Florida Law Review

Volume 50 | Issue 2 Article 2

Cyberlaundering: The Risks, the Responses

Sarah N. Welling

Andy G. Rickman

CYBERLAUNDERING: THE RISKS, THE RESPONSES

Sarah N. Welling[*]
Andy G. Rickman[**]

---

* Professor Welling is the Wendell H. Ford Professor of Law at the University of Kentucky. B.A., 1974, University of Wisconsin; J.D., 1978, University of Kentucky.

This article grows out of Professor Welling's experience as a group leader at the money laundering operational exercise at the RAND Corp. in June 1997. Professor Welling thanks the Financial Crimes Enforcement Network (FinCEN) and RAND for inviting her to participate in the exercise. The exercises are described in Ann Davis, Concerns Rise on Laundering Money On-Line, WALL ST. J., Mar. 17, 1997, *available in* 1997 WL-WSJ 2413155.

** Mr. Rickman is a law clerk for the Honorable Joseph M. Hood, United States District Court for the Eastern District of Kentucky. In 1999-2000, Mr. Rickman will be clerking for Judge Ronald Lee Gilman, U.S. Court of Appeals for the Sixth Circuit.

Mr. Rickman attended money laundering exercises sponsored by RAND and FinCEN at the RAND Corp. in Washington, D.C. on April 17, 1997.

> Technology permits us wonderful new opportunities, but it can also be misused just as creatively to threaten public safety and national security. The public is beginning to understand that information technology, like other human creations is not an unqualified good. . . . I consider high-tech crime to be one of the most serious issues that I face in the Department and one of those that demands much of my attention.
>
> Janet Reno[1]

INTRODUCTION

In the year 2003, Lucky Marciano, head of the Marcianocrime organization, sits at home in front of his personal computer. Lucky is laundering millions of illegally earned profits through the Internet with electronic cash.[2] Several months earlier, police raided the house of Joey Golliti, who runs Lucky's drug operations. They found two kilos of cocaine and $5 million of electronic cash stored on Joey's computer.[3]

In 2004, Lucky's money laundering operation takes another hit. Police arrest six of Lucky's people for trafficking and discover several hundred large denomination "smart cards" in their luggage.[4] These are forfeited. On the other hand, Lucky has been successful laundering money via cellular telephones. Lucky calls his accomplices in Europe and swipes his smart card across the cell phone, instantly sending electronic cash to Europe.[5]

In 2005, Lucky's drug sales via electronic cash increase 250% because welfare recipients start using their government-issued smart cards to buy drugs.

With advances in electronic commerce, this hypothetical could be reality soon. This Article discusses the potential use of electronic cash

---

1. Janet Reno, United States Attorney General, Law Enforcement in Cyberspace, an Address presented to the Commonwealth Club of California (June 14, 1996) (on file with author) [hereinafter Reno Address].

2. For some of the ideas and hypotheticals in this Article, the authors thank RAND Corporation and the Financial Crimes Enforcement Network (FinCEN), an office in the Treasury Department, for inviting us to participate in their simulation and operational exercises in Washington, D.C. We cite the conference as *Cyberpayment Systems Exercise* (Apr. 17, 1997), which refers to the discussions and informational sessions that we attended. We also cite the conference workbook as *Cyberpayment Systems Exercise Workbook.* The workbook is on file with the authors.

3. *See Cyberpayment Systems Exercise Workbook, supra* note 2, at E-3.

4. *See id.*

5. *See id.*; *Cyberpayment Systems Exercise, supra* note 2 (discussing cell-phone technology and the phones' interoperability with electronic payment systems).

for money laundering and possible government responses to the problem. Parts I and II provide an overview of electronic cash. Part III explores the effects that electronic cash can have on money laundering. Part IV explains through a series of hypotheticals how "cyberlaundering" can occur. Part V analyzes the federal government's response to the threat of money laundering with electronic cash. Part VI concludes the Article with suggestions.

I. OVERVIEW OF ELECTRONIC CASH

In the late 1960s, the United States Department of Defense formed what we now call the Internet.[6] The Internet is an infrastructure composed of thousands of computer networks linked together through common routers.[7] An estimated forty million people are linked to the Internet worldwide, and that number is growing rapidly.[8] With a connection to the Internet, people can buy and sell goods and services. Projections for electronic commerce on the Internet in the year 2000 indicate it will be approximately $255 billion in the United States.[9] The

---

6. *See* Peter E. Dyson, *The Seybold Report on Desktop Publishing*, Apr. 4, 1994, *available in* 1994 WL 13596797.

7. *See id.*; *see also* Financial Crimes Enforcement Network, U.S. Dep't of the Treasury, *Exploring the World of Cyberpayments: An Introductory Survey* app. I (1995) [hereinafter *Exploring the World of Cyberpayments*] ("Security Section").

Two sets of frequently seen initials on the Internet, WWW and html, developed as follows:

> The World Wide Web (WWW), developed at CERN (the European nuclear research center), is a system of cross-linked hypertext databases that are distributed widely across the Net. Documents in the Web are prepared in the Hypertext Markup Language (html), which is an sgml-compliant document type that supports non-textual data.

Dyson, *supra* note 6.

8. *See* Ted Bridis, *Internet Traffic Is Doubling Every 100 Days*, LEXINGTON HERALD LEADER, April 16, 1998, at D2; *Exploring the World of Cyberpayments*, *supra* note 7, app. II, at 1. The Internet has more people than 49 American states and 7 of the European Union's 12 members. *See Net Profits*, THE ECONOMIST, July 9, 1994, *available in* 1994 WL 12754212; *International Body Addresses New Issues in Laundering*, REPORT ON SMART CARDS, Mar. 17, 1997, *available in* 1997 WL 8987484 ("there are an estimated 12.8 million host locations and 61.9 million users who generate more than a billion e-mail messages per month").

9. *See* Diane Francis, *Banks Might Be the Casualties in Move to Electronic Money*, FIN. POST, Feb. 11, 1997, *available in* 1997 WL 4087183; *Exploring the World of Cyberpayments*, *supra* note 7, app. II, at 2 (noting that a conservative projection for Internet commerce is $10 billion).

commercial opportunities are causing new retail payment systems to develop.[10]

One new form of retail payment system is electronic cash.[11] Electronic cash is a claim on a party, usually the issuer, stored as a computer code on a plastic card or on the hard drive of a personal computer.[12] Electronic cash is basically a little speck of value in digital form that a computer can read. Just as traditional currency is not value itself but merely represents value, so the digital speck represents value.[13] Electronic cash is issued and sold by private companies. The electronic cash can be sent over open information systems like the Internet[14] or encoded on a plastic card. Consumers use traditional money to buy the electronic cash from the issuing company, and then use it to buy goods and services from merchants who accept electronic cash as payment.[15] Electronic cash is also called e-cash, digital cash, digital money, and cyberpayments.[16] Electronic cash can be used in three ways: on stored value cards, on personal computers, and in hybrid systems.[17]

This description of electronic cash assumes that it is stored value, or in other words, is in "tokenized" form. Electronic cash usually falls into

---

10. *See* Sarah J. Hughes, *A Call for International Legal Standards for Emerging Retail Electronic Payment Systems*, 15 ANN. REV. BANK. L. 197, 207 (1996).

11. *See* U.S. DEP'T OF THE TREASURY, TOWARD ELECTRONIC MONEY AND BANKING: THE ROLE OF GOVERNMENT 5 (Sept. 19, 1996) [hereinafter TOWARD ELECTRONIC MONEY]. *See generally* Symposium, *The Electronic Future of Cash*, 46 AM. U. L. REV. 961-1335 (1997).

12. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 5. Value can be stored in personal computers and moved electronically from one computer to another with no face-to-face interaction. *See id.* DigiCash and Cybercash are systems designed to facilitate electronic commerce on the Internet. *See Exploring the World of Cyberpayments*, *supra* note 7, at 9.

13. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 5. One commentator stated that "SVCs and e-cash are today merely symbols of paper currencies, which are themselves merely symbols of value." *"It Will Change the World,"* REPORT ON SMART CARDS, May 20, 1996, *available in* 1996 WL 15841975.

14. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 3. For example, two companies are developing a hybrid system that will allow electronic cash to be moved from a smart card to the hard drive of a computer and vice-versa. *See* FATF SECRETARIATE, FATF-VIII MONEY LAUNDERING TYPOLOGIES EXERCISE PUBLIC REPORT, Feb. 5, 1997, at 15 [hereinafter FATF REPORT].

15. *See* TOWARD ELECTRONIC MONEY, *supra* note 14, at 5.

16. *See Exploring the World of Cyberpayments*, *supra* note 7, at 1.

17. *See* FATF REPORT, *supra* note 14, at 15-16. Two variations of electronic cash have emerged that descriptively are called "net-around money" and "walk-around money." "Net-around money" involves personal computers and is used for on-line purchases. DigiCash's digital coins are an example of "net around money." "Walk-around money" primarily is used in face-to-face transactions. Mondex cards are an example of "walk-around money." *See* Hughes, *supra* note 10, at 213.

two basic categories, notational or tokenized.[18] Notational systems are account-based and use conventional financial institutions.[19] These systems leave an audit trail and can be integrated into the current payment infrastructure.[20] On the other hand, tokenized systems take full advantage of the Internet and the advancements in technology.[21] Tokenized systems may work outside the traditional banking infrastructure.[22]

To understand the revolutionary character of tokenized electronic cash, it can be conceptualized as a second currency system. The little digital symbol sent over the Internet or encoded on a plastic card and transferred by swiping the card is not just a right to get money from a bank or from a credit card company. Rather, the digital speck is value itself. Like cash, whoever holds the digital speck holds the value, and can redeem it in other forms from the company that issued it. It is as if a $50 bill is sent through the Internet. Checks, credit cards and debit cards are only payment systems, whereas electronic cash can fulfill both roles of traditional cash—as a payment system and as a stored-value system.[23] Throughout this Article, the discussion of electronic cash assumes it is in tokenized form.

