



Altered States:  
Electronic Commerce and Owning the Means  
of Value Exchange

ROBERT D. FRAM\*

MARGARET JANE RADIN\*\*

THOMAS P. BROWN\*\*\*

CITE AS: 1999 STAN. TECH. L. REV. 2 (1999)

[http://stlr.stanford.edu/STLR/Articles/99\\_STLR\\_2](http://stlr.stanford.edu/STLR/Articles/99_STLR_2)

I. PREFACE

¶1 Electronic commerce has been around for a long time. For the better part of two decades, consumers have been able to walk into businesses around the world, hand the clerk a card, and walk out with whatever they desire. To be sure, most of these transactions began with a signature on a paper receipt and ended with a check in the mail, but the intervening steps and, more importantly, the exchange of value among the other interested parties—the business, the acquiring bank, and the issuing bank—happened electronically.

¶2 Electronic commerce, however, is changing, and the catalyst for much of this change (particularly in the United States) is the Internet. Reliable facts and figures about the Internet are difficult to find, but by any count it is growing at a breathtaking rate, from 12.4 million users in the United States in 1995 to 24.8 million users in 1996 to 60 million users in 1998.<sup>1</sup> Driven by this ever-expanding user base, consumer-initiated Internet commerce has exceeded even the most

---

\*Shareholder, Heller Ehrman White & McAuliffe, and co-chair of the firm's Intellectual Property Group.

\*\*Of counsel, Heller Ehrman White & McAuliffe, and the William Benjamin Scott & Luna M. Scott Professor of Law at Stanford Law School.

\*\*\*Associate, Heller Ehrman White & McAuliffe.

<sup>1</sup> See ZD InfoBeads, *PCs Connecting to the Internet by Market Segment as of MY98* (visited Feb. 23, 1999) <[http://www.infobeads.com/InfoBeads/Pages/Viewer/Commentary/Commentary.asp?INFOBEAD\\_ID=C0000960AB](http://www.infobeads.com/InfoBeads/Pages/Viewer/Commentary/Commentary.asp?INFOBEAD_ID=C0000960AB)>; Dataquest, *Worldwide Internet and Enterprise Strategies Market Share*, Table A-19 (July 8, 1997) (estimating 15.3 million users in the United States in 1995 and 28.6 million in 1996).

optimistic forecasts.<sup>2</sup> Consumers are not, however, the sole (or even primary) engine of Internet growth. Recognizing the advantages of belonging to the same networked environment as their customers and suppliers, businesses have also rushed to add their networks to the Internet.

¶3 This digital networked environment is a new means of communication. Just as other developments in communications technology (e.g., the telegraph, telephone, radio, television, satellites, etc.) created new payment systems, so has the Internet. The Internet is not, however, the only catalyst of change in payment systems. The same relentless advances in semiconductor technology that have fostered the development of the Internet have also created new means of exchanging value. The electronic payment systems spawned by these developments fall along a continuum ranging from those that simply extend familiar banking technology, such as end-to-end electronic bill payment systems, to those that break with the past, such as systems that create money in long strings of binary code instead of physical tokens of exchange.

¶4 As information technology plays a larger role in the everyday business of value exchange, the question of ownership of that technology, through the traditional legal means of patent rights, will likely come to the fore in banking and related industries. At the same time, the increasing importance of contracting for information and the role of technology in the contracting mechanisms themselves are giving rise to a new regulatory environment for these industries. Legal advisors to banks and other financial institutions will need to understand how property rights in technology will impact their clients. They must also keep pace with a different and changing contractual and regulatory environment and learn to deal with contracts that are entered into by machines and signatures consisting of bits.

¶5 The purpose of this paper is to lay out a structure in which these emerging legal issues can be understood. It reviews the continuum of electronic payment systems in today's marketplace and discusses the issue of ownership of the technology underlying those systems, focusing on the newly important role of patent rights as applied to various emerging electronic payment systems.<sup>3</sup>

## II. ELECTRONIC PAYMENT MECHANISMS IN TODAY'S MARKETPLACE: WHAT'S NEW?

¶6 Network computing is not new to the payment system industry. For decades, financial institutions have depended upon computer networks to initiate, transfer, and settle payments. The Visa, MasterCard, and Automated Teller Machine (ATM) networks are the best known (at least to consumers), but others exist, including the Federal Reserve's Automated Clearing House (ACH), the New York Clearing House Interbank Payments System (CHIPS), and Society for Worldwide Interbank Financial Telecommunications (SWIFT). These back-end processes—behind the scenes from the consumer's point of view—have been automated for some time.

---

<sup>2</sup> Compare Lawrence Kudlow, *Why the Internet Had a Merry Christmas?*, WALL ST. J., Jan. 6, 1999, at A22 (reporting that consumers spent more than \$13 billion online in 1998) with HAMBRECHT & QUIST, L.L.P., *CREATING LIFELONG CUSTOMER RELATIONSHIPS: WHY THE RACE FOR CUSTOMER ACQUISITION ON THE INTERNET IS SO STRATEGICALLY IMPORTANT* 16, Ex. B (Sept. 1997) (forecasting \$8.5 billion in on-line transactions in 1998).

<sup>3</sup> Appendix A contains a summary of some representative patents in the area, for we believe that the increasing fusion of finance and technology will make such rights increasingly important in the years ahead. See *infra* Part IX.

Automation has taken root more slowly at the point of exchange between and among consumers, merchants, and financial institutions.

¶7 Now both the front-end processes and the connection between the front-end and back-end are being automated. In other words, an end-to-end electronic payment infrastructure is developing. In particular, here's what's new:

- The idea of paying online for products and services.
- The use of an open network (the Internet) for payments and settlements.
- The use of strong cryptography for secure presentation of financial details by consumers.
- The use of strong cryptography for authentication of parties (digital signatures) and message integrity and non-repudiation.
- The use of integrated circuit cards (smart cards) to replace magnetic strip cards in traditional credit and debit card functions.
- The development of digitized cash in which data stored on a disk or chip functions as actual money.
- The use of microprocessors for financial transactions in smart cards, personal digital assistants (PDAs), and other devices, permitting digital money to circulate and settle for periods of time outside the banking systems.

### III. A CONTINUUM OF PAYMENT MECHANISMS

¶8 With these novel features in mind, the payment mechanisms we find in today's marketplace can be placed on a continuum, from those that extend the existing electronic infrastructure to those that break from it. In our view, the emerging continuum looks like this:

- Electronic bill payment by a customer, either with a telephone, home banking software, or personal financial management software.
- End-to-end electronic bill presentment and payment.
- Electronic checks.
- Electronic banking on the Internet.
- Integrated circuit cards (or smart cards).
- Secure presentation of payment cards over the Internet.
- Digital cash implemented on the Internet through money resident on a consumer's hard drive or through a fusion of PCs and smart cards.
- Digital cash optimized for micropayments for information goods.

¶9 Companies such as IBM are integrating these payment systems with the delivery of information goods and other aspects of contracting and transacting, such as EDI,<sup>4</sup> subscription management, catalogue production, inventory control, and

---

<sup>4</sup> Electronic Data Interchange (EDI) refers to sets of standards developed by ANSI and the United Nations to structure business-to-business exchange of data (such as bid requests, purchase orders, and records). EDI has been used by large firms over private networks called VANs (Value Added Networks). As electronic commerce develops, EDI will migrate to the Internet and will integrate inventory control, purchasing, and payment mechanisms, so that, for example, a manufacturing firm could substantially automate its purchasing function. Integration of EDI with financial functions may present a significant opportunity for financial institutions, and Bank of America has been a leader in exploring this field.

procurement. Although this paper will touch on integrated systems in several contexts in order to illustrate the continuing development of payment systems, full treatment of integrated systems is beyond its scope. Consistent with our goal of illuminating the new payment systems landscape and illustrating the growing importance of intellectual property rights, this paper will describe the payment mechanisms themselves rather than discuss how they can be embedded in larger systems.

#### IV. BUSINESS CONCERNS AND THE VARIETIES OF PAYMENT MECHANISMS

¶10 Payment mechanisms, old and new, have developed to meet the needs of the marketplace. Just as certain structures (packages of functional features) that work well in certain contexts have become standard in the physical world—checks, cashier’s checks, traveler’s checks, letters of credit, cash, credit cards, debit cards, and so on—we expect that certain standard functional structures will also coalesce in the digital world. These functional structures will be related to a number of concerns common to all payment systems. The structures that coalesce for electronic payment mechanisms may not be exactly analogous to the array of payment mechanisms in the physical world, because of differing cost and demand structures in the networked digital environment. These new cost and demand structures are evolving and not yet fully understood, so no one can say with confidence which digital payment structures will survive and thrive in the marketplace.

##### A. *Float*

¶11 The question of who has the use of funds while a transaction is in progress, as well as before and after the transaction, is of paramount economic importance to financial institutions. Traditional payment mechanisms run the gamut on this issue, from credit cards (which can allow the holder a “free” loan during the grace period after purchases but before payment) to traveler’s checks (which give the issuer the funds before the holder spends them). Electronic payment mechanisms will also vary widely on the dimension of which party has the float, at what point in the transaction process the party has it, and for how long. As in the physical world, we can say that, *ceteris paribus*, financial institutions will find prepayment arrangements (such as the smart card stored-value systems discussed below<sup>5</sup>) advantageous.

##### B. *Risk of Loss*

¶12 As with the allocation of float, traditional payment mechanisms differ in how they allocate the risk of loss from fraud, system malfunction, negligence, and so on. The risk of loss of cash, for example, is with the holder. We expect electronic mechanisms to vary analogously in response to the cost and demand structures of the developing digital environment. For example, if digital cash is stored on the hard drive of the customer’s computer, as in the DigiCash system (described below<sup>6</sup>), then a computer crash may result in a loss for the customer. Security measures, as outlined below, will develop in response to the magnitude of exposure to risk of loss and who bears it.

---

<sup>5</sup> See *infra* Part VI.D.

<sup>6</sup> See *infra* Part VI.E.1.

¶13 A particular kind of risk of loss for customers in prepayment systems, known as slippage, may become important in the world of digital payment mechanisms. Slippage occurs when the customer loads value on a disposable card, such as a phone card, for example, then discards the card without using up all the value. This kind of small loss for individual customers can add up to substantial aggregate gains for financial institutions, which is one reason that a number of financial institutions are putting substantial effort into developing prepayment systems.

### C. Security

¶14 Whereas locks and bullet-proof glass help ensure security in the physical world, authentication of signatures and assurance of message integrity help ensure security in the digital world. Authentication of signatures identifies parties, and message integrity prevents the alteration and repudiation of transactions. Cryptography can do both, protecting against several types of fraud:

- *Theft*: Encryption of messages is used to prevent attackers from stealing credit card numbers or messages that function as cash.
- *Alteration*: Encryption is also used to prevent attackers from altering messages (so that a digital message worth \$10 does not become a digital message worth \$1,000,000).
- *Man-in-the-Middle Attack*: Authentication is used to prevent attackers from posing as merchants in order to steal credit card numbers or have cash transferred to them. Authentication also prevents attackers from intercepting all communications between two other parties and lifting any transferred funds.
- *Replay Attack*: A message authentication code gives each message a unique sequence number in order to prevent an attacker from capturing a funds transfer message and repeatedly transmitting the same message for his or her own use.
- *Repudiation*: A message authentication code also can prevent a party from denying the fact or circumstances of a transaction.

¶15 In large part, cryptography has made electronic payment possible. Cryptography with sufficient key lengths is widely trusted to repel attacks by unauthorized third parties, who either use “brute force” (harnessing computers to try every possible key looking for the one that will work) or work via a “back door” (taking advantage of a mathematical property of the encryption algorithm to shorten the process of looking for the key).

¶16 Yet cryptography is not all there is to security. Loss and theft can occur before information is encrypted or after it is decrypted. Keys must be kept secret, and people must be responsible for them. People must also be responsible for decryption and working with plaintext. Human error, vulnerability, and corruptibility will still be weak points. Other weak links abound. The ease of copying bits makes the counterfeiting of digital cash a much more serious problem than the counterfeiting of physical currency. The physical security of microprocessors used for payment itself is also a serious problem when devices are widely distributed, especially since it is easier to gain access to the memory of a smart card than to that of a mainframe.

#### D. *Efficiency*

¶17 New electronic payment systems will replace existing payment systems only if they exchange value efficiently. Efficiency is a particular concern for electronic substitutes for cash and systems designed to permit microtransactions (e.g., the payment of a fraction of a cent for a small piece of information). Existing back-end financial systems, which support existing payment systems, were not built with electronic commerce in mind. Those systems are both difficult to interface with and costly to replace. Moreover, security of a payment system comes at some cost. As security increases, the cost of computation involved in each transaction also rises. This concern might prove particularly troublesome for systems that authenticate transactions through one server rather than on the fly or through multiple servers.

#### E. *The “Payments Franchise”*

¶18 The term “payments franchise” refers to the traditional market dominance of banks and financial institutions in the fields of money transfer. In what might be viewed as a trade-off, the financial industry long ago accepted significant government regulation in return for its payments franchise. In the transition to electronic payment systems, many non-bank firms, such as Microsoft and IBM, may make significant inroads on the traditional market dominance of banks and financial institutions.

¶19 One way non-bank firms might capture a significant market share in payments transfer is by taking control of the customer interface—that is, the images and text which appear on the customer’s screen. If a consumer’s screen shows the software company’s logo and not his or her bank’s, and the consumer can use any bank with the same software, the customer bases of banks may erode. Financial institutions are evaluating the payment systems described in this paper and other emerging payment systems partly on the basis of how they structure the customer interface.

### V. PLAYERS IN THE EVOLVING PAYMENT SYSTEMS INDUSTRY

¶20 Many firms, some familiar—e.g., Visa, MasterCard, Citibank, IBM, Microsoft, and Intel—and some not—e.g., CyberCash, Inc.—are staking claims to digital payment systems. Some are trying to protect existing franchises. Others are attempting to capture new business. Some are licensing systems from other developers. Others are inventing their own. Whatever their respective strategies, these firms are altering the industry’s competitive landscape.<sup>7</sup>

#### A. *Visa*

¶21 Long an innovator in the payment systems industry, Visa is currently pursuing a number of initiatives to preserve its position as the leading provider of electronic payment systems. To make the Internet hospitable to payment card transactions, Visa, along with MasterCard, developed the Secure Electronic Transactions (SET)

---

<sup>7</sup> This discussion, like the discussion of emerging payment systems which follows, is illustrative, not exhaustive. New players (and systems) emerge virtually every day.

standard.<sup>8</sup> Visa also unveiled the VisaCash card (a stored value card) at the 1996 Summer Olympics in Atlanta and, together with MasterCard, tested interoperability in late 1997 in Manhattan. Visa is also working on an end-to-end electronic billing system, ePay.<sup>9</sup>

#### B. MasterCard

¶22 MasterCard, with Visa, developed the SET standard for credit card payments. MasterCard also acquired fifty-one percent of Mondex International, a leading stored-value/smart-card company, early in 1997.

#### C. AT&T

¶23 AT&T was one of two American members of the consortium of seventeen global banks and financial institutions that founded Mondex International (the other was Wells Fargo).<sup>10</sup> Today, AT&T is promoting an integrated merchant software program for electronic commerce called Secure Buy,<sup>11</sup> which is based on Open Market, Inc.'s systems.<sup>12</sup>

#### D. IBM

¶24 In October 1997, IBM launched a major marketing campaign for its electronic commerce services. Its services are meant to create customized integrated systems for businesses wishing to create and maintain commercial Web sites, and to interface with systems that might already be in place. IBM offers what it describes as a "network computing framework for e-business". This framework is not a specific product but rather packages IBM's ability to help businesses integrate many aspects of their activities with the online environment.

¶25 IBM assisted in the development of the SET standard and is now trying to implement it. In September 1997, IBM launched a comprehensive set of electronic commerce programs called CommercePOINT Payment. These programs incorporate the SET technical standards for safeguarding payment card purchases made over the Internet and cover the entire payment process.<sup>13</sup>

¶26 In addition to the CommercePOINT family of products, IBM is involved in another major SET initiative, a joint project being conducted with Chase Manhattan Bank USA N.A., First Data Corporation, GlobeSet, MasterCard, and Wal-Mart. The project allows users of the Wal-Mart MasterCard from Chase to make purchases from Wal-Mart On-line, Wal-Mart's electronic commerce site.<sup>14</sup>

---

<sup>8</sup> For a further discussion of SET and other efforts to open the Internet to payment card transactions, see *infra* Part VI.C.2.

<sup>9</sup> For a further discussion of ePay and other developments in electronic bill payment systems, see *infra* Part VI.A.

<sup>10</sup> *Id.*

<sup>11</sup> See AT&T, *AT&T SecureBuy Service* (visited Jan. 26, 1999) <<http://www.ipsservices.att.com/wss/securebuy>>.

<sup>12</sup> See Open Market, Inc., *Open Market's Commerce Service Providers* (visited Jan. 26, 1999) <<http://www.openmarket.com/partners/csp>>.

<sup>13</sup> See IBM Corp., *IBM Payment Suite* (visited Jan. 26, 1999) <<http://www.software.ibm.com/commerce/payment/>>.

<sup>14</sup> See IBM Corp., *IBM Provides Software and Services for First Secure Electronic Transaction Pilot in Canada* (visited Jan. 26, 1999) <<http://www.can.ibm.com/ebusiness/set/>>.

¶27 IBM is developing a micropayment system, MiniPay, to enable small transactions in information over the Internet.<sup>15</sup> IBM is also developing a digital rights management system, or trusted system, called Cryptolope.<sup>16</sup> This technology uses encryption techniques to protect and control digital content so that it can be licensed or sold for particular uses. Systems of this kind are also being developed by Xerox and Citibank, among others.

E. *Microsoft*

¶28 Although Microsoft has kept its specific plans secret, the firm hopes to capture major sectors of the electronic commerce market.<sup>17</sup>

¶29 *PC Financial Software.* Microsoft offers two programs, Money 98 and Money 98 Financial Suite, which help consumers keep track of and automate their household finances. These programs help consumers pay bills, manage accounts, bank online, and create budgets. They also include features for long-term investing and financial planning. In addition, Money 98 allows users to download bank and brokerage statements from over 100 participating financial institutions nationwide. Microsoft has offered Money 98 to PC manufacturers for pre-installation, and Acer America Corp., Compaq Computer Corp., Dell Computer Corp., Gateway 2000 Inc., Packard Bell, NEC, Sony Corp., and Toshiba America Information Systems have all elected to pre-install it.

¶30 *Online Billing.* In June 1997, Microsoft announced that it had formed a joint venture with First Data Corp. According to Microsoft and First Data, the new joint venture, MSFDC, will allow merchants to send bills to and receive payments from consumers online.<sup>18</sup> This new service will use existing payment systems and support a number of Internet pathways, including Web browsers, e-mail, personal finance managers, and Internet “push” technologies.<sup>19</sup> The joint venture planned to start field trials with banks and billers in late summer 1997. To evaluate the progress of the venture, Microsoft and First Data have formed an advisory board which includes a number of major financial institutions (including American Express Company, Bank of America, and Citibank), industry associations (including the American Gas Association, the Edison Electric Institute, and the United States Telephone Association), and billing service providers (including CSG Systems and International Billing Services).<sup>20</sup>

---

<sup>15</sup> See IBM Corp., *Mini-Pay Contents* (visited Jan. 26, 1999) <<http://www.hrl.ibm.com/mpay/docs/presentations/mpay-dev/mpay-devc.htm>>.

