides on the consumer's computer (also known as an "electronic wallet"), another operates as part of the buyer's network server, and one operates within the CyberCash network servers. In essence, the software loaded on the consumer's computer communicates with the "electronic cash registers" on the buyer's server.

Once a buyer purchases an item and receives an invoice presented by the seller, the buyer can access the CyberCash Wallet to click on the "PAY" button. The seller's network server then sends a message to the buyer's computer and the buyer selects which credit card if more than one has been logged for transaction settlement. A series of encrypted messages are automatically transmitted through the three servers to close the purchase process.<sup>16</sup>

#### **Digital check may be preferred**

Electronic or digital checks are modeled after standard paper checks except they rely upon digital signature and public-key encryption. A trusted third party (CA) is involved to authenticate the buyer, the buyer's bank, and bank account. Once a buyer makes a purchase, the buyer electronically transmits a check facsimile to the seller. This information is forwarded to the third party's network server for authorization of payment. The server, in turn, sends the check to the seller's bank for deposit.

Since electronic checks are compatible with current financial

institutional infrastructure, some experts expect digital checks to be a preferred form of electronic payment from the seller's perspective. Coincidentally, buyers also have a preference for electronic checks since they are a form of settlement allowing payees to take advantage of float since there remains a delay before the buyer's account is debited for the transaction.

NetCheck is a prototype electronic checking system that involves an account server that allows organizations to construct a customized in-house, online "bank." This unique virtual bank is then programmed to accept paper checks or credit card payments in exchange for crediting a customer's NetCheck account. The in-house account server is then used to verify the digital signature of the check payer. Once the server verifies the check, it sends a notification to the payee's server and to the payee's bank to secure (i.e., debit) money from the payer's account.<sup>17</sup>

### **Digital cash is popular**

Cash is popular since it enables purchasers to remain anonymous while providing almost unlimited negotiability. Similar to the other electronic payment systems, digital cash relies on public-key and digital signature techniques. A pair of keys are needed to lock (encrypt) and unlock (decrypt) messages, thereby protecting the buyer's asset base. To be equivalent to paper money and coins, digital cash must have the following characteristics:

- **Monetary value:** Digital cash must be backed by actual currency, bank-authorized credit, or a bank-certified cashier's check. Without proper bank certification, digital cash is unreliable and may even be returned due to insufficient funds.
- **Interoperability:** Digital cash must be perceived as equivalent and exchangeable as a valid method of payment. It must be treated similar to other digital cash, paper cash, coins, goods or services, lines of credit, bank account balances, bank notes or obligations, electronic benefit transfers, and the like.
- **Retrievability:** Digital cash must be storable and retrievable. Remote access allows the user to authorize and exchange digital cash from any location. Digital cash can be stored on a PC hard drive, smart card, PDA, or other easily transported standard or special-purpose devices.
- **Security:** Digital cash must be copy-protected and tamper-proof. Obviously, it must be properly secured during an exchange. In order to establish credibility, digital cash must be implemented so that it becomes easy to prevent double spending or counterfeiting.

Currently, a buyer can purchase digital cash from an online

currency server (or bank). To do so, the buyer needs to set up an account with the central online bank and maintain a sufficient account balance to cover purchases. When a withdrawal is initiated, the buyer's computer will distinguish the transaction and transmit the withdrawal amount to the digital bank. The bank will then debit its digital cash reservoir with monies located in the buyer's bank account. However, if the information is not updated in real time, the buyer may be able to double-spend the cash on hand. Thus, it is essential to implement real-time information management to a digital cash transaction system.

An electronic payment system proposed by First Virtual (FV) Holdings allows consumers to pay for purchases through a third party without having to transmit credit card account information. After opening a FV account, the buyer presents his or her account number to the seller. The seller then transmits the buyer's account number to the FV payment server for verification. Once verified, the server sends a return message requesting buyer confirmation of the transaction. Once confirmed, the server authorizes the seller to enable the buyer to download the purchased product or services. Under this scheme, credit card information is not linked to the transaction process.

## References

- <sup>1</sup> "Security: How Safe is the net?" *Business Week* (June 1998): 148-152.
- <sup>2</sup> T.J. Strader and M.J. Shaw, "Characteristics of electronic markets," *Decision Support Systems* 21 (1997): 187.
- <sup>3</sup> D. Henry, S. Cooke and S. Montes, "The emerging digital economy," <http://www.ecommerce.gov>, 1997.
- <sup>4</sup> C. Anderson, "In search of the perfect market," *The Economist* (May 1997): E3-E5.
- <sup>5</sup> "Tremble everyone," *The Economist* (May 1997): E10-E13.
- <sup>6</sup> "Hotels on the web: traffic, bookings rise," *Hospitality Tech Advisor* (June 1998): 1-4.
- <sup>7</sup> D. Boland, "Is your web site ready for e-business?" *Update* (Spring 1998): 17-18.
- <sup>8</sup> D. Berchiolli, "Technology - making a mark in the hospitality industry," KPMG Peat Marwick LLP (1998).
- <sup>9</sup> M. Madley, "Paperless purchasing," <http://www.hotel-online.com>, 1998.
- <sup>10</sup> J. Jesitus, "Promus buys into the Internet," *Hotel & Motel Management* (June 1997): 48.
- <sup>11</sup> H. B. Van Hoof and T. E. Combrink, "U.S. lodging managers and the Internet: perceptions from the industry," *Cornell Hotel & Restaurant Administration Quarterly* 39, No. 2 (April 1998): 46-54.
- <sup>12</sup> W. J. Clinton and A. Gore, "A framework for global electronic commerce," <http://www.iitf.nist.gov/eleccomm/ecom.htm>, 1997.
- <sup>13</sup> A. Bhimani, "Securing the Commercial Internet," *Communications of the ACM* 39, No. 6 (June 1996): 29-35.
- <sup>14</sup> R. Kalakota and A. B. Whinston, "Electronic commerce: a manager's guide," (Reading, Mass.: Addison-Wesley Longman, Inc., 1997): 149-150.
- <sup>15</sup> *Ibid.*: 169-170.
- <sup>16</sup> *Ibid.*
- <sup>17</sup> C. Neuman, "A flexible framework for network payment," R. Kalakota and A.B. Whinston, eds., *Readings in electronic commerce* (Reading, Mass.: Addison-Wesley Longman, Inc., 1997): 229-243.

---

*Michael L. Kasavana* is a professor of Hospitality Information Systems in the School of Business at Michigan State University and *Wonae Cho* is an assistant professor in Hospitality and Tourism Management at the University of Kentucky.