Several conditions drive the move to electronic cash. One is advances in communications technology[24] and decreases in costs. Moreover, economies of scale make electronic money attractive.[25] The point of a payment system is to allow efficient use of money. Traditional retail payment systems other than cash,[26] checks, debit cards, and credit cards,[27] are all account based. They require an elaborate

---

18. *See* Russell B. Stevenson, Jr., *Internet Payment Systems and the Cybercash Approach*, 452 PLI/PAT. 123, 125 (1996).

19. *See id.* at 138.

20. *See id.*

21. *See id.*

22. *See id.* at 125-26.

23. *See* Francis, *supra* note 9.

24. *See* OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, INFORMATION TECHNOLOGIES FOR THE CONTROL OF MONEY LAUNDERING 130 (1995) [hereinafter INFORMATION TECHNOLOGIES]; Benjamin Wittes, *The Dark Side of Digital Cash*, LEGAL TIMES, Jan. 30, 1995, at 1 (consumers now can make purchases over the Internet with digital cash); *see also* Hughes, *supra* note 10, at 206 (noting that both bank and nonbank service providers have developed new payment options, including the nonbank service providers, First Virtual Holdings, Inc. and DigiCash BV).

25. *See Exploring the World of Cyberpayments*, *supra* note 7, at 8.

26. *See id.* Debit cards and credit cards account for less than 10% of all retail transactions, whereas cash is used in almost 80% of all retail transactions. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 30-31.

27. *See Exploring the World of Cyberpayments*, *supra* note 7, at 5. *See also* TOWARD ELECTRONIC MONEY, *supra* note 11, at 30-31 (debit cards are the biggest form of electronic

superstructure to support them. This is expensive. They are also slow because they require a bank or credit card company to clear every transaction.[28] Account based systems can be inefficient when used with high volume, low value goods.[29] Businesses are looking for more efficient retail payment systems to take advantage of the Internet's ability to handle such high volume, low value goods.[30]

Electronic cash could fill that niche, revolutionize the consumer market and eventually make traditional cash obsolete.[31] Companies like Visa and Microsoft are developing electronic cash systems that will give consumers adequate security[32] and will allow financial transac-

---

money whereas credit cards are the most popular payment form); *E-Money Laundering Gets State Department Attention*, REPORT ON SMART CARDS, Mar. 17, 1997, *available in* 1997 WL 8987476 (noting that already in design or use are cyberchecks, cybercredit, and cyberdebit with the common feature being convenient and potentially anonymous transfers); *see generally* Catherine Trevison, *3 Plead Guilty to Laundering Escort Money*, THE TENNESSEAN, Mar. 18, 1997, *available in* 1997 WL 10091991 (involving a case where pimps were accepting credit card payments for their prostitutes' services and calling the credit card companies to verify their clients' credit).

28. *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 456 (1996). Debit cards, however, do leave an audit trail for law enforcement. *See id.* at 457.

29. *See id.*

30. One example of the Internet's use of high-volume, low-value goods is the "micropayment" concept. *See Cybercash Bundling Mondex in Wallet*, REPORT ON SMART CARDS, Oct. 7, 1996, *available in* 1996 WL 15842147. With "micropayments," an information provider could be paid a small amount anytime someone "clicked" on his piece of data. This would give information providers some royalties for their work product. *See* Jared Sandberg, *Cybercash Lowers Barriers to Small Transactions at Internet*, WALL ST. J., Sept. 30, 1996, *available in* 1996 WL-WSJ 1180036 (describing a developing "microtransaction" system). However, credit and debit cards could never work in a micropayment system due to the length of time it would take to clear every transaction. *See id.*; *see also Analysts' New Study Predicts Explosion in Use of E-Money*, REPORT ON SMART CARDS, Feb. 3, 1997, *available in* 1997 WL 8987424 (noting that consumers will not use their credit cards for purchases less than ten dollars).

31. *See* Wittes, *supra* note 24; A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 114 (1996) (the dollar value of electronic commerce could grow rapidly). Another view, however, is that the complete displacement of cash is not likely because around 18 billion currency notes valued at $400 billion are in circulation all over the world. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 17 (one of the most important issues facing people who are substantially affected by financial services is the development of electronic money and electronic payment systems for retail transactions). Around 270 billion dollars of U.S. currency is in circulation outside of the United States. *But see Exploring the World of Cyberpayments*, *supra* note 7, at 6 n.2 (only one-third of all U.S. currency in circulation is domestically held, and thus, it is unlikely that traditional cash would become obsolete in the near future). In some less technologically advanced countries, U.S. currency is the principal form of payment. *See id.* In those places, electronic money is many years away. *See id.*

32. *See* Wittes, *supra* note 24. The following is an interesting account of what can happen with inadequate security. *See* David Gow & Richard Norton-Taylor, *Surfing Superhighwaymen Banks Have Good Reason to Fear Thieves Who Hack into Their Secret Files*, THE GUARDIAN

tions on the Internet.[33] If acceptance of electronic money is analogous to the acceptance of automated teller machines and credit cards, growth will be confined to a small base of users for the first five years and then will expand tremendously.[34]

Electronic cash can be used three ways.

(City Page), Dec. 7, 1996, *available in* 1996 WL 13391656.

One day Roberto Barbosa, director of an Argentinean firm, Invest Capital, stared with dismay and shock at his computer screen after noticing that $200,000 had vanished from his company's account with Citibank. Barbosa stated that, "[w]e were very, very surprised when we opened the cash management account. There were four wire transfers made out of that account without our authorization and anonymously sent to four unknown destinations." *Id.* Shortly after the discovery, Barbosa contacted Citibank executives on Wall Street in New York City.

However, Citibank had more problems than just Barbosa's account because almost 20 of Citibank's accounts, worth around $10 million, were being robbed. The top executives of Citibank gathered on Wall Street to watch helplessly as their clients' funds rapidly were being transferred to accounts in "California, Latin America, Finland, Israel, and the Netherlands." Citibank had become the world's worst victim of "cyberspace" theft.

Citibank, in conjunction with the FBI, obtained evidence that led them to believe that the mastermind behind the thefts was Vladimir Levin. Levin, who is 29 years old, is a computer programmer from St. Petersburg, Russia, and is accused of carrying out the multi-million dollar theft on a laptop computer at the St. Petersburg offices of AO Saturn.

What chain of events led Levin, a struggling computer programmer in Russia, to break into the world's fifth largest bank and become the first person ever to penetrate the supposedly unbreakable electronic payment systems that transfer trillions of dollars each day all over the globe? One explanation is that about a year before Levin's theft, a computer and mathematical genius who goes by the name Megazoid, broke into Citibank's files using only a "computer and modem he bought for $10 and a bottle of vodka." One of Megazoid's accomplices in the crime, a brilliant computer hacker who often was depressed, got drunk and sold the complex and detailed secrets of how to "break into Citibank for $100 and two bottles of vodka." The buyers are thought to be associated with the Russian mafia and used AO Saturn and Levin to carry out their scheme. *See id.*

For related articles, see Joseph L. McCarthy, *Cyberswindle!*, CHIEF EXECUTIVE (U.S.), May 1, 1996, *available in* 1996 WL 9565177; *Citicorp Suffers First "Cyberheist" as Regulators Show Concern*, MONEY LAUNDERING ALERT, Oct. 1, 1995, *available in* 1995 WL 8353546; *Computer Hacker Pleads Guilty to Fraud in Citicorp Theft Case*, WALL ST. J., Jan. 5, 1996, *available in* 1996 WL-WSJ 3085681.

In addition to Levin and his accomplices, some London banks paid a multi-million dollar ransom to criminal hackers who pierced their computer security systems and threatened to launch "logic bombs," which paralyze the system, into the banks' computer systems. *See* Graeme Browning, *Cybercops and Robbers*, NAT'L J., Mar. 22, 1997, *available in* 1997 WL 7228268.

33. *See* Wittes, *supra* note 24; *Analysts' New Study Predicts Explosion in Use of E-Money*, supra note 30 (Visa International, MasterCard International, and American Express are incorporating smart card technology into their existing systems). *See also So Much for the Cashless Society*, THE ECONOMIST, Nov. 26, 1994, *available in* 1994 WL 12754268 (describing the recent growth and interest in developing money for Internet users).

34. *See* TOWARD ELECTRONIC MONEY, *supra* note 11; Francis, *supra* note 9 (stating that in year 2000 electronic commerce will approach $255 million and that 30% of bank profits will come from personal banking done on the Internet).

A. *Stored Value Cards*

Stored value cards (SVCs) are the physical cards that contain the electronic cash.[35] SVCs are also called prepaid cards and value-added cards.[36] The familiar credit cards and debit cards have magnetic strips that store information. SV's, in contrast, can store value and process information.[37] Technologically, the most feasible structure for SVC's is to have a computer microchip embedded on the card.[38] So equipped, SVC's are called smart cards.[39] Microchip-based electronic cash is expanding, and in the future, smart cards will likely play a big role in domestic and worldwide markets as well as payment systems.[40] Stored

---

35. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 5.

36. *See* Gregory E. Maggs, *New Payment Devices and General Principles of Payment Law*, 72 NOTRE DAME L. REV. 753, 756 (1997). Copy cards are an example of stored value cards.

> Patrons may use the card to make photocopies. For every copy made, a card reader reduces the code on the card by the cost of making a copy (typically about ten cents). Patrons may increase the value of the card by inserting the card and additional cash into a machine.

Id. at 756-57.

37. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 5; Maggs, *supra* note 36, at 756 ("[t]hese cards use a magnetic strip or a microchip to hold an encoded number representing a sum of money").

38. Stored value cards can use either magnetic, optical, or chip technology. *See* FATF REPORT, *supra* note 14, at 21. However, due to limited security, magnetic and optical cards are not feasible alternatives for electronic money. *See id.* On the other hand, the microchip provides security and is portable, and thus, a much better substitute for physical currency. *See id.* (noting that magnetic strip cards are more susceptible to fraud than "smart cards" using microchips).