<sup>16</sup> See IBM Corp., *Cryptolopes* (visited Jan. 26, 1999) <<http://www.software.ibm.com/security/cryptolope/>>.

<sup>17</sup> Nathan Myrvold, Microsoft’s chief technology officer, has been quoted as saying that Microsoft’s goal is to receive a “vig” (short for “vigorish,” meaning a cut) in every electronic transaction using a Microsoft program. See David Bank, *Microsoft Moves to Rule On-Line Sales*, WALL ST. J., June 5, 1997, at B1. The *Wall Street Journal* quoted a Microsoft internal memo stating that Microsoft will offer consumers both electronic information and the means to act on it: “We are challenging old and established businesses like newspapers, travel agencies, automobile dealers, entertainment guides, travel guides, Yellow Pages directories, magazines and over time many other areas . . . We must devise ways of working with them or winning away their customers and revenue streams.” *Id.*

<sup>18</sup> See Microsoft Corp., *Citibank to Join Microsoft and First Data Joint Venture (MSFDC)* (visited Jan. 27, 1999) <<http://www.microsoft.com/presspass/press/1998/sept98/citibkpr.htm>>.

<sup>19</sup> See *id.*

<sup>20</sup> See TransPoint, *TransPoint — About, Advisory Board* (visited Feb. 23, 1999) <<http://www.msfdc.com/about/advisory.htm>>.

- ¶31 *Online Trading.* Online trading programs allow consumers to track securities; keep up to date with market summaries, company news, and editorials; locate investment opportunities; research individual companies and mutual funds; and receive notice of significant market movements.
- ¶32 *Online Transaction Protocols.* Microsoft, Intuit, CheckFree introduced a financial transaction protocol called Open Financial Exchange (OFX) in January 1997.<sup>21</sup> OFX combines existing specifications, specifically Microsoft Open Financial Connectivity, Intuit's Open Exchange, and CheckFree's electronic banking and payment protocols. Microsoft's commerce software for banks and financial institutions that need to create Web sites to support financial transactions, Microsoft Internet Finance Server Toolkit, uses OFX.<sup>22</sup>
- ¶33 *Wallet Software.* Microsoft also has its own wallet software, although it is not clear whether Microsoft licenses the wallet from another developer or has developed its own.<sup>23</sup> The Microsoft Wallet is a software payment program that allows consumers to store private information on their PCs and access the information on demand and in a secure environment.<sup>24</sup> The Wallet supports various payment mechanisms such as credit cards, digital cash, and micropayments. The Wallet acts as a plug-in with Netscape Navigator and an Active X control with Internet Explorer. Microsoft shipped the Wallet as part of Internet Explorer 4.0 and will include it in the next version of the Windows operating system, code named Memphis.<sup>25</sup>
- ¶34 *Business Software.* The Wallet was developed to complement Microsoft's merchant server software package. The merchant software program, now called Site Server, Enterprise Edition, integrates various programs in order to make creating and managing online commerce sites easier.<sup>26</sup> Its Commerce Server program supports electronic catalog management, online order processing, and the creation of product and price promotions. Its Buy Now capability lets merchants embed product information and order forms in online ad banners, allowing them to promote and sell without complete online stores. Microsoft is also developing software for business-to-business commerce, to build on existing EDI (Electronic Data Interchange) systems.<sup>27</sup>
- ¶35 *Smart Cards.* Microsoft, along with important hardware manufacturers such as Bull and Schlumberger Ltd, is a member of the PC/SC (Personal Computer/Smart

---

<sup>21</sup> See Intuit Inc., *Intuit, Microsoft and CheckFree create Open Financial Exchange* (last modified Jan. 17, 1997) <[http://www.intuit.com/corporate/press\\_releases/011697.html](http://www.intuit.com/corporate/press_releases/011697.html)>.

<sup>22</sup> See Microsoft Corp., *Microsoft Charts Course for Version 2.0 of Internet Finance Server Toolkit* (visited Jan. 27, 1999) <<http://www.microsoft.com/presspass/press/1998/apr98/mifstpr.htm>>.

<sup>23</sup> See *infra* Part VI.C.2.c.

<sup>24</sup> See Microsoft Corp., *Microsoft Enhances Internet Commerce Strategy* (visited Jan. 27, 1999) <<http://www.microsoft.com/presspass/press/1997/may97/intcompr.htm>>.

<sup>25</sup> Various suppliers of payment software, credit card processors, banks, and financial institutions are working with Microsoft to incorporate their payment systems into the Microsoft Wallet. Among the payment and security technology companies are CyberCash, Inc., DigiCash, First Virtual Holdings Inc., GCTech, Inc., GO Software, Inc., GTE CyberTrust™, IC Verify, GlobeSet, Inc. (formerly Interval, Inc.), Merchant Technical Services, Paylinx Corp., RSA Data Security, Inc., Tellan Software, Inc., Trintech, Inc., VeriFone, Inc., and VeriSign, Inc. Financial institutions and processors include: American Express, Bank America Merchant Services, Barnett Bank, Cardservice International, Inc., e-COMM, First Data Corporation, GZS, JCB, MasterCard International, Old Kent Merchant Services, Royal Bank of Canada, SSB - Società per i Servizi Bancari, Sumitomo Credit Service, Unified Merchant Services (a First Data Corp./NationsBank Venture), Visa International, and Wells Fargo.

<sup>26</sup> See *supra* note 24.

<sup>27</sup> See *id.*

Card) Work Group, which has been developing specifications for integrating smart cards with PCs.<sup>28</sup> In August 1997, Microsoft announced the worldwide free availability of the Microsoft Smart Card Software Development Kit, using PC/SC Work Group specifications to enable Windows and Windows NT operating systems for smart card use.<sup>29</sup> Users will be able to insert a smart card device into a PC smart card reader to log onto their computer or a larger network, view and send messages, conduct online banking, make purchases, and communicate securely with personal and professional contacts. Microsoft claims that manufacturers, including Gemplus, HP, IBM and Schlumberger want Windows to become the smart card platform and that Windows-based smart cards and readers will be shipped soon.<sup>30</sup>

F. *Pandesic (Intel/SAP).*

¶36 In August 1997, Intel and SAP, the preeminent German software firm, formed a new electronic commerce joint venture, Pandesic.<sup>31</sup> Shortly thereafter, Pandesic unveiled its integrated system, the Pandesic Internet business solution.<sup>32</sup> According to Pandesic, this product will handle all of a firm's Internet commerce functions, including marketing, order processing and fulfillment, inventory pricing, materials management, tax handling, payment processing, shipping and handling, financial reporting, and vendor-payment processing.<sup>33</sup> Pandesic, however, has not developed a new payment system. Instead, it will rely upon CyberCash to provide these services.<sup>34</sup>

VI. REFRACTING THE ELEMENTS OF THE (NEW) PAYMENT CONTINUUM

¶37 The payment systems industry is changing rapidly, and its course is far from clear. Some of the industry changes will be incremental, while others will be revolutionary. At this point, only one thing is certain: payment systems and the patents that purport to cover them are proliferating. The systems discussed below (and the patents discussed at greater length in the Patent Appendix<sup>35</sup>) are but a sample.

A. *Modest Extension of the Existing Payment Systems Infrastructure: Electronic Bill Payment.*

¶38 "Electronic bill payment" systems have been around for quite some time. Today, most electronic bill payment systems are not entirely electronic. Instead, some entity in the bill payment chain moves information from the real world to the digital world (and, likely, back again). Next-generation bill payment systems will be

<sup>28</sup> See Microsoft Corp., *PC/SC Workgroup to Develop Open Technology for Integrating Smart Cards and Personal Computers* (visited Feb. 23, 1999) <<http://www.microsoft.com/presspass/press/1996/sept96/smcdrpr.htm>>.

<sup>29</sup> See Microsoft Corp., *Microsoft Announces Availability of Smart Card SDK; Full Support for Windows Enables New Generation of Smart-Card Solutions* (visited Jan. 27, 1999) <<http://www.microsoft.com/presspass/press/1997/aug97/smtcrdrpr.htm>>.

<sup>30</sup> See *id.*

<sup>31</sup> See Pandesic LLC, *SAP and Intel Form New Company to Develop Internet-Based Electronic Business Solution* (visited Jan. 27, 1999) <[http://www.pandesic.com/press\\_releases.asp?MODE=display&PRNUM=16](http://www.pandesic.com/press_releases.asp?MODE=display&PRNUM=16)>.

<sup>32</sup> See Pandesic LLC, *Pandesic LLC Introduces Industry's First Comprehensive Turnkey Electronic Commerce Solution* (visited Jan. 27, 1999) <[http://www.pandesic.com/press\\_releases.asp?MODE=display&PRNUM=15](http://www.pandesic.com/press_releases.asp?MODE=display&PRNUM=15)>.

<sup>33</sup> See *id.*

<sup>34</sup> For more on CyberCash, Inc. and its Internet-based payment products, see *infra* Part VI.C.2.c.

<sup>35</sup> See *infra* Part XI.

fully electronic, taking advantage of the new paths of interconnection between businesses, banks, and consumers.

¶39 CheckFree is the leading supplier of electronic bill payment systems to banks and other financial institutions.<sup>36</sup> Its patented system<sup>37</sup> is a classic example of a traditional electronic bill payment system:

- To use the CheckFree system, a consumer must enter his or her billers' names, addresses, and telephone numbers into the CheckFree software. For each payment, the consumer must also enter his or her account (or invoice) number and the amount of payment. The software stores the information so that the next time a bill is due, the customer can pay it without reentering all of the account information.
- Using this information, the software debits the payment amount from the customer's account and sends it to the biller by either electronic funds transfer or check.
- Billers receiving payments from many CheckFree users get one check (or electronic funds transfer) and a list indicating the amount paid by each customer. This procedure is known in the industry as "check and list."

¶40 As of third quarter 1997, CheckFree supplied electronic bill payment systems to 276 financial institutions, including Bank of America and Wells Fargo, for the use of their customers.<sup>38</sup>

¶41 Although the best known, CheckFree's system is not the only electronic bill payment system.<sup>39</sup> Online Resources and Communications, Inc. also offers an electronic bill payment system. Its system differs from CheckFree's in two respects: It uses the ATM network to process transactions and settles accounts in real time. Like CheckFree, Online Resources relies on the "check and list" system, in which each biller gets one check and a list explaining which customer paid what. Also, like CheckFree, Online Resources holds a patent for its system.<sup>40</sup> Currently, Online Resources serves more than 300 U.S. banks and credit unions.<sup>41</sup>

¶42 Next-generation electronic bill payment systems try to avoid moving information from the real world to the digital world and back again. At this point, three different next-generation methods have emerged: consumers paying bills electronically at their financial institutions' Web sites; consumers paying bills electronically at their billers' Web sites; and customers prompting their financial institutions to transfer funds electronically to their billers' financial institutions.

¶43 CheckFree's second-generation product, E-Bill, will electronically present and pay bills. E-Bill allows a consumer to designate his or her financial institution as his or her electronic bill presentment address. To pay a bill with E-Bill, a consumer will have to visit his or her financial institution's Web site. CheckFree is currently

---

<sup>36</sup> See CheckFree Corp., *CheckFree Corporation* (visited Mar. 7, 1999) <<http://www.checkfree.com>>.

<sup>37</sup> See *infra* Part IX.B.1.

<sup>38</sup> Banks and other financial institutions seem to like one aspect of the CheckFree system in particular—the ability for banks to modify the software so that it displays their brands, not CheckFree's, to consumers. CheckFree also works with personal finance software such as Microsoft Money and Intuit.

<sup>39</sup> For a time, Visa also competed against CheckFree with Visa Interactive. In August 1997, however, Visa sold Visa Interactive to the Integriion Financial Network, a consortium of 17 financial institutions (including Visa) and IBM, which entered into a 10-year partnership with CheckFree Integriion.

<sup>40</sup> See *infra* Part IX.B.2.

<sup>41</sup> See Online Resource & Communications Corp., *Company* (visited Apr. 8, 1999) <<http://www.orcc.com/company.htm>>.

marketing this system to mass billers (e.g., gas companies, power companies, department stores) as well as to financial institutions.<sup>42</sup> In October 1997, Chase Manhattan Bank licensed E-Bill and announced that it expects to become the first bank in the United States to provide fully electronic bill presentment and payment to its customers.

¶44 Visa also has a second-generation electronic bill payment system, ePay. ePay is not an electronic bill presentment system. Instead, businesses participating in ePay continue to send out paper bills but let consumers know that they participate in an electronic billing network. The ePay system works as follows:

- Billers enter data into a Universal Biller File sent to all participating institutions (billers' banks and customers' banks).
- The customer receives a paper bill, and then tells its own (participating) institution to pay using the biller's ID.
- The customer's institution debits the customer's account and deposits payment directly into the biller's account at the biller's institution.

Visa has patented the ePay system.<sup>43</sup>

B. *Another Modest Extension of the Existing Payment System Infrastructure: "Electronic Checks."*

¶45 Electronic checks are another way in which existing banking channels are being enhanced and augmented by new technologies. An electronic check is an electronic message from a payor to a payee that debits the payor's account in favor of the payee's account when the check clears. After the payor transmits the message to the payee, the payee transmits the message to a financial institution at which it has an account, and the payee's institution transmits the message back to the payor's institution. Electronic checks will contain the same information as paper checks: the payor's financial institution and account number, the date, the name of the payee, and the signature of the payor.

¶46 The electronic check project of the Financial Services Technology Consortium (FSTC) is probably the most advanced. The FSTC currently has about sixty members, including banks (such as Bank of America) and government entities (such as the ).<sup>44</sup> The FSTC electronic check system envisions a secure hardware "electronic checkbook" device that plugs into a consumer's PC. The device will store encryption and identification information and maintain the electronic equivalent of a check register. Funds flow through the FTSC system in four ways:

- *Deposit and Clear.* The payor writes and sends a check to the payee using secure e-mail. The payee endorses the check using his own secure hardware device and forwards it to his bank. The bank performs a clearing function with the payor's bank through existing check clearinghouses.
- *Cash and Transfer.* The payee receives the electronic check and cashes it by transmitting it to the payor's bank. The payor's bank then credits

<sup>42</sup> See CheckFree Corp., *CheckFree Corporation* (visited Mar. 11, 1999) <<http://www.checkfree.com/index-info.html>> (listing companies for which CheckFree provides bill presentment services).

<sup>43</sup> See *infra* Part IX.B.3.

<sup>44</sup> The FTSC is also working on a Bank Internet Payment System that will allow for payment through the Internet and implement an Electronic Payments Handler that will permit secure communication between existing back-end systems and public networks.

the payee's bank account using conventional interbank electronic funds transfer. In order for funds to flow in this scenario, the payee and its bank must be able to accept electronic checks.

- *Special Purpose Account (Lockbox)*: The payor sends the electronic check to the payee's bank or to a third party maintaining a special-purpose account for the payee, known as a lockbox. This party receives the electronic check, debits the payor's account, and credits the payee's accounts receivable.
- *Funds Transfer*: The payor sends the electronic check to her own bank, which debits her account and uses conventional interbank electronic funds transfer to credit the payee's bank.

¶47 CyberCash, Inc. also claims to have developed an electronic check mechanism. CyberCash calls its system PayNow. Although little is known about the system, CyberCash claims that the system provides for electronic payments directly from existing checking accounts. The system apparently runs on a consumer's PC and creates messages that function as electronic checks.<sup>45</sup>

### C. *Digital Transactions: Payment Cards on the Internet.*

¶48 From the day the Internet opened to commercial traffic, the possibility of interactive home shopping has attracted a great deal of attention and investment. Initial forays took some time to get off the ground but have now taken flight, witnessed by the breathtaking market capitalizations of ".com" stocks such as Amazon.com and eBay.<sup>46</sup> Notwithstanding this incredible growth, some industry observers, apparently including the Antitrust Division of the Department of Justice, believe that even more shopping would occur online if the security of payment were guaranteed.<sup>47</sup> Although consumers have yet to clamor for even one solution to this problem, two solutions have emerged: keep sensitive information off the Internet altogether or encrypt it before it gets there.

#### 1. *Keeping Sensitive Information off the Internet.*

¶49 One electronic commerce start-up, First Virtual, has tried to solve the Internet security problem by keeping secure information off the Internet. First Virtual designed its system with small-scale sellers of information products in mind. Its scheme does not use encryption. The First Virtual system works as follows:

- A consumer uses the telephone to open an account at First Virtual. During that conversation, the consumer gives First Virtual his or her payment card information.
- In return, First Virtual gives each customer an account number and a PIN.

---

<sup>45</sup> See CyberCash, Inc., *Cybercash Interactive Billing and Payment* (visited Mar. 7, 1999) <<http://www.cybercash.com/cybercash/billers/introduction.html>> (summarizing the PayNow system for consumers).

<sup>46</sup> As of March 10, 1999, the market capitalization for Amazon.com was over \$21 billion, and that of eBay was over \$19 billion. For up-to-date market capitalization, see NASDAQ Corp., *Infoquotes* (visited April 8, 1999) <[http://www.nasdaq-amex.com/asp/quotes\\_full.asp?symbol=AMZN&symbol=EBAY&selected=AMZN](http://www.nasdaq-amex.com/asp/quotes_full.asp?symbol=AMZN&symbol=EBAY&selected=AMZN)>.

<sup>47</sup> See U.S. Dept. of Justice, *DOJ - Antitrust*, (visited Mar. 7, 1999) <[http://www.usdoj.gov/atr/public/press\\_releases/1998/1974.htm](http://www.usdoj.gov/atr/public/press_releases/1998/1974.htm)> (announcing antitrust suit against Visa and MasterCard for, among other things, failing to develop quickly enough "systems to permit secured card transactions over the Internet").

- A customer wanting to buy something over the Internet sends his or her PIN to the seller. The seller then uses that PIN to communicate with First Virtual.
- First Virtual sends the customer an e-mail seeking confirmation of the transaction.
- If the consumer confirms the transaction, First Virtual uses the consumer's payment card to pay the merchant.

¶50 First Virtual's system has simplicity in its favor, but there are drawbacks. For one thing, it may be open to fraud by both merchants and consumers. Merchants may be able to defraud First Virtual (and consumers) by reporting false transactions and intercepting the confirming e-mails sent to customers. Customer can defraud First Virtual (and merchants) by refusing to confirm transactions, although First Virtual will cut off a customer who does this too often. Also, the system is somewhat cumbersome. To consummate a First Virtual transaction, both the buyer and the seller must establish a First Virtual account. (This feature is common to a number of electronic payment mechanisms.) Finally, the First Virtual system is expensive. First Virtual charges merchants 29 cents plus 2 percent on every transaction, plus an additional dollar for wire transfers.

2. *Securing Payment Card Information with Encrypted Transmission.*

¶51 The other, and seemingly more sensible, approach to payment card transactions attempts to secure information through encryption before transmission. One company, CyberCash, entered this field early. Since then, two important standards have emerged: the Secure Electronic Transactions (SET) standard, which is jointly sponsored by Visa and MasterCard, and the Transport Layer Security (TLS) standard, which is based upon Netscape's Secure Socket Layer (SSL) program and has been included in a recent Internet draft.<sup>48</sup>

¶52 TLS and SET, although both designed to protect financial information through the use of encryption, have somewhat different aims. TLS will supplement the basic Internet protocols (TCP/IP). TLS enables a client computer and a server computer to establish a secure transmission channel, by communicating with each other to find out which security protocols they have in common (from among a broad range supported by the TLS standard) and then selecting one to use. The SET standard, on the other hand, specifies particular security protocols that must be used and spells out in detail a set of messages that will complete a secure payment card transaction, without any need for first establishing a secure channel. SET's boosters hope that it will prompt software developers to create compatible programs that permit consumers to use their payment cards on the Internet.

a) *SSL*

¶53 Netscape offers its patented Secure Socket Layer (SSL) program as part of its browser software. The program has also been included in the latest draft of the Internet Transport Layer Security (TLS) standard. Microsoft once used its own analogous program but now has included SSL in its browser software.

¶54 SSL allows customers to send payment card numbers through the customer's browser to merchant sites on the World Wide Web. The customer does not see its

---

<sup>48</sup> See also discussion of the patents assigned to Open Market, Inc., *infra* Part IX.E.1.

operation, except through icons indicating secure transmission and dialog boxes explaining shifts from secure to insecure modes or vice versa. Most people who have purchased anything by transmitting credit card information over the Internet—for example, books from Amazon.com—have used SSL.

¶55 The SSL protocol is designed to use encryption to thwart various kinds of fraud, including replay and man-in-the-middle attacks, so that payment card transactions through the Web can be handled like old-fashioned mail/telephone order transactions. The SSL protocol can handle various kinds of encryption, giving it the ability to operate on different systems:

- When payment is made through SSL, the seller must have an SSL-enabled Web server, and the buyer must have a browser containing SSL client software. The server has a certificate signed by a certificate authority trusted by the client software.
- When the customer decides to buy something, the software provides a form in which the customer's name, address, and payment card number can be entered. The client software requests a URL whose address begins with "https://" instead of "http://," to indicate that SSL is to be used.
- The merchant's computer (the server) authenticates itself and the customer's computer (the client) may authenticate itself. The two computers run a "handshake" program that enables them to choose an encryption program common to both of them.
- Then the buyer's payment card information is sent to the server in encrypted form, where it can be decrypted and processed by the merchant in the same way as a mail or telephone order.

b) SET

¶56 Visa and MasterCard, with assistance from Netscape, IBM, and Microsoft, jointly developed the SET standard.<sup>49</sup> SET uses encryption and digital signatures at every step of the payment card processing path. SET is not a software program but a standard that its sponsors hope will encourage software companies to develop software to its specifications. Companies will likely supplement SET compliance with features like a graphical user interface, such as "wallet" software on the user's computer, and other programs for shopping, price negotiation, etc.

¶57 SET adds one feature to the existing payment card infrastructure: the capability to use the Internet. That feature creates an end-to-end secure processing system. When a cardholder initiates a payment with a merchant using software that implements SET, the merchant uses SET-compliant software to seek authorization of the payment from an entity called a payment gateway (typically operated by an acquirer). The payment gateway is a bridge to the existing payment card network.

¶58 The SET standard defines the encrypted messages that each of these parties (the cardholder, the merchant, the payment gateway) will use to communicate with the others. In addition, SET defines the role of a fourth party, the certificate authority, which authenticates the other parties to each other by means of digital certificates.

---

<sup>49</sup> For a downloadable copy of the SET specifications, see SET Secure Electronic Transactions LLC, *The SET Standard Specifications* (last modified May 31, 1997) <<http://www.setco.org/download.html>>.

- ¶59 Each of the four types of participants uses a combination of DES secret key cryptography and RSA public key cryptography to encrypt the payment card information as it travels among them. Messages are first encrypted with 56-bit DES keys, which are then transmitted between two parties using 1024-bit RSA public key cryptography as a digital envelope. This means that the sending party encrypts the DES key with the public key of the receiving party, so that only the receiving party can decrypt it (using its private key), then use the DES key to decrypt the message.<sup>50</sup>
- ¶60 SET relies upon digital certificates to verify that public keys actually belong to the parties they should. A digital certificate is a verified signature in digital form, consisting of the certificate authority's own digital signature on the customer's cryptographic public key. The public key is then used by others to encrypt information addressed to the customer, which only the customer's private key can decrypt. Certificates are obtained by proving one's identity to the certificate authority firm. Such proof is outside the networked digital environment—for example, the firm might require that the applicant show a photo ID and proof of residence or employment.<sup>51</sup>
- ¶61 How will the parties know that the certificate authority's signature is itself genuine? SET envisions a hierarchy of certificate authorities.<sup>52</sup> Each customer will have his or her own public-key pair packaged in a certificate which includes the digital signature of the card issuer. This digital signature is generated by the cardholder certification authority (CCA). Above the CCA will sit the Brand CA (a certification authority established by each brand such as Visa or MasterCard). At the top of the hierarchy will sit the Root CA with a Geopolitical CA guaranteeing signatures in different countries or jurisdictions. Merchants may also have their own certification authority (the MCA) so that customers can verify the authenticity of the merchant.
- ¶62 In addition to providing for identity authentication through the use of certificates, SET provides for message integrity and authenticity through the use of RSA public key cryptography in combination with a message digest or hash. A digest is produced when a special algorithm called a secure hash function is applied to a message to produce a string of bits shorter than the message itself. The secure hash function has the mathematical property that it is extremely unlikely that two different messages could have the same digest, and it is extremely unlikely that a message could be recreated from its digest.
- ¶63 When a recipient receives a message together with a digest, the recipient can use the same secure hash function to recompute the digest to assure himself that the message has not been altered. Moreover, a message digest when combined with public key cryptography as in the SET standard can function as a digital signature. In this case, the message digest generated by the sender is encrypted with the sender's private key. The recipient uses the sender's public key (authenticated by the certification process described above) to decrypt the digest; then if the decrypted digest matches the digest separately computed by the recipient, the recipient knows

---

<sup>50</sup> See definition of DES in Part X *infra*.

<sup>51</sup> VeriSign is an early entrant into the certificate authority industry. The firm requires varying levels of identification for certificates supplying varying levels of assurances. Its Class 3 certificate, which authenticates identity, requires personal appearance before a notary and presentation of identification documents. See VeriSign, Inc., *Certificate Classes* (visited Apr. 8, 1999) <[http://www.verisign.com/repository/CPS1.2/CPSCH2.HTM#\\_toc361806948](http://www.verisign.com/repository/CPS1.2/CPSCH2.HTM#_toc361806948)>.

<sup>52</sup> See SET Secure Electronic Transactions LLC, *SETCo Certificate Authority* (visited Mar. 10, 1999) <<http://www.setco.org/certificate.html>> (describing the SET Certificate Authority hierarchy).

both that the message has not been altered, and that only the sender could have sent the message (because only the sender would have the private key that matches the public key for that sender).

c) *CyberCash*

¶64 Encryption can be used to present payment cards through the use of customer wallet software, such as that used by CyberCash.<sup>53</sup> Such wallet software can be used to implement SET-compliant programs, and indeed CyberCash, Inc. has announced that it will revise its initial program to implement SET. CyberCash's initial program, implemented before SET was developed, processed payment-card transactions over the Internet in a manner similar to that utilized by SET.

¶65 In the CyberCash system, CyberCash, Inc. maintains a gateway server between the front-end transaction and the back-end clearing functions. In order to use the system, merchants must run CyberCash software on their servers and consumers must download the CyberCash "wallet," the application software used by the consumer to make purchases with payment cards.

¶66 After installing the wallet software, a consumer must place in the wallet (i.e., register) the cards that he or she wants to use. The program validates the cards by communicating with the card issuer through the CyberCash gateway server. The program then encrypts the information and stores it on the customer's PC. To use the wallet, the customer must also create a unique CyberCash ID and pass phrase, which is registered with the CyberCash payment server and maps to the customer's encryption keys (i.e., a public/private key pair). The ID and pass phrase are used to unlock the wallet.

¶67 The customer's payment card data can only be used in a purchase where the payment request has been signed by the customer's private key. Digital signatures are used by all three parties (the cardholder, the merchant, and the CyberCash gateway server) to provide for authentication and nonrepudiation.

- When a customer decides to buy something at a CyberCash merchant's Web site, the customer clicks on the "pay" button at that site.
- The merchant's software sends a message to the customer's browser which causes the buyer's computer to launch the wallet software, and this software receives the transaction information.
- The customer chooses the credit card that he or she wishes to use (from among those previously registered) and clicks on the wallet's "pay" button.
- The wallet software then sends the card details securely to the merchant. The merchant authorizes and clears the payment with the financial network through the CyberCash gateway server and then returns a receipt to the buyer.

¶68 SSL, CyberCash, and SET all deal with the problem of encrypting and transmitting payment card information over the Internet. How do they differ? SET is a standard for Internet payment card payments; it is not an application program but a template for application programs yet to be created. SSL and CyberCash are proprietary application programs (though SSL is the basis of a draft Internet standard, TLS).

---

<sup>53</sup> See, e.g., CyberCash, Inc., *Instabuy* (visited March 8, 1999) <<http://www.instabuy.com>> (describing the CyberCash Instabuy software).

¶69 CyberCash integrates more functions than SSL, since CyberCash operates its own gateway server and provides special wallet software (which furnishes a graphical user interface for the customer). SSL is likewise an application program that creates a secure channel to transmit payment card details securely to the merchant's server, but it does not itself supply the gateway to the back-end processing. SSL also does not itself supply the user with a graphical user interface to facilitate calling up credit card details and sending them when needed. Other systems will supply the user interface. Browser software will include wallets, such as the one included in Microsoft's latest version of Internet Explorer.

¶70 The SET standard is a template for an end-to-end system, not just the front end like SSL. SET specifies particular forms of encryption, whereas SSL allows communicating computers to select from a range of options. SET is a very detailed set of instructions for payment messages, but it is narrowly focused. It does not deal with the user interface or with anything about the shopping process prior to transmission of payment. Again, other systems (such as the integrated systems being developed by IBM and Microsoft) will supply the user interface and will automate other aspects of the process of selling and buying.

#### D. *Digital Cash on Stored Value Cards (Smart Cards).*

¶71 Further out along the digital payment systems continuum (but one step removed from the Internet) falls the smart card. A number of companies have smart card programs, with varying degrees of patent protection.

##### 1. *Citibank*

¶72 Citibank has an active program for developing a smart card with digital currency,<sup>54</sup> and holds a number of patents.<sup>55</sup> The Citibank system generates digital cash (messages composed of bits) with a special sealed "money generator module" in a bank computer. The bank signs each note with its private key and gives each note a serial number and an expiration date. A consumer receives notes whenever he or she transfers money from an account to his or her smart card.

¶73 Money can move from one smart card to another without contacting the issuing bank. A small hardware device allows the microprocessors in the two cards to communicate. The receiving card examines the digital signatures on the note and checks to see whether the signatures are valid. The spending card adds a new layer of bits at the end of the note and then signs the entire package.

¶74 Although notes can travel through several cards prior to their expiration, all notes must be returned to the bank for reissue. This allows the issuing bank to control fraud and double spending. All the notes on a card refresh anytime the card interacts with the bank.

¶75 This system is not, however, immune to fraud. Because any note can return to the bank from any card, the bank cannot immediately shut down cards that spend the same notes more than once. The trail of signatures on each note will show which cards spent which notes—and which cards spent which notes more than once. By blacklisting the digital signatures of rogue cards, the system will eventually shut them down.

---

<sup>54</sup> See Citicorp, *United States Homepage* (visited April 8, 1999) <<http://www.citibank.com/us/home3b.htm>> (providing a link for a future Citibank digital cash website).

<sup>55</sup> See *infra* Part IX.D.1.

¶76 For convenience, the system can split digital notes into parts, making change. Since each smart card can split each note into parts, each note can spawn a progeny of notes of fractional values. Citibank's program will collect the little notes when they return to the bank and reconcile them to the value of the original note, ensuring that no change gets lost (or is spent twice).

¶77 The system can issue notes in foreign currencies and even make loans. In the loan transaction, the bank issues a note worth a certain amount of credit (similar to issuing a credit card with a credit limit of that amount). The system does not allow such a loan note to migrate from card to card. Instead, the recipient must redeem it at the issuing bank (similar to depositing an amount received from a credit card).

## 2. *Mondex*

¶78 Mondex<sup>56</sup> was developed at NatWest, a major U.K. financial institution.<sup>57</sup> Mondex is a stored-value system, the general properties of which are analogous to those of the Citibank system. A successful public trial was completed at Swindon, a town of about 190,000 people near London, in 1995. Mondex International was then formed by seventeen global banks and financial institutions, with Wells Fargo and AT&T as the only American members. MasterCard acquired fifty-one percent of Mondex International early in 1997. Two U.S. patents relate to the Mondex system.<sup>58</sup>

¶79 Each Mondex smart card has its own memory and control program, allowing any two cards to exchange value. Individuals can move cash from one card to another without having to communicate with the central computer at the bank. The chips in the cards communicate with each other by means of a special terminal or device. This device could be many things, including a piece of personal hardware the size of a pocket calculator, a point-of-sale terminal at a retailer, an automatic teller machine, or a special telephone. Vending machines and toll booths can also be fitted with hardware to allow them to accept the card. A card reader device can even be attached to a personal computer to allow Mondex cards to be used for payments over the Internet.<sup>59</sup>

¶80 On its computer, the bank maintains a "bulk purse" that is monitored by a value control and management software system (a "value meter"). The value meter maintains a float-value record which keeps track of the total value drawn down to the bulk purse and the total of values redeemed from the bulk purse. These records are kept in the aggregate and not on an individualized basis. The value meter may have an interface that adjusts the float-value record on command, creating or destroying value within the bulk purse. Presumably, the amount of value in a bank's bulk purse, and whether value is being created or destroyed, would be controlled by a central bank and would be apportioned with the amounts of value allocated to other banks' bulk purses.

---

<sup>56</sup> Mondex has not released many details about its system to the public. We have based our discussion on what has been made available and on the Mondex patents, assuming that the Mondex system as implemented will at least roughly parallel the preferred embodiment described in the patents.

<sup>57</sup> See Mondex International Ltd., *Mondex International: 1990* (visited Mar. 6, 1999) <<http://www.mondex.com/mondex/cgi-bin/printpage.pl?fname=history1.txt&doctype=hist>>.

<sup>58</sup> See *infra* Part IX.D.3.

<sup>59</sup> See generally Mondex International Ltd., *Mondex on the Web* (visited Mar. 6, 1999) <<http://www.mondex.com/mondex/cgi-bin/printpage.pl?style=noframescash&fname=../documents/net2.txt&doctype=genp>> (introducing the Mondex system's Internet uses).

- ¶81 The bulk purses in the banks' computers differ from "purses" in the microprocessors of chip cards and terminals primarily in that the bulk purses can have value loaded and redeemed via the value meter software system as well as by purse-to-purse transactions. In all other respects, the purses are technically similar, although the purses in consumers' cards may have less memory capacity than the purses held by retailers. Consumer cards are limited in the amount of cash each card can hold and also the number of transactions in its lifetime.
- ¶82 In one technological incarnation, the card maintains a record of the last ten transactions. Merchant cards have more capacity and may contain more sophisticated fraud detection schemes, such as the ability to lock out cards recorded on a list of bad cards. The merchant's card keeps a record of the last 300 transactions. Cards with very high value limits can be configured so that they can exchange value directly only with a bank, in order to produce a good audit trail.
- ¶83 Consumers can use terminals connected to the bank's computer to load value onto their cards. The value will be stored in the purse-value record in the card's memory. The value control and management system instructs the bank's accounting systems to debit the cardholder's bank account for the amount transferred to the card. When the consumer uses the card, the purse-value record of the receiving card will be increased by the amount of the transaction, and his or her own purse-value record will be decreased by the same amount.
- ¶84 Public-key cryptography is used to identify each purse and ensure secure transactions between cards. In addition to the value record and a transaction log, the purse's memory holds the following RSA keys: the purse's own public key signed by the global secret key of the master computer (the certified public-key data message); the purse's own private key; and the global public key. When the sending purse communicates with a receiving purse, the sending purse transmits a message using a transaction identifier number which is derived from a combination of the receiving purse identity and a transaction sequence number, along with its authenticated public key. The receiving purse verifies the public-key data message and then uses the sending purse's public key to recover the transaction identifier number.
- ¶85 The sending card constructs a transaction value message from the value it wishes to transfer and from the request message. The message is signed with the sender's secret key. The receiving purse obtains the public key of the sending purse by use of the global public key, then uses the sending purse's public key to recover the transaction value message. The receiving purse checks to ensure that the transaction value message carries the identity of the receiving purse and the appropriate transaction number, then adds the value to its own purse value record and sends an acknowledgment to the sending purse.<sup>60</sup>
- ¶86 Each merchant has its own "purse," along with a terminal containing an interface device, to accomplish the transfer from the customer's card to the merchant's card. Later, the merchant will transfer the value to the bank's stored-value computer and have the amount credited to its account. The merchant's device

---

<sup>60</sup> The Mondex patents contemplate slightly different protocols for transactions between a consumer purse (low computing power) and retailer purse (high computing power). One such protocol has the consumer purse use a symmetrical key cryptographic system (DES) for transmitting transaction value record messages. The lower-power sending purse uses the public key of the receiving purse to encrypt its communications with the receiving purse, and the receiving purse uses DES for messages that the sending purse must decrypt (i.e., the transaction value identifier described above). Another solution is for the consumer purse to transmit its private key to the retailer purse. Then the consumer purse can encrypt using its public key and the retailer purse can decrypt using the consumer purse's private key.

does not have to communicate with the bank's computer at the time of transfer from the customer to the merchant. This feature allows small transactions to be relatively private and free from the burden of communicating with a central verification authority.

¶187 Each Mondex card may contain two different security protocols, one that is active and one that is dormant.<sup>61</sup> This feature might improve system security. The bank might use this feature to rotate security protocols, deleting the active system, activating the dormant system, and transmitting a new dormant system. In principle, this system could isolate and shut down rogue cards.

### 3. *Other Stored-Value Cards*

¶188 Visa and MasterCard each have a stored-value card. Visa piloted VisaCash at the 1996 Olympic Games in Atlanta, and other pilots are currently ongoing around the world.<sup>62</sup> MasterCard launched MasterCash in March 1996 in Australia. MasterCard and the Australian banks are evaluating results and adding new features, such as multi-currency capability.<sup>63</sup> As of late 1997, Visa and MasterCard, together with Chase Manhattan and Citibank, were testing interoperability in a pilot in Manhattan.