One of the most revolutionary aspects of smart cards is their multifunction capability. *See "It Will Change the World," supra* note 13. Like most of the world's information, money is starting to become electronic and digital; therefore, information may be placed and stored on the cash itself. *Id.* When electronic money is programmed for specific uses and purchases, it is called "paramoney." Dr. Alvin Toffler gives the following examples to illustrate paramoney:

> A parent can give a child a smart card that can be used to purchase lunch—but not dessert or cigarettes. If the child tries to purchase the latter, the transaction is blocked by technology embedded in the card's chip. Similarly, the government can issue a card to the poor to authorize purchases of milk and bread, but block purchases of alcohol or candy.

Id. The government would likely find paramoney useful because the government could give welfare recipients a smart card which limits purchases to certain items.

39. We use the terms interchangeably.

40. *See E-Money Laundering Gets State Department Attention, supra* note 27. *See also Going for Olympic Gold Cards*, THE ECONOMIST, Mar. 30, 1996, *available in* 1996 WL 8671578 (banks all over the world are starting to use smart cards).

value cards are versatile because they "can take many forms, from disposable, anonymous, single-use phone cards, to multi-function, reloadable cards with systems that can track unspent values for every card."[41] Stored value cards can be described as part of a closed system or an open one.[42]

1. Closed System

A system that has only a few merchants or that has many merchants in a small geographic area is considered a closed system.[43] One variation of the closed system, the merchant-issuer model, exists where the card issuer and the merchant are the same.[44] Examples of the merchant-issuer model are the subway system in Washington, D.C. and university or campus cards that allow students to purchase goods and services from the university.[45]

The Washington, D.C. subway is a good example of how electronic cash works in a closed environment. If a consumer wants to ride the subway, she puts some traditional money in a metro machine. The machine then will give her back a card with the equivalent dollar value for use on the subway. At this point, the consumer has purchased a claim on the city and has received electronic cash in return.[46] This is the merchant-issuer model because the city is both the issuer of the metro card and the merchant. Once the consumer has the card, she can use the subway.[47] Every time she uses the subway a point-of-sale machine records the transaction and reduces the value of the electronic cash recorded on the metro card.[48] The Washington, D.C. metro system is linked to the traditional payment system by the city's relationship with its bank.[49] Periodically, the city clears out its machines by taking all the cash that has been exchanged for electronic money and putting it in the bank.

---

41. *Waiting for a Smart World*, SMART CARD BULL., Feb. 1, 1995, *available in* 1995 WL 14481050.

42. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 5-8 (the most effective way to distinguish among electronic payment systems is to concentrate on the issuing entity and whether the systems operate in an open or closed environment).

43. *See id.* at 5-6.

44. *See id.* at 6.

45. *See id.*; *see also* Maggs, *supra* note 36, at 757 (the Washington, D.C. metro and the San Francisco subway are users of SVCs).

46. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 6.

47. *See id.*; *see also* Maggs, *supra* note 36, at 757 (stating that SVCs are more convenient for consumers than having to carry around a pocketful of coins).

48. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 6.

49. *See id.*

2. Open System

On the other hand, a system where consumers can use their smart cards at many businesses over a wide geographical area would is an open system.[50] Open system SVCs exist in Europe, the Far East, and the United States.[51] The basic framework for an open system starts with a consumer exchanging traditional money for electronic cash at an issuing company.[52] The consumer then takes the electronic cash and exchanges it for goods and services at a participating merchant. The merchant takes the electronic cash and exchanges it for traditional money at the merchant's bank. The merchant's bank sends the electronic money to a clearinghouse, which deals with interbank fund transfers, and receives an interbank balance. The clearinghouse then sends the electronic cash to the issuing bank and receives back an interbank balance.[53]

An example of how an open system might work is the following:[54] Consumer goes to Bank First and exchanges $1000 of traditional cash for $1000 of Bank First's electronic cash on a smart card. Consumer then goes to Wal-Mart[55] and purchases $500 of groceries, paying for them with the smart card. At the end of the day, Wal-Mart accesses its account at Bank Second via a computer and electronically sends Consumer's electronic cash into its account. Bank Second credits Wal-Mart's account and sends the electronic cash to Big Clearinghouse and receives an interbank balance.

Ultimately, all smart card systems can be characterized as closed systems because they all depend on some set of merchants agreeing to accept the electronic cash as value. The distinction between open and closed systems is not sharp, but it is a distinction being made,[56] and it is helpful in describing the systems.

---

50. *See id.* at 8. An open system includes many businesses over a large geographic area, and so is more attractive to money launderers than a closed system because the laundering is harder for law enforcement to detect. See id. Using the subway example, the electronic cash only could be used to ride the subway in Washington, D.C., and thus, its laundering potential is very limited.

51. *See id.*

52. *See id.* at 9.

53. *See id.*

54. *See id.*

55. Assume Wal-Mart is a participating merchant.

56. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 5-8 (most effective way to distinguish among electronic payment systems is to concentrate on the issuing entity and whether the systems operate in an open or closed environment).

B. *Personal Computers*

Electronic cash can be put on the hard drive of a personal computer as well as on a SVC. Consumers can use the digital money to purchase items over the Internet.[57] These network-based systems give the user global access.[58] DigiCash is an example of a network-based system.[59] Consumers using DigiCash must establish an account at a bank.[60] The consumers then download the money from their bank accounts to an electronic wallet in their computer.[61] Consumers can then purchase products over the Internet using their electronic cash.[62] Internet merchants can exchange the electronic cash for value at traditional banks.[63]

C. *Hybrid Systems*

When SVCs and network-based computer systems work together, they are called hybrid systems.[64] Stored value cards and network-based systems are becoming more compatible with each other,[65] or interoperable.[66] Developers of electronic cash are building smart card interfaces for personal computers that will allow value to be moved back and forth between smart cards and personal computers in seconds.[67] This interrelationship makes it difficult to put them in distinct categories.[68]

Experts in electronic payment systems are projecting that all computers will have built-in chip-card interfaces.[69] In other words, computers will have a smart card reader built in. Consumers then can

---

57. *See id.* at 12.

58. *See* FATF REPORT, *supra* note 14, app., at 30.

59. *See* INFORMATION TECHNOLOGIES, *supra* note 24, at 130-32.

60. *See* Hughes, *supra* note 10, at 210.

61. *See id.*

62. *See id.* at 210-11.

63. *See id.* at 211. Banks would have to recognize or have an agreement with DigiCash before they could accept DigiCash's coins.

64. *See* FATF REPORT, *supra* note 14, at 15.

65. *See id.*

66. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 21-22 (explaining the need for "interoperable" systems).

67. *See* FATF REPORT, *supra* note 14, at 15. Chip-card interfaces are devices that function as miniature ATM machines and are built-in to the consumers' personal computers.

68. *See Exploring the World of Cyberpayments, supra* note 7, at 8-10 (analyzing the differences and similarities between systems). It should be emphasized that "[t]he possible points of contact between PC-based electronic cash and the traditional payment system are functionally identical to those between SVCs and the payment system." TOWARD ELECTRONIC MONEY, *supra* note 11, at 12-13.

69. *See Cyberpayment Systems Exercise, supra* note 2.

do their banking at home by having electronic money sent from the bank's main computer to the consumers' personal computer hard drives. On receiving the electronic cash from the bank, the consumer can purchase items directly from the Internet or swipe a smart card across the computer interface, downloading the electronic money from the hard drive to the smart card. Then, the consumer could take the smart card to the grocery and buy bread and coffee.

II. A BRIEF LOOK AT ELECTRONIC CASH SYSTEMS WORLDWIDE

Electronic payment systems are growing worldwide. In Great Britain, the Mondex system is popular.[70] Mondex is a smart card system that allows consumers to transfer electronic cash to their Mondex cards from their bank accounts using a Mondex-compatible phone or an ATM.[71] The Mondex card holds up to five different currencies per card,[72] and the consumer and merchant do not need signatures or authorizations to complete a transaction.[73] A security code prevents the electronic cash stored on the computer chip from being misused.[74] Consumers can make a payment by inserting their Mondex cards into a merchant's Mondex terminal or into another individual's electronic purse.[75] Therefore, electronic cash users can transfer value among themselves without any intermediaries, i.e., without the issuer or any other financial institution being involved in the transaction. These value transfers directly between users, without any financial institution or electronic cash issuer as intermediary, are called peer-to-peer transfers.[76] Users can trace their previous ten transactions, but the Mondex system does not track all transactions.[77] A typical transaction report from the

---

70. *See* Froomkin, *supra* note 28, at 468. The Mondex system is a product of a joint venture between NatWest and Midland Bank. *See id.* MasterCard International, Inc. recently has acquired Mondex. *See Mondex Becomes MasterCard Subsidiary*, REPORT ON SMART CARDS, Mar. 3, 1997, *available in* 1997 WL 8987462. Mondex will become a subsidiary of MasterCard and will have access to MasterCard's vast resources and distribution networks but will keep its board of directors and London headquarters. *See id.*

71. *See Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 1-2. Mondex and CyberCash have worked out an alliance where consumers now can use Mondex's smart cards to purchase goods on-line via CyberCash's wallet. *See CyberCash Bundling Mondex in Wallet*, *supra* note 30.

72. *See Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 2.

73. *See id.* at 1.

74. *See id.* at 2.

75. *See id.*

76. *See* Froomkin, *supra* note 28, at 468 (no bank intervention is necessary in peer-to-peer transactions).