¶189 Clip, a reloadable card that can handle multiple currencies, has been launched in Europe by Europay International, MasterCard's European marketing partner.<sup>64</sup> Proton, a project of Banksys (a payment service company owned by Belgian banks), has been used in the Netherlands, Brazil, Australia, Sweden, and Switzerland. By late 1997 smart cards had achieved much more market penetration outside the United States than within it. Despite industry predictions that this situation would change by 1998, the majority of smart card use still occurs abroad.<sup>65</sup>

#### E. *Digital Cash on the Internet (Anonymity, Metering, and Micro Payments)*

¶190 The Internet is both a blessing and a curse. On the plus side, the Internet has reduced the costs of communication and promises to reduce these costs still further. This drop in what some would call transaction costs has created new opportunities for commerce in very small transactions, but it comes at a price—a loss of privacy. The Internet's threat to privacy goes beyond making sensitive public and quasi-public records (e.g., court filings, arrest records, credit histories, etc.) widely available. It also enables interested parties to follow people through cyberspace, tracking where they go and what they do once they get there. Some Internet-based payment systems have emerged to capitalize on the opportunities presented by reduced transaction costs and others have developed to protect anonymity.

---

<sup>61</sup> See Mondex International Ltd., *Prevention* (visited Mar. 6, 1999) <<http://www.mondex.com/mondex/cgi-bin/printpage.pl?style=noframescash&fname=../documents/prevention.txt&doctype=genp>>.

<sup>62</sup> See Visa Intl., *Visa Cash: United States* (visited Mar. 6, 1999) <<http://www.visa.com/cgi-bin/vee/nt/cash/usa.html?2+0>>.

<sup>63</sup> See MasterCard Intl., *Breakthrough Demonstration of Mondex Chip Card's Multi-Currency Capability Provides Glimpse of the Future* (visited April 8, 1999) <<http://www.mastercard.com/about/press/980225a.html>>.

<sup>64</sup> See EUROPAY Intl., *SmartCards: Electronic Purse* (visited Mar. 6, 1999) <[http://www.europay.com:80/smartcard/Smartcard\\_electronic\\_purse\\_index.html](http://www.europay.com:80/smartcard/Smartcard_electronic_purse_index.html)>.

<sup>65</sup> See e.g. Banksys Intl., *Banksys and the press - 25/05/98* (visited Mar. 7, 1999) <<http://www.banksys.be/eng/presse23.html>> (describing worldwide use of Proton-based smart cards).

1. *Ecash*

¶91 David Chaum, the founder of now-defunct DigiCash, Inc., invented and patented Ecash.<sup>66</sup> Ecash enables a bank to issue electronic cash and protect against fraud while allowing the holder to anonymously spend his or her Ecash. In this respect, Ecash differs from many other digital payment systems, which create audit trails and eliminate anonymity.

¶92 To use the Ecash system, both the customer and the merchant must have accounts at an Ecash bank. The customer withdraws digital coins against his or her account with the bank and stores them in an Ecash wallet—a software program that runs on his or her PC. The wallet software manages the customer’s coins and keeps a record of all transactions. Because the wallet software makes the steps in the protocol transparent to the customer, the customer does not “see” or have to deal with the protocol.

¶93 The coins themselves are actually “minted” by the customer. The wallet software generates coins (bit-strings), each with a unique serial number (chosen randomly and large enough so that the chance someone else would generate the same number is very small). The coins are then validated by the bank’s signature, using a blind signature protocol so that the bank cannot connect the serial number on any particular coin it signs with the particular customer to whom it is being issue

¶94 Each coin essentially consists of a serial number encrypted with the appropriate secret key of the bank. The coin also contains a public key to allow decryption of the bank’s signature for verification. The bank signs with a different signature key for each denomination of coin, preventing customers from telling the bank it is signing a small digital coin when the coin is really a large one. After the bank signs the coin, it is returned to the customer, and the customer unblinds it so that the bank’s digital signature on the unblinded coin looks the same as any other digital signature.

¶95 There are a number of different species of blind signature protocols based upon Chaum’s basic idea. In the simplest version, the customer essentially multiplies the note serial number he or she generates by a random factor before sending it to the bank for signing. After the bank signs the note, the customer divides out the random factor. Because the note has the customer’s digital signature, the bank knows that it issued a note to that customer, but it will not know the serial number of the note and will not know where and when the note is spent. This simple version of the blind signature idea requires the bank to keep a spent-coin database and a list of all note numbers that have been spent, in order to prevent double spending. In this system, however, if a bank were to detect double spending, it would not be able to identify the double spender. The need for a spent-coin database limits the scalability of the system, and the inability to pinpoint double spenders efficiently is troublesome, especially because it is far easier to counterfeit a digital coin than paper money.

¶96 Chaum and others have modified the blind signature idea in attempting to solve these problems while preserving anonymity. One solution requires the spender of

---

<sup>66</sup> In addition to Ecash, DigiCash, Inc. marketed “firmware” for smart cards. Firmware involves programming systems built into smart cards for digital cash and other smart card applications like toll road collection. DigiCash also developed an electronic payment system, based in part on Chaum’s digital cash protocol implemented in smart cards and hardware wallet devices, which formed part of the European Community’s 1992-1995 project CAFE (Conditional Access for Europe). (“Conditional Access” refers to the use of smart cards to restrict access to secure locations, computers, etc.).

the digital coin to answer a random numeric query about each digital coin when spending it. The cryptographic properties of this system are such that spending such a note once does not make it traceable, but spending it twice reveals enough information to identify the spender.

¶197 An Ecash transaction works as follows:

- When a customer purchases something from a merchant who accepts Ecash, the merchant's software sends a payment request to the customer's wallet software. The request contains the order amount, the currency to be used, the time, the merchant's bank and account ID, and a description of the order.
- If the customer accepts the transaction, the wallet puts together coins from the wallet representing the exact amount.
- The wallet sends the coins to the merchant in a payment message. The message contains a hash of the order description, which can later be used to check on the order if a dispute arises.
- The merchant's software forwards a payment message instructing the bank to deposit the coins in the merchant's account.

## 2. *Micropayments*

¶198 Theoretically, the Internet should allow businesses to sell information to consumers on a pay-as-you-go basis. Consumers could, for example, pay a fraction of a cent for a stock quote or a database query. Existing payment systems were not designed with micropayments in mind. The problem with any micropayment system is the tradeoff between security and transaction costs. In order for a payment system to permit a transaction of a one-thousandth of a cent, the payment system itself must cost far less on a per transaction basis. In addition, in order for microcommerce to work at all, the transactions must happen very rapidly. (No one will pay any amount for a stock quote if it takes more than a minute for the money and the information to change hands). These constraints make securing a payment system against fraud and theft difficult.

### a) *Millicent*

¶199 Millicent is a microcommerce payment protocol under development at Digital Equipment Corporation. Digital officially announced the system in March 1997, and made it available for public testing during the summer of 1997.<sup>67</sup>

¶100 Before using the Millicent system, consumers must install the Millicent wallet, set up an account with a Millicent scrip broker, and buy Millicent scrip from that broker. Millicent scrip is an electronic coupon which allows a consumer to spend a given amount of money with a specific vendor.<sup>68</sup> Brokers will be banks, payment card associations, or other trusted financial intermediaries such as the post office, a telephone company, or an Internet service provider. Brokers will act as aggregators between customers and Internet vendors by issuing Millicent scrip wholesale and selling it retail. In order to accept Millicent scrip, merchants must install Millicent

---

<sup>67</sup> Digital Equipment Corporation subsequently merged with Compaq Corporation on June 11, 1998.

<sup>68</sup> See generally Compaq Computer Corp., *Millicent Glossary* (visited Mar. 7, 1999) <<http://www.millicent.digital.com/glossary/index.html>> (defining "broker," "scrip," and "vendor").

vendor software, which not only accepts scrip from consumers but also performs several important system security functions.

¶101 With the preliminaries out of the way, a Millicent transaction takes place in a few simple steps:<sup>69</sup>

- The customer clicks to make a purchase.
- The customer makes a purchase with scrip, the cost of the purchase is deducted from the scrip's value, and new scrip with the new account balance is returned as change.
- Using a secure hash function, the vendor's software validates the scrip to prevent customer fraud. The vendor's software makes use of customer identifying information generated by the broker when the vendor scrip is created, checking this against information sent by the customer during the transaction.
- The vendor also checks for double spending by checking to see whether the unique identifier in the scrip body has already been spent. (Millicent scrip expires quickly, so that vendors will not have to maintain long lists of spent scrip.).

¶102 The Millicent wallet software allows consumers to automate many of these functions. Consumers can, for example, choose to accept all transactions generated by a particular merchant and/or below a certain price. Consumers can also instruct their Millicent wallets to replenish broker scrip automatically.

¶103 As with all payment systems, security is an issue. The system will try to prevent consumer fraud with hash functions, expiration dates and unique IDs. It will attempt to ward off broker fraud by having consumers and vendors independently maintain account balances. Brokers will control vendor fraud by dropping vendors that take scrip without delivering the goods.

b) *NetBill*

¶104 NetBill, now on pilot at Carnegie-Mellon University, is another micropayment system. Like Millicent, NetBill requires both merchants and consumers to enroll in the system. Merchants must set up a Netbill "till" on their servers, and consumers must install a Netbill checkbook. Before initiating a Netbill transaction, a consumer must deposit money in his or her NetBill account.

¶105 A NetBill transaction for the purchase of information goods works as follows:<sup>70</sup>

- A consumer requests a price quotation from a merchant.
- The merchant returns a quotation.
- If the consumer accepts the price, he or she instructs the Netbill checkbook to send a purchase request to the merchant's till software.
- The till software retrieves the information from the merchant's server. It encrypts them with a one-time key and computes a checksum on the result. It then sends the result to the buyer's checkbook. The checkbook verifies the checksum. If it checks, then the buyer has received the goods.

---

<sup>69</sup> See Steve Glassman et al., *The Millicent Protocol for Inexpensive Electronic Commerce* (visited Mar. 7, 1999) <<http://www.millicent.digital.com/works/details/papers/millicent%2Dw3c4/millicent.html#SECTION300>>.

<sup>70</sup> See Carnegie Mellon University, *How NetBill Works* (visited Mar. 7, 1999) <<http://www.netbill.com/netbill/works.html>>.

- Although the consumer has the goods at this point, he or she does not have the key and cannot decrypt them.
- The checkbook returns a signed electronic payment order to the merchant's till. At this point, the till endorses it and forwards it to the NetBill server.
- The NetBill server verifies that the price, checksums, and other details are in order. If they are, it debits the consumer's account and credits the merchant's account.
- The NetBill server then sends a digitally signed message to the seller notifying it that the transfer is complete.
- The merchant's software sends a digitally signed message to the buyer containing the secret key for decrypting the data.

¶106 NetBill uses cryptographic protocols at every step of the transaction. A modified Kerberos system encrypts messages between the till and the checkbook. A secure hash algorithm (SHA) insures integrity of the goods, and RSA public key cryptography signs the message approving the transaction. All other NetBill messages use a symmetric key algorithm (DES).

¶107 All transactions must pass through the NetBill server only once if all is well, but more often if a glitch occurs. Because of the large volume of traffic that will pass through the central server if the system becomes successful, scalability is an issue. Nevertheless, CyberCash has paid over \$2 million to license the system.

c) *CyberCoin*

¶108 CyberCash has one additional product in its stable, CyberCoin. The CyberCoin system is not really a micropayment system. Instead, it fills the gap between secure payment card transactions and micropayments (roughly anything between \$.25 and \$10).

¶109 The CyberCoin system works as follows:<sup>71</sup>

- CyberCash sells CyberCoins to consumers. Consumers store the CyberCoins in their PC-based CyberCash wallets.
- When a consumer decides to spend a CyberCoin, he or she sends a payment message which includes the CyberCoin to a merchant.
- Upon receipt of the payment message with the CyberCoin, the merchant verifies its validity with the CyberCash server.

¶110 In the CyberCoin system, the pieces of data are not actually money. When a consumer buys a CyberCoin from CyberCash, CyberCash stores this money in an account. The money sits in that account (accruing interest for CyberCash) until a merchant attempts to redeem a CyberCoin. At that point, CyberCash transfers the money represented by the CyberCoin to the merchant's bank account.

F. *A Word on Integrated Systems.*

¶111 A number of big players—notably IBM, Pandesic (Intel/SAP), and Microsoft—are integrating some or all of these payment systems into much larger Internet packages. These packages, or integrated systems, do much more than simply

---

<sup>71</sup> See CyberCash, Inc., *CyberCoin: Micropayments Service Overview* (visited Mar. 7, 1999) <<http://www.cybercash.com/cybercash/services/cybercoin4.html>>.

exchange value. They take a firm's existing operations and integrate them with the Internet. Although the actual elements of an integrated system will vary with the type of firm, these systems will handle such tasks as marketing, inventory pricing, materials management, shipping and handling logistics, and vendor payment.<sup>72</sup>

¶112 Some of these integrated systems will also have the capacity to structure rights management. Rights management means limiting what rights a consumer buys to a particular piece of information. For example, a consumer might purchase the right to read a document but not print it; the right to maintain a copy of a document for seven days; or the right to use it three times over a forty-eight-hour period. Systems that perform these functions are coming to be known as trusted systems (presumably because they are relied upon to control information flows that, once dispensed to a consumer, cannot be monitored).

¶113 Although trusted systems are beyond the scope of the present paper, one firm's efforts in this area deserve attention: Citibank. At this point, only Citibank seems to have developed (and patented) both a smart card system and a trusted system.<sup>73</sup> The basis of the Citibank trusted system is a protocol that enables the exchange of "electronic merchandise" for digital cash. Electronic modules called trusted agents are allied with the money modules of a merchant and a customer, such that the merchandise can be delivered to the customer's trusted agent provisionally—in escrow—until the payment is duly received, at which point the merchandise is released to the customer by the trusted agent.<sup>74</sup> The modules—agents—consist of computer programs. The escrowed provisional delivery is accomplished by means of encryption.

#### VII. WHO OWNS THE NEW ELECTRONIC PAYMENT SYSTEMS?

¶114 Who owns the new electronic payment systems? At first, the question seems a bit bizarre. Historically, private property rights have not attached to the infrastructure of exchange. Nobody owns the system of making payments by writing, presenting, and clearing paper checks. Nobody owns the apparatus of paper currency as a medium of exchange. Nobody owns the general concept of paying and selling by means of a payment card system.

¶115 The question of ownership is not at all bizarre in the new world of electronic payments. Indeed, it is central. As our discussion so far has made clear, money and commercial exchange are in the process of merging with the information technology of the digital networked environment. In the digital networked environment, property rights attach not only to the physical infrastructure of exchange—the computers, cables, and optical fibers that actually transport information—but also to the systems and methods of information exchange itself.

---

<sup>72</sup> IBM and Microsoft may have an advantage in this market because they created the legacy systems with which the comprehensive marketing tools must integrate, and they can offer customized services. Nevertheless, the presence of Open Market, Inc. in this field should be noted. This firm, founded in 1993, is concentrating on software of various kinds that can integrate information delivery and payment and offers customized systems for various different types of businesses. Open Market recently acquired Folio, a developer of content-management software. A number of firms that are advertising integrated commerce services are licensees of Open Market's systems—including AT&T and InternetMCI.

<sup>73</sup> See *infra* Part IX.D.1.

<sup>74</sup> See Visa Intl., *Visa - Electronic Commerce - SET* (visited Mar. 7, 1999) <<http://www.visa.com/cgi-bin/vee/nt/ecom/et/main.html?2+0>> (describing Secure Electronic Transactions including authentication through the use of digital certificates).

A. *The Central Role of Patent Rights*

¶116 In the digital networked environment, patents are the most formidable form of intellectual property. The holder of a patent can prevent anyone else from becoming a competitor in the same product or system for the patent term. And the patent term of twenty years from the date of application is an eternity given the market cycles typical in information industries.

¶117 Trade secrets and copyrights, while significant, are weaker than patents in this context. Aside from the fact that trade secrets are undermined by employee mobility, and occasionally by industrial espionage, trade secrets do not protect against reverse engineering. Trade secret law leaves competitors free to make and sell any system that they can figure out. Although copyright protection lasts much longer than a patent (ninety-five years after publication or 120 years after creation for works made for hire),<sup>75</sup> it only protects against copying. Competitors may make and sell any program whose functioning they can duplicate by writing new code from scratch in a clean room.

¶118 Neither of these limitations applies to the patent monopoly. A patent holder can, in general, exclude all competitors for the patent term or license others on terms it chooses. Unlike the other forms of intellectual property rights, which basically prevent competitors from stealing or copying from each other but otherwise allow competition, a patent prevents competition unless the holder chooses to permit it.

¶119 Moreover, a broad patent can completely preempt a field. Copyright law prohibits firms from copying a specific program exactly or copying its particular structural and organizational features, as long as these features are deemed to be expression of an idea, but not the underlying idea itself. Ideas are free to be copied under the copyright regime. In contrast, a patent claimed in terms of the basic functionality of a system—for example, a smart-card digital-cash system or a bill payment system—can preclude anyone from marketing another system with different particulars but the same basic functional components. A system or software patent can cover a wide range of implementing programs.

¶120 In the past, there was little need for financial institutions to concern themselves with patent disputes. However, the recent decision from the Federal Circuit in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*,<sup>76</sup> disposing of the “mathematical algorithm” and “business methods” exceptions to patentable subject matter, made clear what had long been suspected: The means and methods of electronic commerce are indeed patentable. *State Street Bank*, coupled with the advent of electronic commerce, has turned the stream of patents and patent applications for systems related to electronic commerce into a torrent.<sup>77</sup> The more financial firms restructure their core business methods to capitalize on electronic commerce, the more their managers and legal counsel will need to devote attention to both securing and policing their own patents and to analyzing the patents of competitors.

---

<sup>75</sup> Copyright terms were extended by the newly enacted Sonny Bono Copyright Term Extension Act of 1998, Pub. L. No. 105-298, 112 Stat. 2827 (codified as amended in scattered sections of 17 U.S.C.).

<sup>76</sup> 149 F.3d 1368 (Fed. Cir. 1998).

<sup>77</sup> See, e.g., Scott Thurm, *Online: A Flood of Web Patents Stirs Dispute over Tactics*, WALL ST. J., Oct. 9, 1998, at B1 (describing, inter alia, patents for “on-line frequent buyer programs” and “internet shopping carts”).

¶121 More likely than not, financial institutions will find themselves involved in patent litigation. Patent rights in any field can provoke litigation. But the U.S. Patent Office has turned the possibility into a virtual certainty in this field by issuing, and continuing to issue, a large number of very broad electronic commerce patents. A summary of many such patents is set forth below.<sup>78</sup> At some point, the competing claims of these patents will conflict.

#### B. *What Is Patented Already?*

¶122 As the Patent Appendix makes clear,<sup>79</sup> many electronic commerce and digital payment patents have already been issued. Such patents relate to the payment mechanisms designed for electronic commerce in various ways, from the claim of an entire system (for example, CheckFree's patent<sup>80</sup> for "a system for use by a service provider to pay bills rendered to a consumer by billing entities") to smaller components of a payment system (for example, V-ONE Corporation's patent<sup>81</sup> for "wallet" software to assist consumers in purchasing items over the Internet). At the other end of the spectrum, Citibank has been vigorously building its patent portfolio over a large range of digital payment systems, with some claims of great purported breadth.

¶123 The field of patent analysis for payment systems is in the process of unfolding. In light of this, industry participants (and their legal advisors) should assume that at least some of the payment mechanisms emerging in the marketplace are the subject of patent applications for which patents have not yet issued. Digital Equipment Corporation has patented its Millicent system. Others have kept mum. As of late 1998, we do not know, for example, whether patents are pending for the NetBill system (which public records reveal that CyberCash, Inc. has licensed),<sup>82</sup> or for the software "wallets" in use by CyberCash, Microsoft, and others.

¶124 As each new patent issues, the picture as a whole refocuses. Take, for example, the Secure Socket Layer (SSL) system. U.S. Pat. No. 5,657,390, entitled "Secure Socket Layer Application Program Apparatus and Method," invented by Elgamal and Hickman, and assigned to Netscape, was issued on August 12, 1997. Although SSL had been around for years, no one outside of Netscape knew that a patent on it was pending. Indeed, some have complained about Netscape's efforts to get SSL included in the new TLS standard without revealing its pending patent.

¶125 The SSL patent contains three claims: Claims 1 and 2 are drafted in means-plus-function language (for example, the "means for providing a socket application program interface to an application layer program" is one element of Claim 2). Under Section 112, Paragraph 6 of the Patent Act, these claims would be limited to what is disclosed in the patent specification and "equivalents thereof."<sup>83</sup> The specification appears to be a fairly specific description of Netscape's SSL program.

¶126 Claim 3, however, is not a means-plus-function claim and its breadth is striking. Claim 3 is for "a method of encrypting and decrypting information transferred over

---

<sup>78</sup> See *infra* Part IX.

<sup>79</sup> See *infra* Part IX.

<sup>80</sup> See *infra* Part IX.B.1.

<sup>81</sup> See *infra* Part IX.C.1.

<sup>82</sup> Press Release, *Cybercash Acquires Rights to Micropayment Technology from Carnegie Mellon University* (last modified Oct. 28, 1997) <[http://www.netbill.com/netbill/press\\_release.html](http://www.netbill.com/netbill/press_release.html)>.

<sup>83</sup> 35 U.S.C. § 112 ¶ 6 (1994).

a network between a client application program running in a client computer and a server application program running in a server computer.” The claimed method comprises “providing a socket application program interface to an application layer program,” “providing encrypted information to transport protocol layer services,” “encrypting information received from an application layer program,” and “decrypting information received from transport protocol layer services.” Claim 3 purports to cover the use of any kind of encryption to secure the transport layer, and not just the forms of encryption actually used in Netscape’s SSL-enabled browsers and servers.

¶127 Any attempt to enforce the claim will likely be met with substantial challenges given the prevalence of encryption and transport layer technology in the prior art. The narrower, means-plus-function Claims 1 and 2 may not fare any better unless Netscape can show that it made more than obvious improvements to the prior art.

¶128 Netscape’s representation that it intends to make this patent available for all to license<sup>84</sup> may make this point moot. But the fact that the patent exists at all (and that others may follow) illustrates that patent rights are reshaping the world of electronic payments. The existence of a large number of patents involving electronic payment systems and their component parts demands careful consideration in the new competitive environment. Unlike the old forms of payment mechanisms, the new electronic payment mechanisms are subject to ownership. That simple fact will undoubtedly rearrange the legal and business priorities of financial institutions.

## VIII. CONCLUSION

¶129 In the context of today’s evolving marketplace, we have described a continuum of electronic payment mechanisms. What has become apparent is that financial institutions and their legal advisors will need to pay particular attention to property rights in the information technology underlying these mechanisms. Although patent rights get little attention at the increasing number of symposia, CLE presentations, and publications devoted to electronic commerce and emerging payment mechanisms, the field is crowded with patents, and it is safe to assume that still more are pending. Conflicts are bound to arise as the market unfolds, though it would be premature at this point to try to predict where or when they will erupt.

¶130 As banks and financial institutions enter the world of electronic payments in earnest, more and more of them will become participants—often as licensees—in some of the systems described in this paper, as well as in others yet to emerge. We recommend caution: financial institutions and their legal advisors should analyze the intellectual property status of any information technology they propose to implement.

## IX. APPENDIX A: SELECTED ELECTRONIC COMMERCE PATENTS

### A. *Purpose and Scope of the Patent Discussion*

¶131 We have selected a small number of issued U.S. patents that purportedly bear on some of the payment mechanisms discussed in the text, and which may be

---

<sup>84</sup> See Alex Lash, *Netscape patents crypto protocol* (Sep. 16, 1997) <<http://www.news.com/News/Item/0,4,14302,00.html>> (“[T]he company says it will continue to give it away for free.”).



processing unit, and “means for effecting payment of the bills on behalf of the consumer’s accounts.” With respect to how payment will be effected, the specification states that “[t]he service provider may pay merchants by a draft or check (paper) or by electronic funds transfer”. Methods and mechanisms are described that will accomplish these actions (a Troy printer to put a micro code on paper drafts, an IBM laser printer attached to a micro post processor, electronic funds transfer through the Federal Reserve ACH Network). Consolidated checks are mentioned, which are “checks made payable to a single merchant to cover payments for a number of consumers who all owe the same merchant.” Also mentioned is the possibility of charging the consumer’s credit card “through the RPS Network.” Claim 2 narrows Claim 1 to the system “wherein the preferred form of payment is selected from a member of the group consisting of electronic funds transfer, charge to a credit card, a check, and a draft.”

## 2. *Online Resources & Communications Corporation*

¶137 Online Resources & Communications Corp. is the assignee of U.S. Pat. No. 5,220,501, issued June 15, 1993, and entitled, “Method and System for Remote Delivery of Retail Banking Services” (fifty-one claims).<sup>89</sup> Matthew P. Lawlor, co-inventor with Timothy E. Carmody, is the company’s CEO.

¶138 The system described in the patent specification involves distributing terminals (envisioned as ATM-like) to users, and transmitting messages over an ATM network. The terminals communicate with a central computer operated by a service provider to transmit information related to financial services. The central computer transmits a message in real time over a conventional ATM network to debit the user’s bank account, then pays the payees electronically or “in other ways as appropriate” (i.e., “check and list,” in the same manner as the CheckFree system).

¶139 The patent’s claims all involve using a central computer and home terminals. The company asserts that under the patent it “has the exclusive rights to process real-time electronic transactions of consumers who use any in-home terminal (including telephones computers, and televisions) to purchase goods and services, pay bills and bank through the automated teller machine networks of the financial services industry or any debit network using an ATM-compatible personal identification number.”

¶140 The preferred embodiment as described in the specification envisions using ATM networks and a terminal that looks like an ATM and is distributed to customers by the service provider. In most of the patent’s claims, the terminals are stated to be distributed to users by the service provider, and the network used is stated to be an ATM network. It is thus likely that financial institutions which do not distribute any hardware devices to their customers or do not use an ATM network can avoid coming within the terms of these claims.

¶141 Some of the claims, however, do not contain these limitations. Claim 24 is for “a method of paying bills,” including, inter alia, the steps of “activating a microprocessor-based home banking terminal,” establishing communications with the central computer over a telephone line, using an “ATM network compatible encrypted PIN user identification number,” and “validating and processing . . . an ATM network transaction debit message” at the user’s bank “substantially in real time.” Claim 24, which is apparently the basis of the company’s statement quoted

---

<sup>89</sup> See U.S. Pat. No. 5,220,501, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+931490+0+3+263577+OF+1+1+1>>.

above, does not contain the step of “providing” the user with the terminal or the limitation to an ATM network.

¶142 Claim 38 also does not contain a limitation to systems wherein a terminal is provided by the service provider. Claim 38 purports to claim a system providing for commerce in information by having the service provider deliver information to the user, debit the user’s account through an ATM network, and use the funds to compensate the information provider.

¶143 It thus appears that any firm which implements a bill paying system that clears accounts in real time using ATM-compatible PINs may be requested to license the Online Resources patent. It is possible that such a firm could be asked to license the CheckFree patent as well. It appears that the Online Resources system—at least in Claim 24—is different from CheckFree mainly through the provision for clearing accounts in real time. It might be possible to challenge the validity of the CheckFree patent, since it is possible to argue that the feature of clearing accounts in real time is not enough to distinguish the two (i.e., to make CheckFree non-obvious in light of Online Resources).<sup>90</sup>

### 3. Visa

¶144 Visa International is the assignee of U.S. Pat. No. 5,465,206, entitled “Electronic Bill Pay System” and invented by James J. Hilt and others (thirty claims).<sup>91</sup>

¶145 The patent describes a system apparently instantiated in Visa’s ePay system.<sup>92</sup> The difference between this type of system and the CheckFree type of system is that the Visa system is designed to deliver funds electronically to the bank accounts of billers through a new use of banking networks. The system avoids translating each consumer’s electronic payment requests back into paper checks, but it only works if the consumer’s and biller’s banks participate in the system.

¶146 The claims of the patent relate to a banking network set up to use biller ID numbers to sort payment packets originated by consumers at originating nodes (consumers’ banks) and direct them to appropriate billers’ accounts at unique destination nodes (biller’s banks).

- Claims 1-15 relate to the network as an apparatus, claiming “an electronic funds transfer network for transferring funds from a consumer account to a biller account . . . .”
- Claim 30 relates to “an electronic payment network,” containing, inter alia, “conversion means . . . for converting an outbound payment data packet to an inbound payment data packet,” which involve using the biller ID to direct the payment to the appropriate destination, and “means for crediting the consumer’s account with the biller.”

There are also parallel methods claims.

- Claims 16-27 relate to “a method of paying bills electronically, wherein funds are effectively transferred between a consumer and a biller . . . .”

---

<sup>90</sup> It is possible, of course, that CheckFree might claim priority of invention even though its application was filed later. Online Resources’ U.S. Pat. No. 5,220,501 was issued on June 15, 1993, in an application filed on December 8, 1989. CheckFree’s application was filed on July 25, 1991, and its patent, U.S. Pat. No. 5,383,113, was issued on January 17, 1995.

<sup>91</sup> See U.S. Pat. No. 5,465,206, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+931744+0+3+535988+OF+1+1+1>>. With respect to this patent, a notice of request for reexamination by the owner appeared in the PTO Official Gazette on March 4, 1997.

<sup>92</sup> For a brief explanation of the ePay system, see *supra* Part VI.A.

- Claim 28 states a method claim another way, as a method comprised of steps “for paying a bill from a biller to a consumer.”

C. “Wallet” Storage for Credit Card Information on Consumers’ PCs

1. V-One Corp.

¶147 V-One Corporation is the assignee of U.S. Pat. No. 5,590,197, entitled “Electronic Payment System and Method” and issued on December 31, 1996 (twelve claims).<sup>93</sup> James F. Chen and Jieh-Shan Wang are the inventors. This patent relates to what it terms a “cyber wallet.”

¶148 In general, the term “wallet” refers to an application program for consumer PCs—or smart cards or other consumer interfaces—that stores and organizes credit card information, digital cash, or digital checks, in such a manner that the consumer can select the preferred payment mechanism without having to run any other programs to accomplish payment. One embodiment set forth in the V-One patent describes wallet software for purchasing items over the Internet with payment cards, using public-key cryptography to secure the card information, although the specification makes clear that the wallet can be used for other kinds of transactions, both debit and credit. Another embodiment set forth in the patent describes a system implemented in the integrated circuit of a smart card. The system functions when the smart card is inserted into a card reader.

¶149 Claims 1-6 relate to “an electronic payment system” claimed in means-plus-function form. Claim 1 has the following elements:

- “storage means for storing sensitive account information,” a “browser program” constituting a means for communicating with a merchant over an open network, and a “public key file” including a means for selecting the appropriate public key and using it to encrypt sensitive information to “generate an authorization ticket.”
- “means possessed by a merchant in communication with the storage means” to receive and forward the authorization ticket to an account processor.
- “means in the account processor including a private key for decrypting the authorization ticket and informing the merchant whether a transaction is authorized.”

¶150 Claim 2 adds to Claim 1 the narrowing proviso, “wherein the storage means is in the form of a software program distributed by a credit card company or the merchant to a customer for use on the customer’s own modem-equipped computer.” Claim 3 adds the narrowing proviso, “wherein the storage means is provided on a smart card for use in kiosks equipped with smart card readers.” Claim 12 adds “the step of allowing access to the account information via a PIN mechanism, so that the wallet can be used in situations where encryption of the information is not necessary.”

¶151 While these means-plus-function claims will be limited in accordance with Section 112, Paragraph 6 of the Patent Act,<sup>94</sup> Claims 7-10 are not primarily in

---

<sup>93</sup> See U.S. Pat. No. 5,590,197, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+931895+0+4+121593+OF+1+1+1>>.

<sup>94</sup> 35 U.S.C. § 112 (1998).

means-plus-function form. Claim 7 is for “[a]n electronic payment method,” comprising the following steps:

- providing a customer with personal account information, a browser program for enabling communications with a merchant over an open network, and a public-key file “including means for selecting the public key of a private-public key cryptosystem.”
- generating an authorization ticket from the customer’s encrypted account information.
- transmitting the authorization ticket to the merchant.
- upon receipt by the merchant, adding information pertaining to an order and forwarding the package to a secured account processor.
- “decrypting the authorization ticket using the private key of said public-private key cryptosystem so that the information contained therein can be used to verify whether the transaction is to be permitted.”

¶152 Claim 8 adds a narrowing proviso describing the first step in terms of “distributing a software program to a customer for use on the customer’s own modem-equipped computer.” Claim 9 limits the same step to “providing at least the personal account information and public key file on a smart card for use in kiosks equipped with smart card readers.”

#### 2. *Other “Wallets” that Run on Users’ Computers*

¶153 CyberCash, Microsoft, and IBM distribute “wallet” software to customers. These programs perform the functions delineated by the V-One system (transmitting payment card numbers over the Internet), using the same means (public-key cryptography). It is not public knowledge whether CyberCash, Microsoft, and IBM consider their “wallets” sufficiently technologically distinct from V-One to compete with it (perhaps they have even applied for patents of their own), or on the other hand have licensed the V-One patent. Certainly, on its face the V-One patent purports to cover the wallet function in general, at least as it pertains to software and payment cards.<sup>95</sup>

#### D. *Selected U.S. Patents Relating to Stored Value Card Systems*

¶154 There are a large number of patents relating to smart card systems. Many of them relate to card manufacture. Examples include “firmware” systems that can allocate the “real estate” on a card so that the card can carry various systems without their interfering with each other. Of more interest to our purpose here are patents claiming ownership of an overall transaction system—a digital cash or other electronic commerce scheme—involving cards. We will confine our attention to the patents of a few important players in the field—Citibank, Mondex, Electronic Payment Services, DigiCash, and Bellcore (now .

---

<sup>95</sup> A different approach to a wallet is a separate wireless hardware device that can be carried in the consumer’s pocket. This approach was followed by Currency Scientific, Inc., which, according to the firm, owns two patents with more pending. Currency Scientific describes its product as “the first prototype to conveniently and securely combine purchase and data storage options into a simple, easy-to-use package with a keypad, display and audio speaker.” See BUS. WIRE, Oct. 21, 1997.

1. *Citibank: Electronic Money Patents*

¶155 Citibank has pursued a multi-year development program for an electronic money system implemented in smart cards. Two patents (which stem originally from one application) are each entitled “Electronic-Monetary System”: U.S. Pat. No. 5,453,601, issued on September 26, 1995 (ninety-eight claims),<sup>96</sup> and U.S. Pat. No. 5,455,407, issued on October 3, 1995 (nine claims).<sup>97</sup> Both were invented by Sholom S. Rosen and assigned to Citibank. At least one other patent pertaining to this system is still pending.

¶156 The Citibank system is described in the text of this paper.<sup>98</sup> These patents claim the system broadly in terms of its operative functions. Claim 1 of the ‘601 patent is for “an electronic monetary system,” comprising:

- “an issuing bank having an online accounting system”
- “electronic representations of currency” (digital notes)
- a “money generator module” at the issuing bank, for issuing digital notes
- a “teller module” at the issuing bank, for storing the notes and processing banking transactions involving them
- a “transaction module” for storing digital notes, performing online transactions with the issuing bank, and exchanging notes with other transaction modules in offline transactions, using a processor that will include transfer records in such transactions

¶157 The “money generator module” and the “teller module” would most likely be a programmed central computer at the bank, and the “transaction module” would most likely be a programmed microprocessor in a smart card. In the ‘407 patent, Claim 1 is likewise for “an electronic monetary system” comprising component parts, substantially the same as in the ‘601 patent but with the addition of “a plurality of correspondent banks,” and “a plurality of second teller modules, each associated with one of said correspondent banks.”

¶158 Note that not only do these claims leave out reference to particular equipment, and hence are not limited to hardware or software of any particular type, they also do not refer to any kind of encryption, and hence are not nominally limited to the encryption system used in the system disclosed.

¶159 Claim 13 of the ‘601 patent adds as a limiting element the feature that the electronic representations of currency include an expiration date. Claim 2 of the ‘407 patent claims a “time-based transaction module transfer system” which embodies the idea of expiration dates on electronic notes but does not limit it to the system as otherwise described (i.e., one in which the electronic notes are current liabilities in an online accounting system of an issuing bank, a limitation added by Claim 3 in the ‘407 patent). Similarly, Claim 6 of the ‘407 patent claims a “transaction module transfer system” in which the modules have a processor that can generate a transfer record and append it to each electronic note upon transfer, not limited to the system otherwise described.

---

<sup>96</sup> See U.S. Pat. No. 5,453,601, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+932044+0+3+523074+OF+1+1+1>>.

<sup>97</sup> See U.S. Pat. No. 5,455,407, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+932118+0+3+525092+OF+1+1+1>>.

<sup>98</sup> See *supra* Part VI.D.1.

- ¶160 Among other claims relevant to the payment system are the following:
- Claim 17 of the '601 patent adds the refreshment feature. In other words, it narrows the claimed system to one in which the digital notes are updated whenever the module containing them communicates with the teller module at the bank.
  - Claim 26 claims the same system used to make loans to subscribers (by issuing a credit authorization).
  - Claim 45 adds the feature of a reconciliation system that maintains a record of money issued and compares it to money deposited. This feature is designed to detect counterfeiting.
  - Claim 76 is for a method for subscribers to exchange electronic representations of foreign currencies.

¶161 Many different electronic cash systems that can be envisioned would purportedly come under Claim 1 of the '601 patent or Claim 1 of the '407 patent, which is substantially similar except that it specifies separate online accounting systems for issuing banks and correspondent banks. (Of course, it can be expected that there will be room for argument about what an online accounting system is, and how the inclusion of one or more of them in the claims might limit these patents.) It seems clear, at least, that anyone who is considering developing or implementing a stored value system will have to consider the Citibank patents seriously.

¶162 Other stored value transaction systems are also the subject of issued patents, and presumably more are in the pipeline. It is not yet clear whether all of the patents can survive. Citibank's electronic money claims should particularly be compared with the systems claimed by EPS<sup>99</sup> and Mondex.<sup>100</sup> Prima facie, at least, the claims of the EPS patents do not include a specific device that corresponds to the "money generator module" in Citibank's claim. By contrast, it is arguable that Mondex's "value meter" is a programmed computer that functions in the same way as Citibank's "money generator module," which is also a programmed computer.