77. *See Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 2. The Mondex system has a risk management system in place that can detect potential misuse. For instance, the

Mondex system provides the amount of the transaction and whether the transaction was person to person or person to merchant.[78] The report does not reveal the identity of the person or merchant involved in the transaction.[79]

An interesting aspect of the Mondex system is that it can actually increase the money supply.[80] For instance, if Consumer places $100 in her checking account, the bank can use Consumer's money. Consumer has a claim on the bank for $100, but Consumer does not have use of the money until she purchases something and it clears the bank. However, under the Mondex system, if Consumer gives Mondex $100 in traditional money, Mondex will give Consumer a smart card that will have $100 of electronic cash on it. Consumer has access to $100 of electronic cash, and Mondex has access to $100 of traditional cash. If Consumer buys something with her Mondex card, the merchant might not redeem Consumer's electronic money from Mondex. Instead, the merchant might use Consumer's electronic money in another electronic transaction. Thus, the money supply increases until Mondex redeems the electronic cash.[81] The difference between Mondex and other payment options, such as checking accounts and travelers' checks, is that Mondex urges its users to refrain from redeeming their cards.[82]

The Mondex system is expanding to several Asian countries.[83] Likewise, Royal Bank of Canada and Canadian Imperial Bank of Commerce, Canada's two largest banks, have joined forces with Mondex to start a smart-card system.[84]

France is the single largest European user of smart cards, with more than twenty million in circulation.[85] In France and other parts of Europe, they store medical records on smart health cards.[86]

In Denmark, a company called Danmont has designed a smart card system that is used with pay phones, newspapers, parking meters, public

---

Mondex system has certain threshold levels for typical use. When a person goes beyond the typical boundaries, the system will flag that person for further examination. *See Growing Awareness of Stored-Value Concept Prompts Security, Policy Concerns*, REPORT ON SMART CARDS, July 29, 1996, *available in* 1996 WL 15842064.

78. *See Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 2 n.2.

79. *See id.*

80. *See* Froomkin, *supra* note 28, at 470.

81. *See id.* at 470-71.

82. *See id.* at 470; *see also So Much for the Cashless Society*, *supra* note 33 (people usually want cash to take a physical form and this might hurt electronic cash).

83. *See Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 2.

84. *See id.* at 8.

85. *See id.* at 2.

86. *See id.* app. I (Smart Card Exhibit).

transportation, vending machines, laundry, and cafeterias.[87] The system is based on consumer convenience and is designed to replace coins and to make high-volume, low-value transactions more efficient.[88] The Danmont system uses disposable chip-cards.[89]

In Belgium, a manufacturer has developed a micro-processed smart card called the Proton Smart Card.[90] It can be used with telephones, vending machines, parking meters, mass transit, taxis, cinemas, and pharmacies.[91]

Portugal is the first country to issue a global smart card that can be perpetually reloaded.[92] It designed the smart card to be used with ATMs.[93] Holders of these smart cards can access up to twenty-six services, from booking train tickets and paying utility bills to creating investment portfolios and paying taxes.[94]

South American electronic payment systems are expected to expand very quickly. The infrastructure in Latin American countries will not have to be overhauled for the new systems because checks, credit cards and debit cards have not replaced cash there to the extent they have in the U.S.[95] Visa International and MasterCard International are preparing some smart card tests in Brazil, Mexico, Argentina, and Colombia.[96]

In the United States, most smart cards are used in a few closed systems.[97] However, businesses are spending billions of dollars developing these systems.[98] For instance, Wells Fargo Bank started a Mondex system pilot program in San Francisco.[99] The maximum limit

---

87. *See id.* app. III, at 3.

88. *See id.*

89. *See id.*

90. *See Proton Roll-Out in Belgium*, SMART CARD BULL., Mar. 1, 1995, *available in* 1995 WL 14481052; *Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 3.

91. *See Proton Roll-Out in Belgium*, *supra* note 90; *Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 3-4.

92. *See Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 4.

93. *See id.* at 4-5.

94. *See id.* at 5. This is a good example of an open system.

95. *See id.* at 7.

96. *See id.*

97. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 6; *cf. Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 7 (noting that in Japan and Germany almost 90% of all banking transactions are performed on-line).

98. *See* TOWARD ELECTRONIC MONEY, *supra* note 11.

99. *See Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 8; *Mondex USA Approved for Take-Off*, REPORT ON SMART CARDS, Dec. 16, 1996, *available in* 1996 WL 15842131 (noting that Wells Fargo will own 30%, Chase Manhattan Corp. 20%, AT&T Corp. 10%, MasterCard International, Inc. 10%, Dean Witter Discover 10%, First Chicago NBD 10%, and Michigan National Bank 10%).

on Mondex cards in the United States will be $1000.[100]

Citicorp is also developing an electronic cash system called the Electronic Monetary System (EMS).[101] EMS works on a computer network and will allow safe, instantaneous transactions.[102] EMS cards are used with a consumer's personal computer by inserting the card into a computer interface.[103] One advantage over Mondex is that Citicorp can track the cash it is issuing whereas Mondex cannot.[104] Besides Citibank, the owner of the East Coast's MAC automated teller network is joining with some Delaware banks to launch a pilot program that will place smart card chips in ATM cards.[105]

Other examples of smart card use in the United States are VISA International's experiment during the 1996 Olympic Games in Atlanta and the Jacksonville Jaguars stadium card.[106] Likewise, the New York Metropolitan Transportation Authority is moving towards smart card technology for New York's subway system to increase efficiency and lower costs.[107]

Enigma Logic has developed a smart card called the DES Gold Card.[108] This is a "supersmart" card "because unlike other microprocessor-equipped smart cards, this one doesn't have to be attached to a

---

100. *See Mondex USA Approved for Take-Off*, *supra* note 99.

101. *See Digitising Dollars*, THE ECONOMIST, Mar. 30, 1996, *available in* 1996 WL 8671580.

102. *See id.*

103. *See id.* This would be an example of a hybrid system.

104. *See id.*

105. *See Exploring the World of Cyberpayments*, *supra* note 7, app. III, at 7.

106. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 6, 14. Smart cards only have had limited use in the United States. *See id.* at 14. However, the Jacksonville Jaguar stadium card came out in 1995. The following describes its application:

> [O]ne bank issued cards that fans could use at the stadium to buy food, drink, and souvenirs at football games. The transactions with these stored value cards work much the same as with the merchant-issuer. The special POS [point of sale] devices record the transaction for the merchant, altering the purchaser's stored value card to reflect the decreased value. The merchant later presents the electronic cash to the bank-issuer by downloading the payment information from the POS, receiving traditional funds in exchange, typically in the form of a deposit balance at the bank. The merchant's bank would then send the electronic cash through the traditional payment system in much the same manner as presenting a check.

Id. at 6.

107. *See Testimony Before Congress: The Future of Money*, REPORT ON SMART CARDS, Mar. 25, 1996, *available in* 1996 WL 15842063.

108. *See Citibank Tightens Security on External System Access*, EFT REP., Jan. 17, 1996, *available in* 1996 WL 7063523.

card reader. It has its own key pad and window display for data entry."[109]

III. "CYBERLAUNDERING"

> "Electronic money laundering will boom, traditional paths are already highly supervised."
>
> Dr. James Backhouse[110]

Electronic cash shows promise as an efficient system for money laundering.[111] Using phony businesses to launder money may already be unnecessary;[112] the current trend is to launder money through the Internet.[113] Using the Internet and stored value cards to turn illegally obtained money into clean, untraceable funds is called "cyberlaundering."[114] One government office working to squelch such laundering is the Financial Crimes Enforcement Network (FinCEN), part of the Treasury Department. FinCEN oversees and enforces laws against money laundering, including the reporting laws of the Bank Secrecy Act (BSA). FinCEN believes that the biggest potential money laundering problems are the developments in technology and electronic payment systems.[115] Kenneth Rijock, a convicted money launderer and former banking attorney, stated that money launderers and drug traffickers are becoming computer experts in response to advancements in technology.[116] Laundering money through the Internet may already

---

109. *Id.*

110. Dan Atkinson, *Organized Crime Finds Hiding Place for Loot on Internet*, THE GUARDIAN (City Page), Apr. 24, 1996, *available in* 1996 WL 4021421 (quoting Dr. James Backhouse of the London School of Economics).

111. *See* INFORMATION TECHNOLOGIES, *supra* note 24, at 130-32; Wittes, *supra* note 24, at 1 (discussing potential problems that law enforcement may have in detecting digital cash schemes); *Internet Aids Money Laundering Fraud Expert*, REUTER BUS. REP., June 9, 1995, *available in* LEXIS, Nexis Library, Wires File (finding that the Internet has made it possible for money laundering to become a worldwide $300 billion-a-year activity); FATF REPORT, *supra* note 14, at 16 (it is generally agreed that hundreds of billions of dollars are laundered every year).

112. *See Conference to Examine Money Cyberlaundering*, NEWSBYTES, Apr. 5, 1996, *available in* 1996 WL 8906706.

113. *See id.*; *see also Internet Aids Money Laundering Fraud Expert*, supra note 111.

114. *See Conference to Examine Money Cyberlaundering*, *supra* note 112.

115. *See Money Laundering Via Smart Cards*, REPORT ON SMART CARDS, Mar. 17, 1997, *available in* 1997 WL 8987475.

116. *See* Shannon Henry, *Digital Cash: A Boon for the Mafia?*, WASH. TECH., July 27, 1995, *available in* 1995 WL 9479159.

be a reality for one U.S. company. The Global Financial Network has been taunting the IRS and the FBI with claims of being able to "handle cash derived from any activity," and the ability to conceal and hide assets from the government and law enforcement.[117] However, it appears that after *Money Laundering Alert*[118] started e-mailing the company with questions regarding money laundering and federal law, the company either dissolved or moved its cite.[119]

Electronic cash has advantages for money laundering. First there are physical advantages. Electronic cash is not voluminous like regular cash. On the contrary, vast amounts of electronic cash can be microscopic. So electronic cash helps money launderers deal with the problem of bulk.[120] Electronic cash can be transferred to anywhere in the world in seconds.[121] It has lightning-quick transfer velocity, allowing large amounts of value to be transferred quickly and securely by just pressing a few keys on a computer keyboard.[122]

Also, electronic cash is anonymous.[123] It may actually be more anonymous than regular cash. With regular cash, there is usually, somewhere along the line, a face-to-face transfer, even if just between underlings. This is not inevitable with electronic cash. Electronic cash might be passed around the world with no two people ever seeing each other. Moreover, anonymity can be increased because traditional cash can be identified by serial numbers, but electronic cash may not be

---

117. *See U.S. Company Brazenly Offers Dubious Services on Internet*, MONEY LAUNDERING ALERT, Sept. 1, 1996, *available in* 1996 WL 8687316. The advertisement bragged that it could assist in "concealing the source of your cash earnings, getting cash into the U.S. banking system, getting cash into offshore accounts, and converting cash to other negotiable instruments." *Id.*

118. *Money Laundering Alert* is a journal that focuses on modern trends in money laundering.