## 2. *Citibank: Integrated Systems Patents*

¶163 In addition to staking its claim in the field of digital cash per se, Citibank has also laid claim to some species of integrated systems, in which the transfer of electronic goods and the structure of rights allowed for those goods is unified with the transfer of electronic money in payment for them. Four patents relate to such combination electronic commerce systems.

¶164 Three of these patents stem from one application. They are: "Trusted Agents for Open Electronic Commerce," U.S. Pat. No. 5,557,518, issued on September 17, 1996 (forty-nine claims);<sup>101</sup> "Electronic Ticket Presentation and Transfer Method," U.S. Pat. No. 5,621,797, issued on April 15, 1997 (sixteen claims);<sup>102</sup> and "Method for Acquiring and Revalidating an Electronic Credential," U.S. Pat. No. 5,642,419, issued on June 24, 1997 (twenty-three claims).<sup>103</sup> The fourth is entitled "System and

<sup>99</sup> See *infra* Part IX.D.4.

<sup>100</sup> See *infra* Part IX.D.3.

<sup>101</sup> See U.S. Pat. No. 5,557,518, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+932284+0+4+85789+OF+1+1+1>>.

<sup>102</sup> See U.S. Pat. No. 5,621,797, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+932396+0+5+32900+OF+1+1+1>>.

<sup>103</sup> See U.S. Pat. No. 5,642,419, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+932514+0+5+54866+OF+1+1+1>>.

Method for Commercial Payments Using Trusted Agents,” U.S. Pat. No. 5,671,280, issued on September 23, 1997 (sixteen claims).<sup>104</sup> As with the electronic money patents, Citibank’s integrated systems patents were also invented by Sholom S. Rosen. They involve a method of delivering purchased information in escrow until the payment for it clears, then releasing the information to the buyer.

¶165 The ‘518 patent claims a basic protocol that enables the exchange of “electronic merchandise” for digital cash. Electronic modules called trusted agents are allied with the money modules of a merchant and a customer, such that the merchandise can be delivered to the customer’s trusted agent provisionally until the payment is duly received, at which point the merchandise is released to the customer. The modules presumably consist of computer programs.

¶166 The ‘280 patent claims the procedure by which the money modules can securely accomplish the payment, using remittance advice and commercial payment ticket messages. The ‘797 patent claims a variation of the basic protocol to accomplish exchanges of electronic tickets for services (e.g., event, transportation, and communications services). The ‘419 patent claims another variation that covers the issuance, use, and re-certification of credentials such as driver’s licenses and credit cards.

¶167 The ‘518 and ‘280 claims should be compared with the NetBill system and Open Market, which also have the feature of placing information in escrow until payment is secured. In addition, Claim 38 of the patent held by Online Resources also involves integration of delivery of electronic merchandise with payment therefor.<sup>105</sup>

### 3. *Mondex*

¶168 Jonhig, Ltd., London, was the assignee of two patents, each entitled “Value Transfer System”: U.S. Pat. No. 5,440,634, issued on August 8, 1995 (twenty-six claims),<sup>106</sup> and U.S. Pat. No. 5,623,547, issued on April 22, 1997 (twenty-seven claims).<sup>107</sup> The patents have recently been assigned to Mondex. The inventors of both patents are Timothy L. Jones and Graham R. L. Higgins, founders of Mondex International.

¶169 Claim 1 of the ‘547 patent describes the system in terms of its functional parts:

- a computer system
- electronic purses
- exchange devices comprising the means for communication between purses
- draw-down means for loading purses with value under the computer system’s control
- redemption means
- a value meter system

---

<sup>104</sup> See U.S. Pat. No. 5,671,280, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+932590+0+5+87384+OF+1+1+1>>.

<sup>105</sup> See *supra* Part IX.B.2.

<sup>106</sup> See U.S. Pat. No. 5,440,634, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+932943+0+3+508553+OF+1+1+1>>.

<sup>107</sup> See U.S. Pat. No. 5,623,547, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+932848+0+5+34729+OF+1+1+1>>.

- “one or more of said purses comprising bulk purses having value loaded and redeemed via the value meter system”

¶170 The claims of the '634 patent do not refer to the special function of the bulk purses, but rather speak in terms of a sending purse and a receiving purse. In the '547 patent, the special function of the bulk purse is part of the claims.

#### 4. *Electronic Payment Services, Inc.*

¶171 Electronic Payment Services, Inc. (EPS) is a major firm in the field of electronic funds transfer.<sup>108</sup> The firm is the holding company for both Buypass Corporation, a major third-party point-of-sale processor and debit transaction acquirer, and Money Access Service Inc., an electronic funds transfer processor operating the MAC Network, the largest electronic funds transfer network in the United States.<sup>109</sup> EPS has pursued patent rights to allow it to become a major player in the field of smart card transaction processing as well. So far, it has five issued patents relating to a transaction network that can accommodate smart cards. All of them were invented in part by Terry L. Davis, and assigned to EPS.

¶172 The first EPS patent, U.S. Pat. No. 5,577,121 (issued on November 19, 1996), is entitled “Transaction System for Integrated Circuit Cards,” and contains thirty-seven claims.<sup>110</sup> The patent was issued through an application filed on June 9, 1994, and claims the system in terms of integrated circuit cards, a security module, and verification procedures. Four more patents stem from applications dated September 30, 1994 (and at least one more may still be pending). These four incorporate by reference the specifications of the June 9, 1994, application, but claim the system more broadly, as a transaction network.<sup>111</sup> The specifications of the latter four patents characterize the system claimed in the first application as “a system wherein the present invention may be advantageously applied.”

¶173 As revealed in the specifications, as well as in the claims of the first patent, the system envisioned is a transaction system for smart cards (in the present embodiment). Using a special automated terminal, cardholders load value onto an IC card (i.e., an integrated circuit card) by debiting an existing financial account or inserting cash into the terminal. Thereafter, cardholders use the card to purchase goods and services. The IC card is inserted into a terminal at the point of purchase and, after an automatic verification and validation process, the cost of the goods or services is deducted from the balance stored on the IC card.

¶174 More specifically, in the '121 patent:

---

<sup>108</sup> See generally Electronic Payment Services, Inc., *EPS, Inc., Home Page*(visited Apr. 7, 1999) <<http://www.neteps.com/pages/home.html>>.

<sup>109</sup> See Money Access Service Inc., *About MAS*(visited Apr. 8, 1999) <<http://www.neteps.com/pages/aboutmas.html>>.

<sup>110</sup> See U.S. Pat. No. 5,577,121, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+935192+0+4+107285+OF+1+1+1>>.

<sup>111</sup> The four patents stemming from applications dated September 30, 1994, are: “Information Consolidation Within a Transaction Network,” U.S. Pat. No. 5,544,086, issued on August 6, 1996 (16 claims); “Collection of Value from Stored Value Systems,” U.S. Pat. No. 5,559, 887, issued on September 24, 1996 (26 claims); “Network Settlement Performed on Consolidated Information,” U.S. Pat. No. 5,596,643, issued on January 21, 1997 (three claims); and “Transferring Information Between Transaction Networks,” U.S. Pat. No. 5,621,796, issued on April 15, 1997 (12 claims). These four patents all have the same text for the detailed description of the preferred embodiment, and all have identical drawings. All incorporate by reference the description of the system in the earlier (June 1994) application. In addition, one of the patents (patent '643 issued in January 1997) is a division of another application of September 30, 1994, that was apparently still pending as of September 1997.

- Claims 1-18 refer to a method of transaction between an IC card bearing a particular code and a terminal including a security module, which includes comparison of encrypted data.
- Claims 18-25 refer to a “method of establishing a secure audit trail for verifying a transaction between the IC card and the terminal.”
- Claims 26-31 refer to “a method of verifying the validity of the IC card and the terminal at the initiation of and under the control of the terminal for establishing a secure session between the IC card and the terminal.”
- Claims 32-37 refer to “a method of establishing a secure audit trail at the initiation of and under the control of the terminal.”

¶175 In contrast with these specifics, the other four EPS patents claim the system in terms of networks and devices not limited to IC cards. U.S. Pat. No. 5,621,796 claims the system as a pair of networks containing “devices” (value transferring devices, a consolidation device, a network settlement device).<sup>112</sup> U.S. Pat. No. 5,621,887 focuses on the communication between the devices in the system (i.e., between the IC card and the various terminals where the value stored on the card is increased or decreased) and how the system determines what value resides where.<sup>113</sup> The ‘887 patent is nominally narrower than the ‘796 patent in one respect—it makes encryption part of the claims (but the claims are not limited to any specific kind of encryption). The ‘887 patent also specifies that the devices have ID numbers.

¶176 U.S. Pat. No. 5,544,086 focuses on how the devices in the system consolidate sums transferred and settle accounts.<sup>114</sup> The claims refer to a “cash-equivalent module” and “cash-equivalent value.” The broader claims do not include any references to encryption.

¶177 U.S. Pat. No. 5,596,643 claims “a system for determining value” and, like patent ‘796, claims the system in terms of a network (Claim 1) or a pair of networks (Claim 2).<sup>115</sup> The patent may be couched more generally than patent ‘086 in one respect—patent ‘086 refers to cash-equivalent value and patent ‘643 only to stored value.

¶178 It seems apparent that these patents will have to be considered by any entity that wishes to be in the business of clearing transactions over a network when the transactions involve smart cards. In addition, the claims should be compared with those of the Citibank electronic money patents<sup>116</sup> and the Mondex stored value system patents.<sup>117</sup>

---

<sup>112</sup> See U.S. Pat. No. 5,621,796, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+950335+0+5+32899+OF+1+1+1>>.

<sup>113</sup> See U.S. Pat. No. 5,621,887, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+950335+0+5+32899+OF+1+1+1>>.

<sup>114</sup> See U.S. Pat. No. 5,544,086, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+950571+0+4+71118+OF+1+1+1>>.

<sup>115</sup> See U.S. Pat. No. 5,596,643, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+921095+0+5+6615+OF+1+1+1>>.

<sup>116</sup> See *supra* Part IX.D.1.

<sup>117</sup> See *supra* Part IX.D.3.

E. *Selected U.S. Patents Relating to Internet Payment Technologies*1. *Open Market, Inc.*

¶179 Open Market, Inc. is an electronic commerce software company founded by Shikar Ghosh and David B. Gifford.<sup>118</sup> In March 1998, Open Market announced the issuance of three patents, invented by Gifford and assigned to Open Market, relating to Internet payment technologies. Described as “breathhtaking” in scope,<sup>119</sup> the three patents—U.S. Pat. Nos. 5,708,780,<sup>120</sup> 5,715,314,<sup>121</sup> and 5,724,424<sup>122</sup>—purport to cover a wide range of Internet technologies.

¶180 The ‘780 patent claims a method for using session identifiers to restrict access to information made available over the Internet and to track requests for that information. The claimed method relies on server systems to check all incoming requests for session identifiers. If the server does not find a session identifier, it redirects the request to another server which, after confirming that the source of the request is authorized to retrieve the requested information, assigns the source a session identifier. The claimed method then uses the session identifiers to track the requests of different sources.

¶181 The ‘314 patent lays claim to a network sales system. One variant of the claimed system, set forth in Claims 34 through 39, includes an online shopping cart which allows users to store multiple representations of products and to purchase those products with a single payment method.

¶182 The ‘424 patent stakes the broadest claim, purporting to cover systems for securing consumer payment information in Internet transactions. Although various elements of the claimed system change in the patent’s fifty-eight claims, the security system remains essentially constant. In the claimed system, a consumer generates a “payment request” that apparently contains the consumer’s private payment information. The system relies on a “digital signature” and a “principal-specific secret key,” which identify the consumer and protect the payment request from forgery and replay attack.

2. *DigiCash*

¶183 David Chaum has almost a dozen digital cash patents, which were assigned to now defunct DigiCash in 1996.<sup>123</sup> A group of the Chaum patents relate to deployment of cryptographic techniques, in particular to techniques of “blinding,” which let banks issue authenticated digital coins while allowing the user to remain anonymous. Other patents relate to tamper-resistant hardware and software implementations of this system, and to a system that sets up trusted third parties to verify digital signatures.

---

<sup>118</sup> See generally Open Market, Inc., *The Open Market Vision* (visited Apr. 8, 1999) <<http://www.openmarket.com/over/>>.

<sup>119</sup> Paul C. Judge, *They’ve Got the Patents—But So What?*, BUS. WK., June 1, 1998, at 154.

<sup>120</sup> See U.S. Pat. No. 5,708,780, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+921729+0+6+5362+OF+1+1+1>>.

<sup>121</sup> See U.S. Pat. No. 5,715,314, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+921777+0+6+12838+OF+1+1+1>>.

<sup>122</sup> See U.S. Pat. No. 5,724,424, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+921823+0+6+23160+OF+1+1+1>>.

<sup>123</sup> DigiCash announced that it had filed for Chapter 11 reorganization in November 1998.

a) *Blind Signature Systems*

¶184 U.S. Pat. No. 4,759,063 was issued on July 19, 1988, and is entitled, “Blind Signature Systems” (forty-one claims).<sup>124</sup> U.S. Pat. No. 4,759,064 was also issued on July 19, 1988, and is entitled, “Blind Unanticipated Signature Systems” (forty-four claims).<sup>125</sup> The basic scenario contemplated by the invention is the signing of digital coins by a bank without it being able to find out later who is spending them. The initiating party (the customer) would first blind the message and then submit it to a third-party signer (the bank) for a signature. The initiating party would then be able to unblind the signed message received from the bank and recover the original message with the bank’s digital signature on it. Thus, the message would now be an authenticated coin, but because the message identifying the coin (i.e., its serial number) is not known to the bank, it will not know who is subsequently spending the coin.

¶185 The basic blinding methodology claimed in these two patents involves having the bank sign a large number of messages from the customer without knowing which one is the one that will actually be used. RSA public key cryptography is described as the type of digital signature envisioned in the preferred embodiment. The ‘064 patent is put forward as an improvement on the ‘063 patent in not requiring computation during blinding for anticipating which of a plurality of possible signatures will be made by the bank during signing.

¶186 Claim 1 of the ‘063 patent is for a method for processing a plurality of digital messages before and after they are “transformed with public-key digital signatures by a signer party” (i.e., a bank), in which the processed messages are said to be blinded because, “although the public key digital signatures of said resulting digital messages are checkable using a public key, the signer is unable to determine the correspondence between” individual messages before and after processing. The method has the following steps:

- “blinding a plurality of original digital messages by a plurality of corresponding supplier parties (*i.e.*, customers) transforming each such message at least partially responsive to a corresponding first key to produce corresponding digital first messages;”
- “signing each of said first messages by a signing party applying a public key digital signature thereto to produce a corresponding plurality of digital second messages;”
- “unblinding said plurality of second messages by said supplier parties transforming each at least partially responsive to said first keys to produce a corresponding plurality of digital third messages which retain a public key digital signature property related to said original messages and to said signing step;” and
- “said blinding step being performed by said supplier parties using said first keys so as to make said signer party without the corresponding first keys unable to readily determine the correspondence between individual messages within said plurality of third messages and individual messages within said plurality of first messages.”

---

<sup>124</sup> See U.S. Pat. No. 4,759,063, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+935733+0+2+212813+OF+1+1+1>>.

<sup>125</sup> See U.S. Pat. No. 4,759,064, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+935913+0+2+212814+OF+1+1+1>>. Although the two patents were issued on the same date, the first one stems from an application dated August 22, 1983, and the second from an application dated October 7, 1985.

¶187 Claim 1 of the '064 patent is similar except that it refers to a set of secret signing keys, and the first step adds a phrase about not needing to anticipate which key in the set the bank will use. It thus reads:

blinding a plurality of original digital messages by a plurality of corresponding supplier parties transforming each such message at least partially responsive to a corresponding first key to produce corresponding digital first messages, without anticipating which of a set of corresponding signing keys will be used to sign each first message

¶188 Other Chaum patents build upon and extend this system. U.S. Pat. No. 4,914,698, issued on April 3, 1990, and entitled "One Show Blind Signature Systems" (one claim), is directed at detection of double spending.<sup>126</sup> U.S. Pat. No. 4,947,430, issued on August 7, 1990, and entitled "Undeniable Signature Systems" (forty-eight claims), is directed at non-repudiation.<sup>127</sup> U.S. Pat. No. 4,949,380, issued on August 14, 1990, and entitled "Returned-Value Blind Signature Systems" (fourteen claims), is directed at making change for digital cash.<sup>128</sup> U.S. Pat. No. 4,991,210, issued on February 5, 1991, and entitled "Unpredictable Blind Signature Systems" (four claims), claims blind signature systems that are secure against chosen message attacks.<sup>129</sup>

---

<sup>126</sup> See U.S. Pat. No. 4,914,698, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+918664+0+2+380193+OF+1+1+1>>. The scenario contemplated by the invention in the '698 patent is a customer who purchases digital coins with blind signatures in denominational amounts from a bank. The customer then spends the signatures at shops which can check with the bank in an online transaction whether the signed coin has already been spent elsewhere. The basic methodology is a challenge-and-response system, which functions to reveal the identity of a customer, but only if that customer has previously engaged in the challenge-and-response process (i.e., only if the coin has previously been spent). It does this by dividing up the identifying information in such a way that going through the process more than once will reunite the parts.

The steps of the claimed method include "issuing a plurality of signatures to insure that each said signature contains identifying information divided between at least two parts"; "showing and checking said digital signatures to reveal at least one of said at least two parts of each"; and "performing a test on a set of said signatures shown, that would yield at least one of said identifiers if different parts of at least one of said issued signatures had been revealed in showing at least one issued signature more than once."

<sup>127</sup> See U.S. Pat. No. 4,947,430, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+918914+0+2+415819+OF+1+1+1>>. The '430 patent extends the challenge-and-response protocol by enabling whoever is verifying a signature to distinguish between a situation where the signature is not valid and a situation where the signer is responding improperly to messages in an effort to deny a valid signature. The invention is thus directed to non-repudiation. Claim 1 is for "a cryptographic method for forming and checking undeniable signatures where the signatures are called 'undeniable' because they can be verified in a protocol between a signing party and a checking party and the signing party is unable to conduct the protocol improperly so as to 'deny' the validity of a valid undeniable signature previously issued by the signing party without such improper denial giving at least a probability with at least a known lower bound that the checking party will learn that the signing party has conducted the protocol improperly." (Claim 37 adds the limitation that the lower bound on the probability of learning of the signer's improper denial is known to be at least one half.)

<sup>128</sup> See U.S. Pat. No. 4,949,380, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+918977+0+2+417934+OF+1+1+1>>. The '380 patent discloses methods for making change (i.e., returning a lesser value from previously higher-value signatures after transactions which do not use up all the value inherent in a signature). Because of the blinding process, the payments cannot be linked to withdrawals, and the returned difference can be accumulated across payment transactions and can be divided between a plurality of payment transactions. The preamble in Claim 1 locates the invention "in a method for transferring value between parties that is based on public-key-digital blind signatures," and the claim is for the improvement whereby digital signatures on blinded messages can be used to diminish value.