119. *See U.S. Company Brazenly Offers Dubious Services on Internet, supra* note 117. We tried unsuccessfully to find the brochure of the Global Financial Network. For any one who would like to try and hunt down the Global Financial Network its website was www.globalfinance.com.

120. *See* FATF REPORT, *supra* note 14, app., at 7. Smart cards are easier to conceal than cash. *See id.* Pamela Johnson, Assistant Director of FinCEN, noted that electronic cash is easier to deal with than big sacks of cash. Johnson stated that, "[n]ow you have guns, drugs and money. Soon you'll have guns, drugs, money, the Internet and smart cards." Henry, *supra* note 116; *see also* Sarah N. Welling, *Smurfs, Money Laundering, and the Federal Criminal Law: The Crime of Structuring Transactions*, 41 FLA. L. REV. 287, 292 (1989) (noting that large physical amounts of currency often are generated through the drug trade).

121. *See Exploring the World of Cyberpayments, supra* note 7, at 16.

122. *See id.*.

123. Electronic money on the Internet can be moved anonymously, which means that neither the initiator nor the recipient is identified. *See* Alan F. Westin, *Privacy and Security Issues in the World of Electronic Financial Affairs*, in AALS Conference Pamphlet 486 (1996) (discussion paper) (on file with author).

individually identifiable. Anonymity is also enhanced because illegitimate cyberbanks can hide their location through phantom electronic forwarding addresses.[124] The phantom locations of some cyberbanks, along with the ease of movement from one location to another, will make it hard for the government to track money launderers.[125]

Electronic cash also has legal advantages. Regular cash is, at least initially, the payment system of choice for people with dirty money because cash tells no tales—it cannot be traced. But cash is not a good medium for holding booty in the long run because in large quantities it is unwieldy. Also, in cash form, it provides no return. It must be placed into the financial system to cure these problems. So, persons with dirty money eventually seek to get it into the financial system.

Exploiting this need, the government has imposed reporting requirements for large cash transactions.[126] When cash is put into the financial system or moved into or out of the U.S., financial institutions, businesses and persons are under a series of reporting duties which create a trail on the cash. Reporting requirements are imposed at a series of information chokepoints. The reports make the cash traceable.

Electronic cash is not covered by the Bank Secrecy Act reporting requirements now. But even if the BSA definitions were adjusted to make the reporting requirements apply to electronic cash, it would not be a complete solution. Electronic cash might not present as good an information chokepoint as cash because persons holding electronic cash have less need to insert it into the existing financial system. Assuming electronic cash is widely accepted, the value can stay in electronic cash form indefinitely. There is not the same incentive to get it into the regular financial system because it does not have the unwieldy bulk of

---

124. *See also* Sarah J. Hughes, *"Phantom" Cyberbanks Pose Laundering, Tax Evasion Threat,,* MONEY LAUNDERING ALERT, July 1, 1995, *available in* 1995 WL 8353498 [hereinafter Hughes, *"Phantom" Cyberbanks*].

125. *See id.* The process of money laundering is often described as having three phases:

> placement, layering and integration. Electronic money facilitates each of these phases. It will help with placement. Money launderers want to place their money in legitimate sources like financial institutions and real estate where law enforcement officials cannot easily trace the money. Second, cyberspace banking will help launderers layer their transactions to make it harder to identify the beneficial owner. Third, it will enhance integration because cyberbanks give money launderers the ability to transfer huge sums of money with speed and anonymity that was nonexistent in the past.

See id.

126. *See generally* 2 SARAH WELLING ET AL., FEDERAL CRIMINAL LAW AND RELATED CIVIL ACTIONS §§ 18.1-18.5 (1998).

cash. On the other hand, the other incentive for seeking entry into the traditional system–the urge for a return–would still exist with electronic cash. There are no investment opportunities (yet) outside the traditional legal system. So electronic cash might provide an effective information chokepoint, and BSA reporting requirements would be helpful in creating a trail.

IV. CYBERLAUNDERING HYPOTHETICALS

As mentioned in the previous section, financial institutions play a crucial role in combating traditional money laundering because the reporting laws rely on them as information chokepoints. The following hypotheticals illustrate how electronic cash allows launderers to bypass information chokepoints.[127] These hypotheticals flesh out the advantages of electronic cash under the current system.

Assume Lucky Marciano, the crime kingpin, has accumulated $1,000,000 in cash from illegal operations. Because only so much can be absorbed through his lifestyle, Lucky has to launder the money.

One traditional approach would be to set up a legitimate, cash-oriented business and commingle the legitimate cash with illegally obtained cash.[128] This would give Lucky's illegal money a legitimate cover when placed in the financial system.[129] The placement phase, i.e., when cash is being entered into the financial system, however, is the stage where money launderers are most susceptible to being detected because of the reporting requirements on financial institutions.[130] With financial institutions under pressure to implement anti-money laundering programs and report any suspicious activity,[131] Lucky has

---

127. The director of FinCEN offered the following as a hypothetical:

> A person could take his government-issued welfare card that would double as a smart card, load money off of it to a drug dealer, and then the dealer could wire the money to Colombia over the Internet, without ever touching a bank. As banks are the primary way to track money-laundering, this trend effectively eliminates the money trail that feds follow to find launderers.

Henry, *supra* note 116 (quoting Stanley Morris).

128. *See* Scott Sultzer, *Money Laundering: The Scope of the Problem and Attempts to Combat It*, 63 TENN. L. REV. 143, 149 (1995).

129. *See id.*

130. *See id.* For a comprehensive and detailed discussion of the Bank Secrecy Act and bank reporting requirements, see 2 WELLING, *supra* note 126, §§ 18.1-18.5 (1998); Matthew R. Hall, Note, *An Emerging Duty to Report Criminal Conduct: Banks, Money Laundering, and the Suspicious Activity Report*, 84 KY. L.J. 643 (1995-96).

131. *See* Hall, Note, *supra* note 130. One commentator suggests that more vague and subjective standards will be released regarding the reporting of suspicious transactions along with

a problem. If Lucky can avoid financial institutions, which have the reporting requirements, and launder the money as electronic cash, then his problem just got smaller.

Electronic cash allows Lucky to avoid financial institutions because the companies issuing electronic cash are not currently defined as financial institutions. For instance, assume that Lucky has twenty minions working for him. He sends all twenty of them to the local Mondex shop where they each exchange $500 of traditional cash for Mondex's electronic cash on a smart card. They take the smart cards, which total $10,000, back to Lucky. He swipes the smart cards across his computer interface, which transfers the electronic money from the smart cards to Lucky's hard drive. Now, Lucky can get on the Internet and order goods and services from anywhere in the world and pay for it with electronic cash, or send his electronic cash anywhere in the world.

Assume that Lucky orders some furniture from Toni's Furniture and pays in electronic cash. Toni's Furniture then can take the electronic cash and either buy something with it on the Internet (which perpetuates the avoidance of information chokepoints), or deposit the electronic money into a bank that recognizes Mondex's electronic cash. The bank would credit Toni's Furniture account with the money and decrease Mondex's account.

Lucky has avoided financial institutions and so avoided the reporting requirements. The only party taking traditional cash to a bank was Mondex when it initially took the money received from Lucky's minions to the bank for its daily deposit. Mondex was not required to make a report about Lucky's suspicious minions because it is a not a financial institution.[132] Thus, the only customer that a bank could make a report about is Mondex, not Lucky.

In addition, electronic cash helps Lucky with the import and export of money. Suppose that Lucky has some illegal operations outside the United States, and he deposits all of his illegal cash in European Union Bank.[133] At this point, Lucky could have all of his illegal money sent

---

stiffer penalties for bank noncompliance. The commentator makes the interesting point that a $9500 cash transaction could be construed to be more suspicious than a $24,000 cash transaction. *See* Douglas Barnes, *Money Laundering and Regulation* (visited Mar. 29, 1997) <http://enfo.com/MailLists/rre/0099.html>.

132. Only financial institutions are covered by the reporting requirements. *See* 31 U.S.C. § 5312.

133. European Union Bank (EUB) on the Caribbean island of Antigua boasts that it is "the first offshore bank on the Internet." Antigua has extremely strict bank secrecy laws, and Antiguan banks are not under any money laundering regulations. Furthermore, Antiguan banks advertise that Antigua is not a party to any treaties that would allow for the transfer of financial information to other countries. *See Antigua Cyberbank Tests Laundering Curbs*, MONEY

to his computer's hard drive and move it anywhere.[134] Smart cards help, too. If Lucky smuggled more than $10,000 cash across United States borders, or structured around this amount, he would violate reporting requirements and getting the money across the border would have risks.[135] Last year, the government confiscated $200 million in cash from people illegally trying to enter or leave the country.[136] On the other hand, if Lucky took smart cards across the border, he would be successful.[137] The Customs Service's money-sniffing canines would be ineffective against plastic smart cards.[138] Smart cards also would be less bulky to smuggle than currency. At any rate, because smart cards are not currently defined as monetary instruments, Lucky would not have to report the cards even if their value exceeded $10,000.[139]

The Internet also can facilitate money laundering by allowing Lucky to set up a front company on the Internet. This company holds itself out as a supplier of information services. The criminal uses the company as

---

LAUNDERING ALERT, June 1, 1996, *available in* 1996 WL 8687227. *See generally European Union Bank information page* (visited Apr. 2, 1997) <http://www.eubank.ag/-eub/abouteub.htm>.

134. The Director of FinCEN has also posed a hypothetical:

> Suppose my Internet user is a narcotics trafficker or an agent for any gang of sophisticated criminals. Consider the invoices the trafficker might pay, the supplies he might order and the transactions he might accomplish if, for instance, he could download an unlimited amount of cash from a smart card to a computer, and then transmit those funds to other smart cards in locations around the world—all anonymously, all without an audit trail, all in a matter of seconds, and all without the need to resort to a traditional financial institution.

FY97 Treasury, Postal Service Appropriations Before the Subcomm. on Treasury, Postal Service & General Government, Committee on Appropriations, U.S. Senate, Apr. 17, 1996, *available in* 1996 WL 10162336 (statement of Stanley Morris, Director, Financial Crimes Enforcement Network) [hereinafter Morris Statement].

135. *See* 31 U.S.C. § 5316 (illegal to import/export $10 thousand or more in any monetary form); 2 WELLING ET AL., *supra* note 126, § 18.4 (1998) (§ 5316 only requires reports for physical movements of money). Thus, computer transfers of currency would not be covered. *See id.*

136. *See Feds Hype Electronic Commerce at Meeting of Treasury Heavies,* REPORT ON SMART CARDS, Oct. 7, 1996, *available in* 1996 WL 15842151.

137. *See* Browning, *supra* note 32 (quoting Robert E. Rubin, Treasury Secretary, "'[w]e are concerned about the use of electronic transfer of value for cross-border money laundering or cross-border tax evasion'").

138. *See Feds Hype Electronic Commerce at Meeting of Treasury Heavies, supra* note 136. For an interesting discussion of canines, their detection capabilities, and currency, see Andy G. Rickman, Note, *Currency Contamination and Drug-Sniffing Canines: Should Any Evidentiary Value Be Attached to a Dog's Alert on Cash?*, 85 KY. L.J. 199 (1997).

139. *See E-Money Laundering Gets State Department Attention, supra* note 27.

a clearinghouse for illegally obtained funds.[140] Currently, cyberlaunderers using this approach are susceptible to detection when they attempt to convert their electronic money into traditional cash.[141] However, there will come a time when the electronic cash will never return to the traditional banking system as more goods and services become available for purchase on the Internet.[142]

V. THE GOVERNMENT'S RESPONSE TO CYBERLAUNDERING

With electronic cash developing, the government is anticipating changes in money laundering.[143] Regulators are under pressure with the current growth of cyberspace financial activities to come up with a plan to combat cyberlaundering.[144] FinCEN believes that less than one percent of suspected computerized money laundering is prosecuted.[145]

To understand what laws are needed, the various interests at stake should be examined.[146]

A. *Competing Interests*

Electronic cash is still in the developmental stages.[147] Many electronic payment systems are being designed; only a few systems make it beyond the field-test stage.[148] However, many corporations and banks are planning to offer electronic products.[149] At the design stage, these companies will make decisions about cost, security, and anonymity[150] because there are no uniform standards for electronic

140. *See* Atkinson, *supra* note 110 (quoting Dr. James Backhouse of the London School of Economics).

141. *See id.*

142. *See id.*

143. *See* TOWARD ELECTRONIC MONEY, *supra* note 11. The government's anticipation of new issues was the impetus for the simulated exercises described in *supra* note 2.

144. *See id.*

145. *See Internet Aids Money Laundering Fraud Expert, supra* note 113.

146. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 28. One way FinCEN is trying to determine the various interests at stake and the impact of electronic cash on money laundering is by holding conferences and simulated exercises. The authors attended simulated exercises conducted by RAND in the spring of 1997. These simulations are described in Ann Davis, *Concerns Rise on Laundering Money On-Line*, WALL ST. J., Mar. 17, 1997, *available in* 1997 WL-WSJ 2413155.

147. *See* Froomkin, *supra* note 28, at 454.

148. *See id.*

149. *See* Wittes, *supra* note 24; Froomkin, *supra* note 28, at 454.

150. *See* Froomkin, *supra* note 28, at 454.

cash.[151] The attractiveness of these systems to money launderers will depend on the features chosen.[152]

Electronic cash providers will design their systems to maximize customer acceptance and minimize fraud.[153] The government can influence the designs of these systems.[154] The government's goal is "[t]o try to nudge the industry in a direction that does not mandate any new regulatory scheme."[155] For competitive reasons, banks want electronic cash issuers to be placed under the same recordkeeping requirements as banks.[156]

Privacy interests of consumers and merchants often will conflict with the government's interest in obtaining information to prevent money laundering.[157] If the government begins regulations too soon, it risks stifling innovation and hurting U.S. businesses' ability to compete in a global market.[158] For this reason, many experts believe it is too early for the government to intervene.[159]

---

151. *See id.*

152. *See* FATF REPORT, *supra* 14.

153. *See id.*, app., at 9.

154. *See id.* Thomas Feegel of First Virtual Holdings, Inc., an on-line financial service provider, stated that it was essential for government to be involved in the developmental stages in order to send a message to would-be money launderers.

155. Ann Davis, *Rules of the Game: On-Line Money-Laundering Sets the Regulators Abuzz*, WALL ST. J. (Europe), Mar. 18, 1997, *available* in 1997 WL-WSJE 3808229..

156. *See Internet Gives "Cash Tracking" Concerns to Task Force*, TELECOMWORLDWIRE, Mar. 20, 1997, *available in* 1997 WL 10056245; Davis, *supra* note 155 (uniform regulations are needed).

157. *See Exploring the World of Cyberpayments, supra* note 7, at 17-18; TOWARD ELECTRONIC MONEY, *supra* note 11, at vi (stating that law enforcement's interest in obtaining information often conflicts with consumers' privacy interests).

158. *See Exploring the World of Cyberpayments, supra* note 7, at vi. Alan Greenspan, Chairman of the Board of Governors of the Federal Reserve System, believes that the private sector should be allowed to solve any problems that develop in the electronic payment system area. Greenspan stated that, "[i]f we wish to foster financial innovation, we must be careful not to impose rules that inhibit it." *Feds Hype Electronic Commerce at Meeting of Treasury Heavies, supra* note 136.

159. Dr. Alan Westin has stated that it is too early to legislate in the areas of smart cards and Internet commerce. *See* Testimony of Dr. Alan F. Weston, Professor of Public Law and Government, Columbia University, and publisher of *Privacy & American Business*, Before the Subcomm. On Domestic and International Monetary Policy of the Committee on Banking and Financial Services, U.S. House of Representatives, Washington, D.C. (June 11, 1996), *available in* 1996 WL 316039 [hereinafter Westin Testimony]. According to Westin, Congress should monitor the advances of new technology in the financial services field. *See id.* In addition to Westin, Ira Magaziner, a top White House aide who heads a task force that is writing a proposed policy paper on electronic commerce, and Christina Varney, a Federal Trade Commissioner, have urged the federal government to proceed with caution regarding Internet regulation. *See* Mitch Wagner, *Feds Lean Toward Minimal Electronic-Commerce Regulations*, COMPUTERWORLD, Mar. 24, 1997, *available in* 1997 WL 7733567. Magaziner spoke at the Seventh Conference on

One of the government's main interests is in having an audit trail on electronic cash that can be followed. The critical difference between electronic cash and other payment systems (checks, credit and debit cards, wire transfers, cash) is that the other systems leave an audit trail, whereas electronic cash can be configured to leave an audit trail or not. Currently, they are designed not to generate a trail.[160] David Chaum, founder of DigiCash, Inc., stated that his corporation has received multiple requests from people wanting to change their offshore bank accounts to electronic money[161] because DigiCash does not leave an audit trail.[162]

B. *The Audit Trail*

The audit trail is the key.[163] Reconstructing the transactions is essential to any investigation and prosecution. Congress recognized this and so mandated creation of a paper trail for cash through a series of reporting requirements. Similarly, the reporting and record keeping requirements for wire transfers[164] recognize the importance of reconstructing the sequence of transactions. For electronic cash, systems can be engineered to create a trail or not.[165] Smart cards can allow the tracking and recording of almost every payment a person makes and

---

Computers, Freedom and Privacy. *See id.* Likewise, Alan Greenspan, Chairman of the Board of Governors of the Federal Reserve System, stated that the smart-card industry should be self-regulated, allowing government regulations to serve only as gap-fillers for the private sector. *See Feds Hype Electronic Commerce at Meeting of Treasury Heavies, supra* note 136; Browning *supra* note 32 (paraphrasing Greenspan as saying that the government should not interfere with the development of electronic money). Greenspan went on to say that, "[c]onsumers and merchants, not governments, will ultimately determine what new products are successful in the market place. . . . Government action can retard progress, but almost certainly cannot ensure it." *Feds Hype Electronic Commerce at Meeting of Treasury Heavies, supra* note 136. Similarly, Ian J. Macfarlane, Chairman of the Reserve Bank of Australia, stated that we should view smart cards as travelers' checks as opposed to currency. Therefore, regulating the cards would not be appropriate for the Reserve Bank. *See* Browning, *supra* note 32.

160. *See* Atkinson, *supra* note 110.

161. *See* Davis, *supra* note 155. Chaum added that his company always declined such requests. *See id.*

162. *See id.* DigiCash's system has one-way privacy in that "the system only records the origin of money that comes in, not the path of money when it goes out." *See id.*

163. *See Unaccountable for Their Actions,* SMART CARD BULL., June 1, 1996, *available in* 1996 WL 9677143 ("[t]he issue of whether or not smart cards should have an audit trail lies at the heart of the electronic purse debate"). Former head of the FBI national computer crimes squad, James Settle, stated that following the money trail resolves many crimes. *See* Wittes, *supra* note 24.

164. *See* 31 C.F.R. § 103.33.

165. *See* Froomkin, *supra* note 28, at 473.

generate extensive audit trails.[166] The government should require the issuers to design the electronic cash systems to create an audit trail, even if is more expensive.[167]

Besides an audit trail, two other suggestions minimize the benefits of electronic cash to laundering. The first is low value limits. Technology exists to allow unlimited value to be carried on a smart card.[168] But the value carried on a smart card or on the Internet can also be limited. So called micropayments, where Internet merchants receive small amounts for their merchandise, are not a major concern[169] Laundering money with electronic cash will not be economically feasible for criminals if they are limited to small amounts.[170]

The second approach to minimize laundering through electronic cash is to limit the number of peer-to-peer transactions that can be done before the electronic cash has to be encashed back through an intermediary company such as a financial institution or electronic cash issuer.[171] Peer-to-peer transactions make electronic money almost a cash equivalent. Tracking it is more difficult if, once launched, electronic cash never has to pass through any potential information chokepoint again.