Claim 1 does not refer to specific encryption algorithms or any details about the method other than that it is based on public-key blind signatures. Claim 8 is an apparatus claim in means-plus-function form ("means for diminishing the value of a first blind signature by a first party from an original value to a diminished value," and so on). The specification describes a system that uses RSA but states that other mathematical functions can be used.

<sup>129</sup> See U.S. Pat. No. 4,991,210, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+919046+0+3+11516+OF+1+1+1>>. In a chosen-message attack, the attacker chooses a special dangerous message, obtains a signature on it, and then is able to use this signature to break the whole signature scheme. The purpose of the '210 patent is to flesh out the requirement in the basic '063 patent that the underlying system be secure against chosen-message attack. The method involves having the data processor of

*(footnote continued)*

¶189 U.S. Pat. No. 4,996, 711, issued on February 26, 1991, and entitled “Selected Exponent Signature Systems” (fifteen claims), discloses a method whereby the customer selects exponents for the signature, which is said to improve computation, storage, and bandwidth requirements for blind signature systems, and prevents the bank from falsely incriminating a customer by claiming double spending.<sup>130</sup> Another patent, U.S. Pat. No. 5,434,919, issued on July 18, 1995, and entitled “Compact Endorsement Signature Systems” (six claims), is directed at compressing the signature functions so that endorsement of notes will take up less storage space.<sup>131</sup>

b) *Tamper-Resistant Microprocessors*

¶190 U.S. Pat. No. 4,926,480, issued on May 15, 1990, and entitled “Card-Computer Moderated Systems” (eighteen claims), envisions a hand-held personal computer configured to include an independent tamper-resistant microprocessor that can take the form of a smart card.<sup>132</sup> One use for the invention is to accomplish the one-show blind signatures used in payments.<sup>133</sup> The tamper-resistant microprocessor can construct or check the form of the messages between the card and the bank, and possibly obtain the final signature from the bank. The point of the invention is that even if tamper resistance is compromised, security is not completely lost, because the cryptographic security remains. Other uses for the invention include creating credentials for authorizing individuals to enter restricted areas or use restricted data.

¶191 The patent covers an apparatus that implements the challenge-and-response protocol of the ‘698 patent, and there are corresponding method claims as well. Note that in U.S. Pat. No. 5,131,039, described next, Chaum criticizes the approach of this patent in the embodiments to date, because it would require that the hand-held computer and/or the tamper-resistant smart card make cryptographic transformations during transactions with an external system. The specification of the ‘039 patent states that “these ‘while-you-wait’ computations, as well as other preparatory computations, would make extensive use of public-key cryptographic techniques, which would be impracticably slow with today’s smart cards.”

¶192 U.S. Pat. No. 5,131,039, issued on July 14, 1992, and entitled “Optionally Moderated Transaction Systems” (nine claims), discloses a tamper-resistant part (e.g., a smart card or a portion of its memory) that can conduct transactions with an external system through a moderating user-controlled computer.<sup>134</sup> It is intended as an improvement on the ‘480 patent above, providing for pre-computation of portions of the blind signature protocol to avoid the inefficiency of “while-you-wait” computations. A continuation of patent ‘039, U.S. Pat. No. 5,276,736, issued on January 4, 1994, and also entitled “Optionally Moderated Transaction Systems”

---

a blind-signature issuing party apply exponents to candidate messages provided to it where these exponents cannot be determined by the party providing the candidate messages.

<sup>130</sup> See U.S. Pat. No. 4,996, 711, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+919683+0+3+17618+OF+1+1+1>>.

<sup>131</sup> See U.S. Pat. No. 5,434,919, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+919741+0+3+502148+OF+1+1+1>>.

<sup>132</sup> See U.S. Pat. No. 4,926,480, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+914948+0+2+392884+OF+1+1+1>>.

<sup>133</sup> The system is described in conjunction with the ‘698 patent. See *supra* note 126.

<sup>134</sup> See U.S. Pat. No. 5,131,039, available at <<http://patents.uspto.gov/cgi-bin/ifetch4?ENG+PATBIB-ALL+0+915042+0+3+165285+OF+1+1+1>>.

(eight claims), is directed toward use of the same tamper-resistant part and moderating computer to improve on the earlier blind signature system, such as that in the '063 patent, by restraining customers from spending more than the value stored in their equipment (rather than having double spending show up only after the fact).<sup>135</sup>

c) *Third-Party Signature Confirmation*

¶193 U.S. Pat. No. 5,373,558, issued on December 13, 1994, and entitled “Designated-Confirmer Signature Systems” (twenty-four claims), involves the equivalent of certificate authorities.<sup>136</sup> Its intent is to deal with a difficulty in the method of “undeniable signatures”:<sup>137</sup> the fact that the signer needs to be available and to cooperate in any subsequent confirmation of a signature. If the signer were to die or default, then the signature would be useless to the recipient.

¶194 This patent contains general method and apparatus claims for the procedure of signing, receiving, verifying, and confirming designated-confirmer signatures, in which designated confirmers are third parties in the business of validating signatures. The basic idea envisioned is that the signing party can prove to the receiving party that a third-party confirmer can verify the signature without the original signer’s cooperation (thus providing for non-repudiation). However, without the cooperation of the third-party confirmer, the receiving party cannot use the signature by showing it convincingly to someone else. There can be more than one confirmer: Some of the claims involve “hinged” signatures, which are hierarchies in which one confirmer party is validated by another, and so on.

3. *Bell Communications Research*

¶195 Bell Communications Research is the assignee of a patent entitled “Efficient Electronic Money,” U.S. Pat. No. 5,511,121, issued on April 23, 1996, and invented by Yacov Yacobi (fifty-one claims).<sup>138</sup> The system envisioned uses an El Gamal signature scheme<sup>139</sup> (in conjunction with other public key cryptographic techniques) to protect privacy of users in legitimate transactions, while at the same time permitting the identity of a double spender of a particular electronic coin to be revealed.

¶196 The El Gamal scheme involves constructing a digital coin as a certified linkage between a public key and a random element such that if the user invokes the random element more than once, the linkage becomes transparent and the user’s identity is revealed. Thus, if a bank detects double spending, it can identify the user, but if an e-coin is only deposited once, the bank would have no way of discerning the identity of the payer from the transaction record. Furthermore, the e-cash could be used in direct transactions from payer to payee, deposits, exchanges, and withdrawals and would require as few real-time operations as possible.

---

<sup>135</sup> See U.S. Pat. No. 5,276,736, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+915111+0+3+326482+OF+1+1+1>>.

<sup>136</sup> See U.S. Pat. No. 5,373,558, available at <<http://patents.uspto.gov/cgi-bin/iftch4?ENG+PATBIB-ALL+0+936227+0+3+433844+OF+1+1+1>>.

<sup>137</sup> See *supra* note 127.

<sup>138</sup> See U.S. Pat. No. 5,511,121, available at <<http://www.bellcore.com/BC.dynjava?BellcoreHomeHomeGeneralHome>>.

<sup>139</sup> See generally RSA Data Security, Inc., *What Are Some Other Public-Key Cryptosystems?* (visited Apr. 9, 1999) <<http://www.rsa.com/rsalabs/faq/html/3-6-8.html>> (describing the ElGamal system).

¶197 The envisioned implementation is a network including a plurality of electronic e-coin processing units such as portable money modules belonging to users, one or more banks, and a certificate authority. The portable money modules include a microprocessor and memory. They may be connected to one another temporarily via telephone by means of a modem, or via various wireless modalities. The bank station comprises a server and memory, with the server connected to the telephone network. The certificate authority station also includes a server and memory, with the server connected to the telephone network.

¶198 The patent specification describes the operation of the coin in the context of typical transactions:

- *Payment*: The payor sends a coin to a payee, and the payee verifies the certificate (i.e., bank signature). The payee challenges the payor to sign a message using a signature from the El Gamal family along with the public key and random element embedded in the coin. If the coin has already been signed/spent, the identity of the payor is exposed.
- *Deposit*: If the payee wants to deposit the coin in a bank, the payee transmits the coin and the payor's El Gamal signature to the bank. The bank verifies the coin and compares it to a list of previously deposited coins to make sure it was not deposited in the past.
- *Exchange*: In an exchange of old money for new, the payee would deposit old coins in the banks and get new coins in the same total value without the payee's identity revealed (unless, of course, the payee was attempting the exchange after already spending the coin).
- *Withdrawal*: In a withdrawal, a blinded linkage between a public key and a random element is transmitted to the bank (the blinding is used so that the bank does not discern the identity). The bank verifies the proper structure of the linkage and returns it to the user who then formulates a coin.
- *Certification*: To obtain the certification of her public key by the certificate authority, the user transmits a blinded candidate certificate incorporating a random element with the key. The user proves to the certificate authority that the key is properly formatted (i.e., related to the user's identity) without revealing the user's identity, using cryptographic techniques that enable only enough information to be revealed to accomplish the proof. The certificate authority then issues the certificate.
- *Refreshment*: The public key and certificate can be refreshed periodically to guard against breaches of security external to cryptography. In this procedure the user selects a new key and a random element, then goes through a similar procedure with the certificate authority.

¶199 Claim 1 of the patent purports to cover all of these functions by referring to a method for performing "an electronic cash transaction," comprising the step of transmitting between two "electronic coin processing unit[s]" an electronic coin "comprising a linkage of a public key of a party and a random element, said linkage being signed using a secret operation of public key cryptographic system, wherein said public key" is a public El Gamal key of the party (the customer). In Claim 2, "said linkage is signed using an RSA secret exponent of a bank."

¶200 Other method claims are directed to the types of transactions envisioned. Claim 17 is for a method for "detecting the double spending of a particular electronic coin in an electronic coin system where each of the coins comprises a certified linkage of a public key of a user and a random element." Claim 20 is for a method for performing a payment; Claim 28, for processing an electronic coin at a

bank station; Claim 33, for electronically withdrawing an electronic coin from a bank; Claim 34, for certifying a public key of a user of an electronic cash system; and Claim 36, for refreshing a certificate of a public key of a user.

¶201 The patent also contains claims for the coin itself. Claim 38 is for an “electronic coin . . . comprising a certified linkage between a public key  $P_i$  of a party  $i$  and a random element chosen by the party  $i$ , the identity  $I_i$  of the party  $i$  being embedded in the discrete log of the public key and being exposed when there is double spending of the coin.”

¶202 The Bell system has a number of features in common with the Citibank system and the Chaum system, such as creating and validating digital coins, exposing double spending, making change, refreshing certificates, using challenge-and-response systems, using third-party signature authentication, and using RSA public-key cryptography in the preferred embodiment. Each of the patents contains broad claims that arguably overlap, even if the narrower claims are more differentiated. Chaum’s patents are earlier than the others. If the owners of the DigiCash patents choose to challenge either Citibank or Bell, the two providers will have to show that their systems are non-obvious in light of Chaum’s patents, which might be difficult to do for the broadest of the claims. As of late 1997, DigiCash was struggling to make headway in the market, whereas the Citibank system is under development but has not been rolled out, and the status of the Bell system is unknown. A firm intending to license one of these systems and enter the market would be prudent to undertake a thorough investigation of these patents before doing so.

## X. APPENDIX B: GENERAL CRYPTOGRAPHIC PROCESSES AND TERMS RELATED TO CRYPTOGRAPHY<sup>140</sup>

### A. Key Processes

#### 1. *The Process of Symmetric (Secret Key) Encryption for Sending a Message.*

- A plaintext message exists in a form humans can read while the encrypted product is called ciphertext. A key is a data string used by an algorithm for encryption and decryption, the value of which affects the result. In symmetric key cryptography, all parties wishing to communicate must somehow previously have been distributed a shared secret key.
- When A wants to send a message to B, A encrypts a plaintext message using the shared symmetric key. B also has this key.
- When Party B receives the message, she must decrypt it using the same shared secret key.
- Once decrypted, the ciphertext becomes readable plaintext again.

#### 2. *The Process of Asymmetric (Public Key) Encryption for Sending a Message.*

- Parties A and B, who want to communicate securely, each uses her computer to generate a pair of keys: a public key and a private key.

---

<sup>140</sup> See generally RSA Laboratories, *Frequently Asked Questions About Today's Cryptography* (visited Nov. 24, 1998) <<http://www.rsa.com/rsalabs/faq/>>.

The public key is published and widely distributed while the private key is secret.

- When A wants to send a message to B, she looks up B's public key in a public directory (or gets it some other way) and uses it to encrypt the message. After encrypting the message, A sends it to B.
- B uses her private key to decrypt the message.
- Anyone can have access to B's public key and can send B a message, but only B has access to the private key needed to decrypt it.
- The reason the process works is because of a one-way function. The calculation is simple to do in one direction, but difficult to do in the reverse direction. One analogy is to a simple mathematical process—it is easy to square a two-digit number without a calculator but far more difficult to find the square root of a four-digit number.

### 3. *Use of Asymmetric (Public Key) Encryption for Authentication (Identity of Sender).*

- A wants to send a message to B, but B wants to be sure that A is really the sender.
- Rather than encrypting the message with B's public key, A can encrypt the message with A's own private key.
- B can decrypt the message by applying A's public key. If A's public key works, then B knows A produced the message, provided that B has a way of authenticating A's public key. B can be confident the message is from A because only A has A's private key, and only A's private key can produce a message that A's public key can decrypt.

### 4. *The Process of Using a Message Digest with Asymmetric (Public Key) Encryption for Authentication (Identity of Sender and Message Integrity).*

- A computes a message digest using a hash algorithm (see below) and encrypts this shorter message digest with her private key. This message digest, encrypted with A's private key, can be thought of as A's digital signature.
- A transmits the message (which may be in plaintext or may be encrypted), along with the encrypted message digest (digital signature) to B.
- When B receives the message and the message digest, B uses the same hash algorithm to produce another message digest.
- B then uses A's public key to verify that the message digest she just computed matches the message digest (or digital signature) that A included with the message.
- If the two message digests match, B can be certain both that the message has not been altered (message integrity) and that the message comes from A (identity of sender).

### 5. *The Process of Sending a Message in a Digital Envelope.*

- When A wants to communicate securely with B and does not want to use only secret key cryptography because of the risk that the key might be compromised, but also does not want to use only public key cryptography because of its inefficiency (the inefficiency being due largely to speed issues), A can combine the two techniques.

- A creates a plaintext message and encrypts it with a secret key using a symmetric encryption algorithm, such as DES (see below).
- A then encrypts the secret key using a public-key encryption algorithm such as RSA (see below) with the public key of B so that B will be able to decrypt the secret key.
- A transmits both the encrypted message and the encrypted secret key to B.
- B uses her private key to “open the envelope” (decrypt the secret key).
- Then B uses the secret key to decrypt the message.

#### 6. *Use of Digital Certificates to Verify Identity*

- A wants B to know that she can use A’s public key to send A messages.
- A must prove to B that A is who she says she is.
- A goes to a trusted third party called a “certification authority” or “CA”.
- The CA, after verifying A’s identity, uses the CA’s private key to sign a message, called a digital certificate, that says “A’s public key is X.”
- When B wants to send a message to A, B gets the digital certificate and, using the CA’s public key, verifies that the CA signed the message.
- If the CA’s signature checks out, this confirms that A is who she says she is.

#### B. *Key Terms*

*Attack:* A method by which a third party tries to recover a cryptographic key in order to be able to decrypt messages.

*Blind Signature:* A method that allows a person (for example, a bank) to sign a message (for example, a piece of digital cash) without seeing its contents.

*Certificates:* A certificate is the digital signature of a certificate authority, a trusted third party in the business of guaranteeing the identity of holders of public keys. In order to authenticate his public key, the sender can attach a certificate to the message. Using the public key of the certificate authority (users are presumed to have the public keys of certificate authorities), the recipient can verify the certificate, and the sender’s public key will then be authenticated.

*Certification Authority (CA):* A trusted third party that issues certificates that link public keys to the particular identity of the holder. VeriSign, Inc., a spin-off of RSA Data Security, is one such firm. The United States Postal Service has proposed itself to be an appropriate certification authority.<sup>141</sup>

*DES:* The Data Encryption Standard is a complex algorithm employing a block cipher that goes through sixteen stages to encrypt, was adopted by

---

<sup>141</sup> See United States Postal Service, *Postal Service Leverages Private Sector Expertise to Enable Electronic Commerce Through the Internet* (last modified Oct. 16, 1996) <<http://www.usps.gov/news/press/96/96108new.htm>>. But see Jane Kaufman-Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1215 n.150 (1998).

the U.S. government in 1977. It operates on one block of data at a time, and it encrypts 64 bits of plaintext to produce an equal number of bits of ciphertext. The DES key length is 56 bits. DES is a symmetric key encryption algorithm, meaning that both parties must possess the single secret key.

*Digital Signature.* Public key cryptography can be used for authentication purposes through the use of a digital signature. This signature, which is created by encrypting a message digest with the sender's private key, is sent along with the message (which can be encrypted or in plaintext). The recipient decrypts the message digest with the sender's public key, and compares it to the message digest she computed herself. If the two match, the integrity and origin of the message is assured.

*Dual Signature.* In protocols where more than two parties are involved, the dual signature provides a link between a message and an identity without disclosing the contents of the message. For instance, in a credit card purchase, the information concerning the content of the purchase can be separated from the financial details that make the transaction possible.

*Export Control.* Strong cryptography is restricted to use within the United States through the use of export controls because cryptography is traditionally classified as munitions.<sup>142</sup> The export of commercial cryptography and machines that contain cryptography is covered by the Export Administration Regulations (EAR),<sup>143</sup> and companies have to obtain a license from the Bureau of Export Administration of the U.S. Department of Commerce. These restrictive controls on export are the subject of extensive industry debate and government lobbying efforts.

*Hash Algorithm.* An algorithm used to create a message digest, a shorthand way of ensuring message integrity. In other words, hash functions reduce a large file to a relatively short number which is then used as a surrogate for the full file. Hash algorithms should be resistant to collision, meaning that two messages should not have the same hash. In addition, hash algorithms should be difficult to invert—an analyst should not be able to recreate a message with a given hash.

*Kerberos.* A security protocol developed by MIT and typically used in domain-wide (private) network environments. A central server (Kerberos server, or KDC for Key Distribution Center) stores the keys of each client on the network and plays the role of authenticator. When a user and an application server wish to communicate, they exchange tickets<sup>144</sup> issued by KDC to authenticate each other. Because KDC houses so much sensitive information (secret keys and identification data) of the clients, the server needs to be kept locked up using conventional security methods (i.e., locks, vaults, and guards).<sup>145</sup>

---

<sup>142</sup>See United States Munitions List, 22 C.F.R. § 121.1 (1998). The current version no longer contains general cryptographic items, but military cryptographic (including key management) systems and some others are still on the list.

<sup>143</sup> 15 C.F.R. § 730-744 (1998).

<sup>144</sup> Tickets are special messages that authenticate a party's identity.

<sup>145</sup> For more information about Kerberos, see generally Massachusetts Institute of Technology, *Kerberos: The Network Authentication Protocol* (last modified June 29, 1998) <<http://web.mit.edu/kerberos/www/>>.