Some private sector electronic cash proponents argue that electronic cash can actually reduce money laundering rather than increase it.[172] Their argument relies on the assumption that eventually electronic money will replace traditional cash as the dominant form of payment.[173] They argue that properly designed electronic cash, i.e., electronic cash systems that create a trail and are limited to low dollar amounts, could be the solution to money laundering problems.[174]

---

166. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 19-21. Electronic cash can be as fungible as traditional cash and not leave a paper trail depending upon its development. *See id.* at 27; Froomkin, *supra* note 28, at 453 (electronic or digital cash can leave a detailed audit trail or provide more anonymity than cash).

167. Suggestions for combating the money laundering potential of smart cards include forcing issuers and developers to design the cards to leave an audit trail. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 28. Results from other countries show a low criminal interest when smart cards leave audit trails. *Id.*

168. *See id.*

169. One commentator downplayed the role of the Mondex card in money laundering schemes, suggesting that Mondex cards probably were going to be limited to $500 per card. *See* Froomkin, *supra* note 28, at 475.

170. *See id.* CyberCash has limited its micropayments to $10.

171. *See* FATF REPORT, *supra* note 14, app., at 6.

172. *See* Browning, *supra* note 32.

173. *See id.*

174. *See id.*

These suggestions limits on the value of smart cards and computer accounts and limits on the number of peer-to-peer transfers before the electronic cash must go through a chokepoint—are helpful, but they are no substitute for an audit trail. Components of a working audit trail are a trail that exists, a trail that is readable, and a trail that is followable.

1. *Creating the Trail: Information Chokepoints*

> "Our primary focus has been on banks as the linchpin of any effective anti-money-laundering strategy. . . . If technology permits anonymous transactions outside the regulated banking sector, our efforts to make money-laundering riskier and costlier may go out the door."[175]

The government must be able to trace transfers of value to detect and prosecute money laundering.[176] The Bank Secrecy Act (BSA) is the set of laws that makes cash traceable. The BSA requires financial institutions, consumers, and businesses to provide data that enable law enforcement to track money.[177] The government relies on financial institutions as information "chokepoints."[178] Chokepoints are intervals or portals through which funds must pass and be recorded.[179] The BSA ensures that financial institutions maintain a paper trail on cash that the government can follow.[180]

Whether the BSA will apply to electronic cash depends on whether the issuers and products meet the BSA's definitions.[181] Regardless of whether the BSA is modified to apply to electronic cash, though, electronic cash systems should be designed to create an audit trail. As noted above, just changing the BSA to apply to electronic cash may not be effective because electronic cash does not depend as heavily on entry into the traditional financial system. The BSA was designed for cash, and merely extending it to electronic cash is not a complete solution.

---

175. Davis, *supra* note 155 (quoting Stanley Morris).

176. *See Exploring the World of Cyberpayments, supra* note 7, at 4.

177. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 28.

178. *See* FATF REPORT, *supra* note 14, app., at 4; *see also* TOWARD ELECTRONIC MONEY, *supra* note 11, at 28 (law enforcement relies on financial institutions to provide crucial information to help in the detection of money laundering); *Exploring the World of Cyberpayments, supra* note 7, at 16 (law enforcement needs banks to provide data in order to fight money laundering).

179. *See Exploring the World of Cyberpayments, supra* note 7, at 16; TOWARD ELECTRONIC MONEY, *supra* note 11, at 28 (chokepoints are checkpoints through which cash must pass).

180. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 28.

181. *See id.;* FATF REPORT, *supra* note 14, app., at 4 (definitions will play a key role in the regulation of electronic payment systems). Definitions are in 31 U.S.C. § 5312.

If money laundering is not detected in the placement phase, then electronic payment systems can make it almost impossible to catch cyberlaunderers.[182] Currently, tracking even large wholesale transfers of value by banks over wire networks is difficult.[183] Controlling laundering becomes even more difficult when any consumer with access to a computer or telephone can transfer funds instantly all over the world.[184]

2. *Reading the Trail: Cryptography*

> [E]ncryption . . . is simply a code that can prevent people from understanding what you're saying and what you're communicating, but it is a terribly sophisticated technological device.[185]

Encryption is one of the most important aspects of electronic cash.[186] Encryption protects consumer privacy and electronic commerce by preventing electronically stored value from being intercepted, stolen, and counterfeited.[187] But encryption likewise could help laundering.[188] Some encryption devices are almost undecipherable and could help facilitate criminal activities.[189] Cryptographic technology allows an Internet user to send anonymous messages.[190] Encryption software could make it almost impossible for the government to trace financial transactions.[191] According to the American Bankers

---

182. This is due to the amount of layering and integrating that is possible with high-speed computer applications. *See* INFORMATION TECHNOLOGIES, *supra* note 24.

183. *See Exploring the World of Cyberpayments, supra* note 7, at 16. Wholesale electronic transfers of funds among banks is an everyday practice around the world. *See* INFORMATION TECHNOLOGIES, *supra* note 24. However, these transfers are backed by some form of legal tender. *See Exploring the World of Cyberpayments, supra* note 7, at 22.

184. *See Exploring the World of Cyberpayments, supra* note 7, at 16.

185. eno Address, *supra* note 1, at 576, 578.

186. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 20; *Exploring the World of Cyberpayments, supra* note 7, at 11 (encryption prevents electronically stored value from being stolen).

187. *See* Westin Testimony, *supra* note 159, at 470; *Exploring the World of Cyberpayments, supra* note 7, at 11.

188. *See* Westin, *supra* note 123, at 485; TOWARD ELECTRONIC MONEY, *supra* note 11, at 30 (private sector's new innovative encryption technology could cause law enforcement some problems).

189. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 30; Reno Address, *supra* note 1, at 579 (United States supports export controls over undecipherable cryptography for national security reasons).

190. *See* Froomkin, *supra* note 28, at 414.

191. *See* Westin, *supra* note 123, at 486.

Association, "military-grade cryptography plus anonymous re-mailers plus fully anonymous digital cash plus bad guys equals perfect crimes."[192]

Encryption is a technical and complicated mathematical subject.[193] Encryption techniques are based on formulas that substitute a symbol for the true letter, number, or symbol being communicated.[194] The specific formula, called the "key," is used to code or encrypt a message.[195] If a person knows the key, he or she can unlock or decrypt the code.[196] Strong encryption techniques allow businesses and consumers in the digital world to have confidence that the information they are sending is secure.[197] The private sector is building stronger and better encryption devices into their systems to ensure reliability and authenticity.[198] DigiCash's encryption is so powerful that it cannot keep track of how its customers spend their money.[199] Technology like this creates problems for the government, which needs to be able to decrypt these messages when criminal activity is suspected.[200]

Powerful home computers make banks susceptible to financial crime.[201] Thus, banks have been developing strong security systems that will protect users on the Internet.[202] Strong security systems that protect data also can make it harder to gather the information necessary to detect money laundering.[203]

Encryption technology customarily has been developed by the military.[204] However, software developers now can write almost impene-

---

192. Wittes, *supra* note 24, at 1 (quoting Kawika Daguio of the American Bankers Association).

193. *See Exploring the World of Cyberpayments, supra* note 7, at 11. In smart card systems, the encryption lock is encoded and placed in the card's magnetic chip. *See id.*

194. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 29-30.

195. *See id.* at 30; *Don't Tell It to the Spartans*, THE ECONOMIST, Feb. 18, 1995, *available in* 1995 WL 9568266 (noting that a "key" is the rules that allow a person to encode or decode the message).

196. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 30.

197. *See id.*

198. *See id.; Net Profits, supra* note 8 (CommerceNet, a private company, will issue Mosaic with "public-key cryptography").

199. *See* Davis, *supra* note 155. DigiCash's system has one-way privacy in that "the system only records the origin of money that comes in, not the path of money when it goes out." *Id.*

200. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 30.

201. *See id.*

202. *See id.*

203. *See* Wittes, *supra* note 24. Strong cryptography could allow money laundering to become even more profitable. *See id.*; Westin, *supra* note 123, at 470 (stating that innovations in cryptography could hurt law enforcement).

204. *See* Benjamin Wittes, *The Year in Cyberlaw: The Rapid Development of the Internet Poses Intriguing New Legal Problems, as well as Possibilities*, LEGAL TIMES 5 (1996).

trable codes with relatively ease.[205] The National Security Agency has released for commercial use the Clipper Chip, which is an encryption standard that gives the government an electronic back door to decrypt codes.[206] With court authorization, law enforcement could retrieve two escrowed codes that the government maintains in storage and decrypt the signals.[207] The government hopes to encourage private companies to use Clipper chips by buying Clipper products for government use. Thus, anyone wanting to do business with the government must be using Clipper products.[208] Industry does not like the Clipper plan because it removes private enterprise from the market by establishing a uniform encryption standard.[209]

The government's ability to control money laundering may depend on decisions made in the genesis of electronic payment systems. Setting up a "key" system will allow the government access to the information upon a showing of probable cause. Of course this approach would not expand government power but would only preserve the status quo.[210]

Some cryptographic algorithms are almost impenetrable and are more protected than currency.[211] Janet Reno stated that "our goal must be to encourage strong encryption for privacy in commerce [while] preserving law enforcement's ability to protect public safety and national security."[212] Encoding the cash where only the government or a

---

205. *See id.*

206. *See id.* For a comprehensive examination of the issues surrounding the "Clipper Chip," see Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189 (1996); Henry R. King, Note, *Big Brother, The Holding Company: A Review of Key-Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224 (1995); Charlene L. Lu, Note, *Seeking Privacy in Wireless Communications: Balancing the Right of Individual Privacy with the Need for Effective Law Enforcement*, 17 HASTINGS COMM. & ENT. L.J. 529 (1995); Mark I. Koffsky, Comment, *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, 9 HIGH TECH. L.J. 131 (1994).

207. *See* Wittes, *The Year in Cyberlaw*, *supra* note 204.

208. *See id.*

209. *See id.* The Clinton Administration has started buying Clipper phones. *See id.*

210. *See* Reno Address, *supra* note 1, at 577.

211. David Chaum, who heads DigiCash, has made a series of mathematical algorithms and formulas that use encryption technology to make financial transactions untraceable. DigiCash's on-line payment system, "e-cash," is in the later stages of testing.

212. Reno Address, *supra* note 1, at 577. Reno also stated that,

> Some suggest that the answer is simply better technology and more money for law enforcement. They say if law enforcement is given the money, it can decode even sophisticated 56-bit encryption. That's simply not true. Money aside, decoding a 56-bit key using current technology is so time consuming as to render the results useless to law enforcement. We estimate that even with the top of the line super-

trusted third party could read and understand it is one way to provide privacy and meet law enforcement's needs.[213] The government's right to use the information from this "clipperized cash" could have built-in safeguards to prevent abuse.[214] Janet Reno went on to state that,

> A consensus is now emerging throughout much of the world that the best way to achieve this balance is by creating a system, otherwise known as Key Escrow, to entrust the encryption keys with a neutral third party—these keys, in effect, unlocking the code under certain circumstances. The government would then obtain the keys from the escrow agent to decrypt the data but only as part of a legally authorized and court-supervised investigation. We are not looking to expand federal power or to increase our authority to wiretap or to search. We look only to make existing law apply to new technology.[215]

Currently, a Key Management Infrastructure (KMI) has been proposed.[216] With the permission of the court, the KMI would allow certain federal officials access to the "keys" that would decrypt messages that were encrypted by private sector technology.[217] The debate continues on this proposal.[218]

Encrypted data must be accessible by the government,[219] but it should only be accessible on a showing of probable cause. This would mean no change in the Fourth Amendment law beyond adjustments to accommodate new technology.

3. *Following the Trail: International Cooperation*

The audit trail has to exist, it has to be readable, and ultimately it has to be followable. Electronic cash flows easily over borders, so following an audit trail on electronic cash demands international cooperation. Global economic integration benefits criminals as well as

---

> computer, decoding a 56-bit key would take over a year and the evidence would be long gone. That's clearly too long.

Id. at 576-78.

213. *See* Froomkin, *supra* note 28, at 503.

214. *See id.*

215. Reno Address, *supra* note 1, at 577.

216. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 30.

217. *See id.*

218. *See id.*

219. *See* Reno Address, *supra* note 1, at 576; *Net Profits*, *supra* note 8 (noting that the federal government is discouraging encryption technology that cannot be tapped).

legitimate business;[220] money can be laundered without regard for international borders.[221] Governments have to cooperate; global cooperation in fighting money laundering is essential.[222] The Internet allows anonymous international cash flows.[223] The Internet and the global marketplace could allow money launderers to transfer funds to countries that have weak money laundering laws.[224] FinCEN projects that cyberspace activities will allow billions of dollars to be transferred across national borders every year.[225]

One problem with international enforcement of money laundering measures is determining jurisdictional authority.[226] The current regulatory system is based on established geographic and financial

---

220. *See Noble Warns of Technological Progress as Boon to Laundering*, MONEY LAUNDERING ALERT, June 1, 1995, *available in* 1995 WL 8353473.

221. *See id.*; TOWARD ELECTRONIC MONEY, *supra* note 11, at 34 (stating that many electronic payment systems operate beyond national boundaries).

222. *See* FINCEN YEAR END REVIEW (1994); *E-Money Laundering Gets State Department Attention*, *supra* note 27. Money laundering through electronic payment systems by drug traffickers and mafia organizations is one of the biggest problems that the Bureau for International Narcotics and Law Enforcement Affairs (INL) faces. INL is part of the United States Department of State. *See id. See also* TOWARD ELECTRONIC MONEY, *supra* note 11, at 34. For an interesting discussion of how cultural differences in Thailand, China, and Taiwan may preclude effective anti-money laundering legislation, see Douglas Barnes, *Money Laundering and Bank Regulation* (visited Apr. 3, 1997) <http://www.enfo.com/ maillists/rre/0099.html>. Barnes, who attended the Fourth International Conference on Money Laundering, Forfeiture, Asset Recovery, Offshore Investments, the Pacific Rim and International Financial Crimes, stated that,

> Chinese people (who are in the majority in Taiwan, and form an economically active minority in Thailand) are very cash-oriented; I vividly remember payday in Taiwan, with the boss sitting at a table piled with money, bundling up salaries for everyone. I'd come home at the end of each month with a giant wad of cash from my several different jobs. One could hardly imagine a better environment for money laundering than a society in which large quantities of cash change hands on a regular basis.

Id.

223. *See Internet Aids Money Laundering Fraud Expert*, *supra* note 113; Wittes, *supra* note 24 (stating that national borders are irrelevant on the Internet); *E-Money Laundering Gets State Department Attention*, *supra* note 27 (finding that the movement of large amounts of drug-tainted money across international borders via electronic payment systems is one of the biggest problems facing law enforcement).

224. *See* FATF REPORT, *supra* note 14, app., at 7. Money launderers have a tendency to move their operations to countries that have weak anti-money laundering laws. *See* FINCEN NEWS, U.S. Dept. Of Treasury, FATF REPORT HIGHLIGHTS MONEY LAUNDERING TRENDS, Feb. 6, 1997 [hereinafter FINCEN HIGHLIGHTS].

225. *See* Hughes, *"Phantom" Cyberbanks*, *supra* note 124.

226. FATF REPORT, *supra* note 14, at 16.

boundaries.[227] Because international borders are less important with modern technology, global cooperation and coordination is necessary to fight money laundering.[228] As long as one industrialized nation chooses not to regulate anonymizing technology, the Internet will allow everyone connected to have anonymous communications.[229]

The Financial Action Task Force (FATF) is a twenty-six nation organization formed to address the international problem of money laundering.[230] The primary purpose behind the 1996-97 FATF Typologies meeting at the Organization for Economic Co-operation and Development (OECD) was to start a dialogue between FATF members and international designers of electronic payment systems.[231] In an attempt to fully address the ramifications that those electronic payment systems could have on international money laundering, the FATF invited private-sector representatives and banking associations to its 1996 meeting.[232]

As to privacy concerns, the European Union (EU) approach poses a glitch for the United States. The (EU) has issued Directive 95/46/EC, which establishes protections for individual privacy that are not necessarily reciprocated by United States law.[233] The EU's Data Protection Directive states that if a company is outside of the EU and wants to transfer personal data regarding an EU citizen outside of the EU, then the company must satisfy one of the following requirements: (1) the country that will be receiving the information must have "adequate" privacy safeguards based on EU standards, or (2) the business must show that its procedures meet the EU's standards by other means.[234] The Directive might prohibit EU member states from

227. *See E-Money Laundering Gets State Department Attention*, *supra* note 27; FATF REPORT, *supra* note 14, at 16 (stating that jurisdictional authority is based on national borders).

228. *See* FATF REPORT, *supra* note 14, at 16; *see also* Greg Steinmetz, *Tax Cheats, Mafia Still Drawn to Swiss Banks—Firms' Penchant for Secrecy Undercuts Tough Anticrime Effort*, WALL ST. J., July 3, 1996, *available in* 1996 WL-WSJ 3109339 (noting that the following countries lead the way regarding mutual legal assistance requests: (1) Switzerland—189, (2) Canada—138, (3) U.K.—136, (4) Germany—99, (5) Cayman Islands—83, (6) Mexico—79, and (7) Bahamas—59).

229. *See* Froomkin, *supra* note 28, at 400.

230. *See* FINCEN HIGHLIGHTS, *supra* note 224.

231. *See* FATF REPORT, *supra* note 14, app., at 1. This meeting was held in Paris, France. On a related point, Janet Reno stated that, "While some countries still have weak laws, or no laws, against computer crime, I am pleased to report that this is changing. U.S. law enforcement agencies are quick to help with training and also unhesitatingly offer and solicit cooperation in investigating international computer crimes." Reno Address, *supra* note 1, at 580.

232. *See* FATF REPORT, *supra* note 14, at 1.

233. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 34.

234. *See* Westin Testimony, *supra* note 159; TOWARD ELECTRONIC MONEY, *supra* note 11,

sending computer processed information on individuals being investigated by the United States.[235] The EU will activate the Directive in 1998.[236]

Neither the Clinton Administration nor the Congress supports the adoption of a privacy regulatory authority similar to the one in the EU.[237] Likewise, the American public does not support a privacy regulatory authority.[238] However, without comprehensive privacy policies, U.S. companies might have problems expanding the globalization of their services. They may have to deny the government information from EU member states.[239]

The resolution of this international glitch remains unclear. What is clear is that countries have to work out a way to coordinate their money laundering laws.[240]

VI. CONCLUSION

Money laundering with electronic cash could become a major crime if the government does not move carefully. It is probably too early to legislate in this area, but the government should keep in mind the possibilities of limiting the value of electronic cash that can be put on smart cards and Internet-based accounts and limiting the number of peer-to-peer transactions. More importantly, the government should work to be sure (1) that electronic cash systems are engineered to produce an audit trail; (2) that the trail can be decrypted on a showing of probable cause by use of the Clipper Chip; and (3) that the trail can be followed by continuing efforts toward international cooperation. These approaches will minimize, and perhaps extinguish, the advantages electronic cash provides for money laundering.

---

at 34-35 (stating that the Directive declares that a member country should not transfer information about an individual to a third country unless that country offers similar privacy protections).

235. *See* TOWARD ELECTRONIC MONEY, *supra* note 11, at 35.

236. *See* Westin Testimony, *supra* note 159, at 471; *see generally* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995) (discussing the EU Directive and its potential effects).

237. *See* Westin, *supra* note 159, at 485.

238. *See id.*

239. *See id.*

240. *See* Lisa A. Barbot, Comment, *Money Laundering: An International Challenge*, 3 TUL. J. INT'L & COMP. L. 161, 200 (1995); *Money Laundering Via Smart Cards*, *supra* note 115 (stating that governments are starting to understand the need for cooperation in order to combat money laundering).