*Key Escrow.* A process wherein a copy of the key used by every encryption program is held in trust by an appropriate escrow agent (preferably a neutral third party). Key escrow was the subject of a series of failed Clinton administration proposals.<sup>146</sup> One such proposal, key recovery, provides that every encrypted communication be prefaced by a special-key recovery data block which contains the session key used to encrypt the message. This session key is itself encrypted with a public key belonging to the key recovery service. Essentially, key recovery is one step removed from key escrow since the key recovery service does not hold any user's private key. However, if the private key of the key recovery service is compromised, many users will have all of their messages potentially subject to attack.

*Man-in-the-Middle Attack:* An attack where communications between two parties are intercepted in order to enable funds to be transferred (or diverted) to the attacker.

*Message Digest:* A digesting or hash algorithm is applied to a message to produce a shorter message digest. The message digest is useful for verifying the identity of the sender and the integrity of the message, because it is extremely unlikely that two different messages would have the same digest.

*Public Key Encryption:* Also known as asymmetric encryption cryptography. Each party has a key pair, and one key is made public while the other is kept private. Information encrypted with either component of the pair can be decrypted only with the other component. The advantage of public key encryption is that the public key can be made available to everyone without compromising security while the private key is not distributed at all.

*Replay Attack:* An attack where valid messages are recorded and played back in different context. For example, a message to transfer funds could be played multiple times to transfer funds to an attacker. One way to thwart such an attack is to use a message authentication code that gives each message a unique sequence number.

*RSA:* The de facto standard algorithm for public-key cryptography. RSA can be used for both encryption and authentication purposes. Invented by Rivest, Shamir, and Adelman in 1977, its security is largely based on the difficulty and time-consuming nature of factoring large numbers. The public and matching secret keys are generated through a computational process involving prime numbers and Euclid's algorithm. Encryption takes place by breaking the message into blocks and performing computations on each block. The typical key size ranges from 512 bits to 2048 bits. Due to speed concerns, RSA is often used to create digital envelopes (see above) to protect secret keys, rather than to encrypt message text itself.

*Server-Substitution Attack:* In this form of attack, attackers pose as merchants in order to steal confidential consumer information (e.g., credit card numbers). Message authentication can prevent this type of attack.

*SET:* Secure Electronic Transactions. A standard proposed by Visa and MasterCard for processing credit card transactions over networks.

---

<sup>146</sup> Key escrow was an important part of the original Clipper Initiative. See the April 16, 1993, White House press release at <<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/1993/4/19/6.text.1>> (proposing that a "key-escrow" system be established to prevent the abuse of the Clipper chip). Though the Clinton administration eventually abandoned the Clipper chip, it never stops trying to promote some sort of key-escrow system.

*SHA*: Secure Hash Algorithm.

*Symmetric or Secret Key Encryption*: A form of cryptography which uses the same key to both encrypt and decrypt data. Transfer of the key between parties (*i.e.* key distribution) without outside knowledge is one difficulty of secret key encryption.

## XI. APPENDIX C: GLOSSARY OF TERMS

*Acquirer:* In a typical payment transaction, a merchant accepts a payment card from a customer for the provision of goods or services. The merchant then presents the card transaction data to an acquirer for verification and processing. An acquirer is usually a bank or a third-party processing firm separate from the merchant, the customer, and the issuer of the card.

*Analog:* Generally means not a digital transaction. An example of an analog payment transaction would be paying a bill by writing a paper check and sending it in a paper envelope via the postal service.

*Application:* Software (i.e., a computer program) that provides a service to a user such as word processing or spreadsheet functions. An application can be understood in contrast to a program that operates the computer (e.g., Windows 95) or a program that facilitates connection to other computers (e.g., TCP/IP).

*Architecture:* The physical and operational structure of a computing configuration. Architecture can include hardware (physical machines or silicon chips), operating systems, software applications, and network interfaces. Architecture can either be closed (i.e., governed by proprietary rights with specifications not observable by the user) or open (i.e., governed by non-proprietary standards and specifications readily observable by the user).

*ATM Network:* Automatic Teller Machines are self-service units that allow financial transactions such as deposit and withdrawal with proper identification and account relationship. An ATM network can be visualized as the entire collection of ATMs that allow users from different banks to complete financial transactions (e.g., the network of Cirrus or Plus). An ATM network can also refer to a private bank network (e.g., VersaTeller or Wells Fargo) in the sense that customers using the network of their own bank are not charged usage fees.

*Authentication:* The process of verification that a particular name and claimed identity match.

*Automated Clearing House:* An organization that handles automated payments such as direct debits, payroll deposits, and credit transfers. The clearing house can also consolidate billing services. The Federal Reserve's ACH is a private banking network for settlement of financial transactions.

*Back End:* Behind the scenes processes (from the customer's point of view) of payment, transfer and settlement.

*Batch Processing:* Batch processing bundles several computer processes together so that they can run more quickly and more efficiently. For example, a merchant engaged in electronic commerce might transmit collections of small transactions once or twice a day as opposed to each time a transaction takes place.

*Biller:* Firms issuing bills.

*Bit:* A bit is the basic element of electronic information and is derived from the words "binary digit." Consisting of zeros and ones for switches (switches are either on or off), electronic messages are composed of bits.

*Blind Signature:* A method that allows a person or an organization, such as a bank, to sign a message without seeing its contents.

*Browser:* Software that runs on a user's personal computer and provides access to data on the World Wide Web. Netscape Navigator and Microsoft Internet Explorer are examples of popular browsers.

*Certificates:* A certificate is actually a digital signature. In a payment transaction, the certificate acts as verification because it vouches for the authenticity of the sender's cryptographic key.

*Certification Authority:* A trusted third party who issues certificates.

*Check and List:* In a bill payment system that uses this procedure, the bill payment processor sends one check via postal mail to the firm whose bills are being paid, along with a list of customer accounts to which the aggregated payments must be credited.

*Checksum:* A value computed through a special procedure and used to verify the integrity of a message (block of data).

*Clearance:* The procedures involved in clearing financial transactions between parties, typically banks, such as reconciliation, billing, and statement processing.

*Click:* The action of pushing the button on a mouse when the cursor on the screen points to data on a program the user wants to select or "open." Clicking on hypertext links will transport the user to the data or location specified by the link.

*Client-Server:* A model of computing that allows for the distribution of work across computers. For example, a desktop PC (the client) can request access to a file or program from a remotely located computer (the file server).

*Configuration:* A particular arrangement of software, hardware, operating systems, and/or network connections.

*Content:* The actual information involved in a transaction (i.e., the text of a message or the information provided in a payment transaction). Also information such as newsletters, stories, and music that is published and sold.

*Customer Interface:* A customer interface can refer to both the connection between the customer and the payment mechanism, and between the customer and the merchant. The screen the customer sees, with a brand name and other identifying features, is the most important aspect.

*Database:* A collection of information and data arranged in a searchable fashion.

*Decryption:* The process of recovering plaintext from an encrypted message.

*Dialog Box:* A message box appearing on a user's computer screen with specific instructions or error notification.

*Digital Cash:* Cash existing in digital rather than analog (i.e., paper) form. Digital cash exists as a string of bits (i.e., a digital block of data) and is stored on devices such as the user's hard drive or stored-value cards.

*Digital Signature:* A digital signature is generated for authentication purposes by means of public key cryptography.

*Distributed Computing:* The idea of performing portions of a transaction or task on different or multiple computers. Client/server computing can be considered a form of distributed computing since programs and data which function in concert are spread out across networked computers.

*Double Spending:* The fraudulent act of spending digital cash more than once. A serious problem because digital data is so easily replicated.

*Download:* The process of bringing information from a remote site (i.e., another computer or web site) to your own computer.

*Electronic Funds Transfer:* A funds transfer sent electronically through telecommunications devices or through magnetic media. Usually refers to the transfer of funds through established private banking channels.

*Electronic Merchandise:* Information in digital form that is offered for sale through electronic means.

*Electronic Wallet:* A software application program or hardware device such as an integrated circuit card or hand-held terminal that can store credit card information and/or digital cash and which can execute a variety of financial transactions.

*E-mail:* Electronic mail sent and received over a network.

*Encryption:* The process of encoding a text message or other information in order to maintain its secrecy.

*Firewall:* A security measure employed on networks that allows and prevents receipt of certain types of network information and messages. Firewalls are installed at the point where network connections enter a site.

*Firmware:* A program layer between physical hardware and applications software. Often, the operating system (e.g., Windows 98 or MacOS 8.5) is called firmware. Also, the built-in program on a stored-value card, implemented on a chip, is called firmware.

*Front End:* The communications network equipment located at a central site and used to interface with individual processes and protocols. In other words, the system that communicates between buyer and seller (customer and merchant).

*FTP:* File Transfer Protocol is one of the oldest ways of transmitting information over the Internet from a server computer to a client computer.

*Gateway:* A computer connecting multiple networks. Gateway computers or gateway servers route packets among appropriate destinations. Gateway computers also translate information from one format to another.

*GUI:* A Graphical User Interface is the “look and feel” of the screen as the user interacts with a program. GUI generally refers to the appearance of an application or operating system.

*Handshaking:* A process taking place between two hardware devices such as a modem or card, or two computers such as a client and server, that establishes a common dialog for communication and interface.

*Hardware:* The physical components of a particular computing configuration such as the terminal, monitor, modem, and data storage devices.

*HTML:* This acronym stands for HyperText Markup Language, the language used to write Web pages.

*HTTP:* This acronym stands for HyperText Transfer Protocol and is the TCP/IP protocol for transferring Web pages across the Internet from one computer to another. Allows for the transfer of multimedia and hyperlinked data.

*Hypertext:* The linkage of related documents that reside on different network sites (computers). Links can be used to connect a main document with attachments, notes, graphs, and other relevant information.

*IC Card:* An Integrated Circuit card contains integrated circuits on a silicon chip which functions as a micro-computer. Also known as chip cards or smart cards.

*Icor:* A graphical representation as part of a graphical user interface (GUI) that represents an application, document, or folder.

*Information Goods:* Information goods are pieces of digital information to be sold. Information goods can include stock quotes, songs, particular sections or chapters of literary works, multimedia content, and encyclopedia entries.

*Interface:* A connection between two points (e.g., a user and a computer, two computers, or hardware and software).

*Interoperability:* The ability of diverse software and hardware packages from different vendors to work together seamlessly.

*Intranet:* A privately constructed network that is not directly connected to the global Internet. Used for communications within an organization. Private networks can remain private by not using TCP/IP or by connecting to the Internet using firewalls.

*Internet:* A single, globally connected network that operates through layers of protocols. As used in common parlance, the Internet refers to the entire collection of e-mail, news groups, and the World Wide Web.

*ISP:* Internet Service Provider. An ISP provides individual users with access to the Internet.

*Issuer:* The bank or other financial institution identified on the cardholder's card. This bank issues the credit card to the customer and bears the risks and costs associated with billing, collection, and default.

*Key:* All encryption algorithms use keys, the value of which affects the functions of encryption and decryption. A key is literally a string of digits or letters and an associated process used to encrypt information.

*Key Pair:* A pair of keys used in the encryption process. In private or symmetric key encryption, both keys are the same and are kept secret. In public or asymmetric key encryption, one key of the key pair is public and widely distributed while the other is unique to the individual user.

*Layer:* The Internet is organized into layers, each with its own set of protocols for transmitting information. Applications, especially client/server applications, communicate through these delineated network layers. Each layer has a special function: the lowest layers relate to hardware and basic network transmission, while the highest layers relate to user services such as e-mail and application presentation.

*Link:* Hypertext connections between documents and information sites on the World Wide Web. For example, a link might potentially provide a connection from an individual stock quote to more detailed information about the company and its financial history.

*Magnetic Strip Card:* A card with a magnetic strip where signals are stored electromagnetically. An example is an "old-fashioned" credit card or ATM card.

*Memory Card:* An integrated circuit card lacking a microprocessor (and, hence, the ability to calculate), but which can store information.

*Merchant Server:* A computer performing an electronic commerce function for a merchant—such as storing and transmitting information goods and accepting payment for these goods or services.

*Micropayments:* Payments for microtransactions in very small amounts, typically less than one cent. Micropayment systems must be able to make verification inexpensive and must not involve complex cryptographic techniques.

*Microtransactions:* Transactions for information goods, the value of which is less than traditional cash denominations. Examples could include getting stock quotes, accessing songs or literary works, or consulting online encyclopedias.

*Modem:* A device designed to allow individual computers intermittent access to other computers and the Internet through the use of telephone lines. Modem is an abbreviation of modulator/demodulator.

*Multi-Application Card:* A card that supports more than one application, potentially provided by many commercial parties.

*Networked Digital Environment:* The entire environment including the Internet, private Intranets, the World Wide Web, and various forms of e-mail communications. This environment transmits information in digital form using particular protocols (rules).

*Non-repudiation:* A security property that indicates that the author of a message cannot disclaim authorship, for example to get out of a deal.

Digital signatures strive for non-repudiation in order to gain parity with comparable paper documents.

*One-Time Key:* A key used for encryption that can only be used for one transaction.

*Online:* Connected to, served by, or available through a computer or telecommunications system.

*Operating System:* The program that serves as the connection between the software (applications) and the hardware (the physical components of the computer).

*Packet:* Packets are network message fragments including the message fragment itself, a header with identifying information about the message fragment, error control data, and addressing data. As a message fragment travels along the network, each layer or gateway adds routing information to the packet before passing it to the next destination. Packets are not full messages; each message a user sends (for example, a typical e-mail communication) is broken up into packets and transmitted across the Internet via the best available routes.

*Packet Sniffing:* Stealing information from a network by collecting information from packets transmitted across various routes.

*Packet Switching:* Network technology that allows data to be transmitted in packets. Packets are routed from source to destination through the most cost- and speed-efficient routes, and message transmission does not rely on a stable and direct connection between source and destination.

*Pass Phrase:* A phrase that functions in the same way as a password.

*Payment Gateway:* A payment gateway computer is a bridge between the merchant and customer on the Internet and provides a connection to the existing card financial network, through which the issuer can be contacted to authorize the transaction.

*Payments Franchise:* The “payments franchise” refers to the traditional market dominance of banks and financial institutions in the fields of money transfer.

*PC/SC Workgroup:* Personal Computer/Smart Card Workgroup is an industry group formed to develop open technology for the integration of smart cards and personal computers. It plans to make smart card interfaces standard on low-cost workstations.

*PIN:* A Personal Identification Number is a secret code possessed by the customer for use in verifying identity. Commonly used for Automatic Teller Machines, calling cards, etc.

*Prepaid Card:* A card purchased with a set amount of stored value. As the user completes transactions, the value decreases accordingly. Also called a stored-value card.

*Protocol:* In the Internet context, protocols are basic rules regarding message format, for communications between network computers. In essence, a set of instructions for how computers should interact with each other over the

Internet. Protocols more generally can refer to rules for interaction between hardware and software, and users and applications.

*Public Key Encryption:* Also known as asymmetric encryption, each party has a key pair, and one key is made public while the other is kept private. Information encrypted with either component of the pair can be decrypted only with the other component. The advantage of public-key encryption is that the public key can be made available to everyone without compromising security while the private key is not distributed at all. Also provides ready mechanisms for key distribution, authentication, and authorization.

*Real Time Processing:* As opposed to batch processing, real time processing computes each transaction as it takes place.

*Route:* The path of network data from point of origin to point of destination. Several packets constituting the same message may follow different paths between sender and receiver.

*Server:* Servers are computers that provide services to other network entities such as client computers. Servers can also be sites for information storage such that clients can access data remotely without the expense of having to house the data themselves.

*SET:* A standard produced by Visa and MasterCard for processing credit card institutions and merchants on the Internet and the private banking networks.

*Settlement:* The process of completing a payment transaction in the sense that the customer receives the goods or services and the merchant receives payment. Also refers to the process in which banks settle accounts among themselves.

*Slippage:* Refers to the fact that in any prepayment system, consumers will let small amounts of cash expire without contacting the bank for reissue. In the aggregate, this could add up to a significant profit for the bank.

*Smart Cards:* Integrated circuit cards designed to make decisions.

*Socket Layer:* A data structure on the Internet that allows communication between programs. A socket works as a pipeline between communicating programs and is made up of an address and a port number.

*Software:* This term generally refers to computer programs. Software includes application programs that provide services to users. Common examples are home financial management software, word processors, and spreadsheets.

*Spent Coin Database:* A collection of data organizing digital coins that have been spent. The database should be easily accessible by merchants or banks wishing to check whether digital coins offered by customers are valid.

*SSL:* Secure Socket Layer (SSL) is a cryptographic protocol that is applied to data at the socket interface between communicating programs. Developed and patented by Netscape, SSL enables merchants' computers and customers' computers to agree on an encryption program such that credit card information can be sent securely. For example, SSL would be

used in a transaction where a user buys merchandise from an online store using his or her credit card. The transmission of the credit card between the user interface (the browser) and the store would be protected by SSL.

*Standard:* An agreement to a uniform and consistent method or specification. A standard is carefully designed to achieve a common result or action. Different programs can be developed to implement a common standard.

*Strong encryption:* Cryptography that exceeds the standards for lightweight or medium-strength cryptography and thereby faces many U.S. export restrictions.

*Symmetric or Secret Key Encryption:* Unlike public-key encryption, symmetric or secret-key cryptography uses the same key both to encrypt and decrypt data. The well-known DES algorithm is a form of secret-key encryption.

*TCP/IP:* A set of complex network protocols that connect the entire Internet. TCP (Transmission Control Protocol) organizes data into packets and effectuates packet delivery across the network (i.e., packets arrive in proper order and are not misrouted). TCP will retransmit data that does not reach its destination in proper form and insures a connection between a server and a client. IP (Internet Protocol) delivers TCP and UDP (User Datagram Protocol) packets across the Internet, and allows packets to be automatically routed through many networks if the sending and receiving hosts are not on the same network.

*Transmission:* Passing data between a client and a server or multiple host computers through a wired network or using wireless technology.

*Transport Layer:* The transport layer is Layer 4 in the TCP/IP network model and contains the TCP and UDP protocols.

*Trusted System:* A system that integrates payment and other aspects of commercial transactions including delivery of goods and specification of rights.

*URL:* A URL (Uniform Resource Locator) is the standard way to reference information on the World Wide Web. The "http://" in a Web address specifies the protocol for accessing the information, and the rest of the URL specifies the exact location.

*Wallet Software:* Software installed on the consumer's PC and used to store credit card information and/or digital cash, and to handle elements of payment transactions, identification transactions, and debit transactions.

*Web Site:* A location on the World Wide Web consisting of a set of HTML documents stored on a server (computer) and made available to access from other computers. A typical company Web site would describe products and services and would link the information together using hypertext pointers. Web sites can also be linked in this manner to other relevant Web sites.

*World Wide Web:* Literally, a huge hypertext document that uses HTTP and HTML. The Web allows information located on computers around the world to be accessed through browsers such as Netscape Navigator. The Web is accessed as a single multimedia document with links that can be

followed using simple point-and-click techniques. The architecture of the Web follows a client/server model, and enables users to access information that might be housed on computers spread out across the globe.